

MCAFFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

19970 - IBM AIX OpenSSL Denial of Service Vulnerability

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

Risk Level: High

CVE: CVE-2016-2842

Description

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

Observation

IBM AIX is a Unix-like operating system.

A denial of service vulnerability is present in some versions of IBM AIX. The flaw lies in OpenSSL component. Successful exploitation could allow an attacker to cause denial of service condition.

19985 - Apache Struts2 Dynamic Method Invocation Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-3081

Description

A remote code execution vulnerability is present in some versions of Apache Struts.

Observation

Apache Struts is a web application framework.

A remote code execution vulnerability is present in some versions of Apache Struts. The flaw lies in Dynamic Method Invocation. Successful exploitation could allow an attacker to execute arbitrary code.

144547 - SuSE Linux 11.4 openSUSE-SU-2016:1157-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1019

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1157-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-04/msg00100.html>

SuSE Linux 11.4

x86_64

flash-player-gnome-11.2.202.616-182.1

flash-player-11.2.202.616-182.1

flash-player-kde4-11.2.202.616-182.1

i586

flash-player-gnome-11.2.202.616-182.1

flash-player-11.2.202.616-182.1

flash-player-kde4-11.2.202.616-182.1

144548 - SuSE Linux 11.4 openSUSE-SU-2016:1107-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6150, CVE-2013-4408, CVE-2013-4496, CVE-2015-0240, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-5330, CVE-2015-5370, CVE-2015-7560, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1107-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-04/msg00077.html>

SuSE Linux 11.4

i586

libtevent0-debuginfo-0.9.11-141.1

samba-winbind-debuginfo-3.6.3-141.1

libnetapi0-3.6.3-141.1

libtdb1-debuginfo-1.2.9-141.1

libsmbsharemodes0-debuginfo-3.6.3-141.1

libnetapi-devel-3.6.3-141.1

libtalloc-devel-2.0.5-141.1

libldb1-debuginfo-1.0.2-141.1

samba-winbind-3.6.3-141.1

libldb1-1.0.2-141.1

libnetapi0-debuginfo-3.6.3-141.1

samba-devel-3.6.3-141.1

libsmbclient-devel-3.6.3-141.1

samba-client-3.6.3-141.1

samba-krb-printing-3.6.3-141.1

samba-3.6.3-141.1

libsmbclient0-debuginfo-3.6.3-141.1

libtevent-devel-0.9.11-141.1

libsmbsharemodes0-3.6.3-141.1

libsmbclient0-3.6.3-141.1

libwbclient0-debuginfo-3.6.3-141.1

libldb-devel-1.0.2-141.1

samba-debugsource-3.6.3-141.1
libtdb1-1.2.9-141.1
libtalloc2-debuginfo-2.0.5-141.1
samba-client-debuginfo-3.6.3-141.1
libwbclient-devel-3.6.3-141.1
samba-debuginfo-3.6.3-141.1
libsmbsharemodes-devel-3.6.3-141.1
samba-krb-printing-debuginfo-3.6.3-141.1
libwbclient0-3.6.3-141.1
libtalloc2-2.0.5-141.1
libevent0-0.9.11-141.1
libtdb-devel-1.2.9-141.1
ldapsmb-1.34b-141.1

noarch
samba-doc-3.6.3-141.1

x86_64
libevent0-debuginfo-0.9.11-141.1
libsmbclient0-32bit-3.6.3-141.1
libtdb1-32bit-1.2.9-141.1
samba-winbind-debuginfo-3.6.3-141.1
libnetapi0-3.6.3-141.1
libtdb1-debuginfo-1.2.9-141.1
libldb1-32bit-1.0.2-141.1
libsmbsharemodes0-debuginfo-3.6.3-141.1
libnetapi-devel-3.6.3-141.1
libtalloc-devel-2.0.5-141.1
libldb1-debuginfo-1.0.2-141.1
samba-winbind-3.6.3-141.1
libwbclient0-32bit-3.6.3-141.1
samba-32bit-3.6.3-141.1
libldb1-1.0.2-141.1
libldb1-debuginfo-32bit-1.0.2-141.1
libevent0-32bit-0.9.11-141.1
libnetapi0-debuginfo-3.6.3-141.1
samba-client-32bit-3.6.3-141.1
samba-debuginfo-32bit-3.6.3-141.1
samba-devel-3.6.3-141.1
libsmbclient-devel-3.6.3-141.1
samba-client-3.6.3-141.1
samba-krb-printing-3.6.3-141.1
samba-3.6.3-141.1
libtalloc2-32bit-2.0.5-141.1
libsmbclient0-debuginfo-3.6.3-141.1
libevent-devel-0.9.11-141.1
libsmbsharemodes0-3.6.3-141.1
libsmbclient0-3.6.3-141.1
libwbclient0-debuginfo-3.6.3-141.1
samba-winbind-debuginfo-32bit-3.6.3-141.1
libldb-devel-1.0.2-141.1
samba-debugsource-3.6.3-141.1
libtdb1-1.2.9-141.1
samba-winbind-32bit-3.6.3-141.1
libsmbclient0-debuginfo-32bit-3.6.3-141.1
libtalloc2-debuginfo-2.0.5-141.1
libwbclient0-debuginfo-32bit-3.6.3-141.1
samba-client-debuginfo-3.6.3-141.1
libevent0-debuginfo-32bit-0.9.11-141.1
libtdb1-debuginfo-32bit-1.2.9-141.1

libwbclient-devel-3.6.3-141.1
samba-debuginfo-3.6.3-141.1
libsmbsharemodes-devel-3.6.3-141.1
samba-krb-printing-debuginfo-3.6.3-141.1
libtalloc2-debuginfo-32bit-2.0.5-141.1
libwbclient0-3.6.3-141.1
samba-client-debuginfo-32bit-3.6.3-141.1
libtalloc2-2.0.5-141.1
libtevent0-0.9.11-141.1
libtdb-devel-1.2.9-141.1
ldapsmb-1.34b-141.1

144551 - SuSE SLES 11 SP4 SUSE-SU-2016:1145-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9767, CVE-2015-7803, CVE-2015-8835, CVE-2015-8838, CVE-2016-2554, CVE-2016-3141, CVE-2016-3142, CVE-2016-3185

Description

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

SUSE-SU-2016:1145-1

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-April/002026.html>

SuSE SLES 11 SP4

i586

php53-gd-5.3.17-59.1
php53-suhosin-5.3.17-59.1
php53-snmp-5.3.17-59.1
php53-mysql-5.3.17-59.1
php53-bz2-5.3.17-59.1
php53-gettext-5.3.17-59.1
php53-fileinfo-5.3.17-59.1
php53-ftp-5.3.17-59.1
php53-iconv-5.3.17-59.1
php53-pear-5.3.17-59.1
php53-mbstring-5.3.17-59.1
php53-pdo-5.3.17-59.1
php53-mcrypt-5.3.17-59.1
php53-dom-5.3.17-59.1
php53-curl-5.3.17-59.1
php53-zlib-5.3.17-59.1
php53-pgsql-5.3.17-59.1
php53-dba-5.3.17-59.1
php53-tokenizer-5.3.17-59.1
php53-exif-5.3.17-59.1
php53-fastcgi-5.3.17-59.1
php53-json-5.3.17-59.1
apache2-mod_php53-5.3.17-59.1
php53-ldap-5.3.17-59.1
php53-sysvmsg-5.3.17-59.1
php53-sysvshm-5.3.17-59.1
php53-pcntl-5.3.17-59.1

php53-gmp-5.3.17-59.1
php53-soap-5.3.17-59.1
php53-zip-5.3.17-59.1
php53-sysvsem-5.3.17-59.1
php53-ctype-5.3.17-59.1
php53-pspell-5.3.17-59.1
php53-xsl-5.3.17-59.1
php53-shmop-5.3.17-59.1
php53-calendar-5.3.17-59.1
php53-odbc-5.3.17-59.1
php53-bcmath-5.3.17-59.1
php53-intl-5.3.17-59.1
php53-openssl-5.3.17-59.1
php53-xmlreader-5.3.17-59.1
php53-xmlrpc-5.3.17-59.1
php53-wddx-5.3.17-59.1
php53-5.3.17-59.1
php53-xmlwriter-5.3.17-59.1

x86_64

php53-gd-5.3.17-59.1
php53-suhosin-5.3.17-59.1
php53-snmp-5.3.17-59.1
php53-mysql-5.3.17-59.1
php53-bz2-5.3.17-59.1
php53-gettext-5.3.17-59.1
php53-fileinfo-5.3.17-59.1
php53-ftp-5.3.17-59.1
php53-iconv-5.3.17-59.1
php53-pear-5.3.17-59.1
php53-mbstring-5.3.17-59.1
php53-pdo-5.3.17-59.1
php53-mcrypt-5.3.17-59.1
php53-dom-5.3.17-59.1
php53-curl-5.3.17-59.1
php53-zlib-5.3.17-59.1
php53-pgsql-5.3.17-59.1
php53-dba-5.3.17-59.1
php53-tokenizer-5.3.17-59.1
php53-exif-5.3.17-59.1
php53-fastcgi-5.3.17-59.1
php53-json-5.3.17-59.1
apache2-mod_php53-5.3.17-59.1
php53-ldap-5.3.17-59.1
php53-sysvmsg-5.3.17-59.1
php53-sysvshm-5.3.17-59.1
php53-pcntl-5.3.17-59.1
php53-gmp-5.3.17-59.1
php53-soap-5.3.17-59.1
php53-zip-5.3.17-59.1
php53-sysvsem-5.3.17-59.1
php53-ctype-5.3.17-59.1
php53-pspell-5.3.17-59.1
php53-xsl-5.3.17-59.1
php53-shmop-5.3.17-59.1
php53-calendar-5.3.17-59.1
php53-odbc-5.3.17-59.1
php53-bcmath-5.3.17-59.1
php53-intl-5.3.17-59.1
php53-openssl-5.3.17-59.1

php53-xmlreader-5.3.17-59.1
php53-xmlrpc-5.3.17-59.1
php53-wddx-5.3.17-59.1
php53-5.3.17-59.1
php53-xmlwriter-5.3.17-59.1

144553 - SuSE Linux 13.2 openSUSE-SU-2016:1135-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1651, CVE-2016-1652, CVE-2016-1653, CVE-2016-1654, CVE-2016-1655, CVE-2016-1656, CVE-2016-1657, CVE-2016-1658, CVE-2016-1659

Description

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

openSUSE-SU-2016:1135-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-04/msg00091.html>

SuSE Linux 13.2

x86_64

chromedriver-debuginfo-50.0.2661.75-94.3
chromium-desktop-gnome-50.0.2661.75-94.3
chromium-ffmpegsumo-debuginfo-50.0.2661.75-94.3
chromedriver-50.0.2661.75-94.3
chromium-debuginfo-50.0.2661.75-94.3
chromium-ffmpegsumo-50.0.2661.75-94.3
chromium-desktop-kde-50.0.2661.75-94.3
chromium-debugsource-50.0.2661.75-94.3
chromium-50.0.2661.75-94.3

i586

chromedriver-debuginfo-50.0.2661.75-94.3
chromium-desktop-gnome-50.0.2661.75-94.3
chromium-ffmpegsumo-debuginfo-50.0.2661.75-94.3
chromedriver-50.0.2661.75-94.3
chromium-debuginfo-50.0.2661.75-94.3
chromium-ffmpegsumo-50.0.2661.75-94.3
chromium-desktop-kde-50.0.2661.75-94.3
chromium-debugsource-50.0.2661.75-94.3
chromium-50.0.2661.75-94.3

144554 - SuSE Linux 13.1 openSUSE-SU-2016:1106-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6150, CVE-2013-4408, CVE-2013-4496, CVE-2015-0240, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-5330, CVE-2015-5370, CVE-2015-7560, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

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

openSUSE-SU-2016:1106-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-04/msg00076.html>

SuSE Linux 13.1

i586

libregistry-devel-4.2.4-3.54.2

libsamdb-devel-4.2.4-3.54.2

libndr-standard0-4.2.4-3.54.2

libsamba-util0-debuginfo-4.2.4-3.54.2

libsmbconf0-4.2.4-3.54.2

libnetapi0-debuginfo-4.2.4-3.54.2

libsmbconf0-debuginfo-4.2.4-3.54.2

libnetapi0-4.2.4-3.54.2

ctdb-devel-4.2.4-3.54.2

samba-pidl-4.2.4-3.54.2

libsamba-util0-4.2.4-3.54.2

libsamba-hostconfig-devel-4.2.4-3.54.2

libregistry0-4.2.4-3.54.2

libsamba-policy-devel-4.2.4-3.54.2

libdcerpc-atsvc0-debuginfo-4.2.4-3.54.2

samba-debuginfo-4.2.4-3.54.2

samba-libs-4.2.4-3.54.2

libsamba-credentials0-debuginfo-4.2.4-3.54.2

ctdb-tests-4.2.4-3.54.2

ctdb-pcp-pmda-4.2.4-3.54.2

libtevent-util-devel-4.2.4-3.54.2

libsmbclient-devel-4.2.4-3.54.2

libdcerpc-binding0-debuginfo-4.2.4-3.54.2

libsmbclient0-4.2.4-3.54.2

libsamba-credentials-devel-4.2.4-3.54.2

libndr-nbt0-4.2.4-3.54.2

samba-python-4.2.4-3.54.2

libdcerpc0-debuginfo-4.2.4-3.54.2

libnetapi-devel-4.2.4-3.54.2

libsamba-credentials0-4.2.4-3.54.2

libdcerpc-samr0-4.2.4-3.54.2

libsamba-hostconfig0-4.2.4-3.54.2

libsmbconf-devel-4.2.4-3.54.2

samba-test-debuginfo-4.2.4-3.54.2

libsamba-policy0-4.2.4-3.54.2

libsamba-util-devel-4.2.4-3.54.2

libtevent-util0-debuginfo-4.2.4-3.54.2

samba-winbind-debuginfo-4.2.4-3.54.2

libdcerpc-samr-devel-4.2.4-3.54.2

libsamdb0-4.2.4-3.54.2

libsamba-passsdb0-debuginfo-4.2.4-3.54.2

libndr-nbt0-debuginfo-4.2.4-3.54.2

samba-libs-debuginfo-4.2.4-3.54.2

samba-debugsource-4.2.4-3.54.2

samba-python-debuginfo-4.2.4-3.54.2

libsamba-passsdb-devel-4.2.4-3.54.2

libwbclient0-debuginfo-4.2.4-3.54.2

libwbclient-devel-4.2.4-3.54.2

libsmbclient-raw-devel-4.2.4-3.54.2

ctdb-4.2.4-3.54.2

libdcerpc-binding0-4.2.4-3.54.2
libndr-standard0-debuginfo-4.2.4-3.54.2
libndr-standard-devel-4.2.4-3.54.2
ctdb-pcp-pmda-debuginfo-4.2.4-3.54.2
libwbclient0-4.2.4-3.54.2
samba-client-debuginfo-4.2.4-3.54.2
libregistry0-debuginfo-4.2.4-3.54.2
libgensec-devel-4.2.4-3.54.2
libndr-krb5pac0-4.2.4-3.54.2
libsmbldap-devel-4.2.4-3.54.2
libtevent-util0-4.2.4-3.54.2
samba-client-4.2.4-3.54.2
libsmbldap0-debuginfo-4.2.4-3.54.2
samba-winbind-4.2.4-3.54.2
samba-4.2.4-3.54.2
samba-test-devel-4.2.4-3.54.2
libgensec0-debuginfo-4.2.4-3.54.2
libndr0-4.2.4-3.54.2
libdcerpc-devel-4.2.4-3.54.2
libdcerpc-samr0-debuginfo-4.2.4-3.54.2
libndr-krb5pac0-debuginfo-4.2.4-3.54.2
libsmbclient0-debuginfo-4.2.4-3.54.2
libgensec0-4.2.4-3.54.2
libndr-devel-4.2.4-3.54.2
libdcerpc0-4.2.4-3.54.2
libdcerpc-atsvc0-4.2.4-3.54.2
samba-test-4.2.4-3.54.2
ctdb-debuginfo-4.2.4-3.54.2
libsmbclient-raw0-debuginfo-4.2.4-3.54.2
libsamdb0-debuginfo-4.2.4-3.54.2
libndr-nbt-devel-4.2.4-3.54.2
libsmbclient-raw0-4.2.4-3.54.2
samba-core-devel-4.2.4-3.54.2
libdcerpc-atsvc-devel-4.2.4-3.54.2
libndr-krb5pac-devel-4.2.4-3.54.2
ctdb-tests-debuginfo-4.2.4-3.54.2
libsamba-hostconfig0-debuginfo-4.2.4-3.54.2
libsamba-passdb0-4.2.4-3.54.2
libsmbldap0-4.2.4-3.54.2
libndr0-debuginfo-4.2.4-3.54.2
libsamba-policy0-debuginfo-4.2.4-3.54.2

noarch
samba-doc-4.2.4-3.54.2

x86_64
libsamba-passdb0-32bit-4.2.4-3.54.2
ctdb-debuginfo-4.2.4-3.54.2
libsamba-util0-debuginfo-32bit-4.2.4-3.54.2
libndr-standard0-4.2.4-3.54.2
libsmbclient0-debuginfo-4.2.4-3.54.2
libsamba-passdb-devel-4.2.4-3.54.2
libndr-standard0-32bit-4.2.4-3.54.2
libgensec-devel-4.2.4-3.54.2
libsamba-passdb0-4.2.4-3.54.2
libwbclient0-32bit-4.2.4-3.54.2
libregistry0-32bit-4.2.4-3.54.2
samba-debuginfo-4.2.4-3.54.2
libsamdb0-4.2.4-3.54.2
libdcerpc-samr0-debuginfo-4.2.4-3.54.2

libgensec0-4.2.4-3.54.2
libsamba-passdb0-debuginfo-4.2.4-3.54.2
libsamba-util-devel-4.2.4-3.54.2
libndr-krb5pac0-debuginfo-4.2.4-3.54.2
libsamba-credentials0-debuginfo-32bit-4.2.4-3.54.2
libndr0-4.2.4-3.54.2
libsamba-policy0-debuginfo-4.2.4-3.54.2
samba-test-debuginfo-4.2.4-3.54.2
libdcerpc-atsvc-devel-4.2.4-3.54.2
libdcerpc-atsvc0-4.2.4-3.54.2
samba-libs-32bit-4.2.4-3.54.2
libdcerpc-devel-4.2.4-3.54.2
samba-32bit-4.2.4-3.54.2
libsmbldap-devel-4.2.4-3.54.2
libsmbldap0-debuginfo-4.2.4-3.54.2
libsamba-policy-devel-4.2.4-3.54.2
libsmbconf0-debuginfo-32bit-4.2.4-3.54.2
libsmbconf0-32bit-4.2.4-3.54.2
samba-winbind-debuginfo-32bit-4.2.4-3.54.2
libgensec0-32bit-4.2.4-3.54.2
libregistry0-debuginfo-32bit-4.2.4-3.54.2
libdcerpc0-4.2.4-3.54.2
libdcerpc-binding0-debuginfo-32bit-4.2.4-3.54.2
samba-pidl-4.2.4-3.54.2
libsmbldap0-4.2.4-3.54.2
libnetapi-devel-4.2.4-3.54.2
libwbclient0-debuginfo-32bit-4.2.4-3.54.2
samba-client-debuginfo-32bit-4.2.4-3.54.2
libsmbclient0-32bit-4.2.4-3.54.2
libsmbclient-raw0-debuginfo-32bit-4.2.4-3.54.2
samba-winbind-4.2.4-3.54.2
samba-libs-debuginfo-32bit-4.2.4-3.54.2
libsmbclient-raw0-32bit-4.2.4-3.54.2
libdcerpc-binding0-4.2.4-3.54.2
libsamdb0-32bit-4.2.4-3.54.2
ctdb-devel-4.2.4-3.54.2
libgensec0-debuginfo-32bit-4.2.4-3.54.2
samba-client-32bit-4.2.4-3.54.2
libsamba-policy0-debuginfo-32bit-4.2.4-3.54.2
libdcerpc0-32bit-4.2.4-3.54.2
libtevent-util-devel-4.2.4-3.54.2
libsmbclient-raw0-4.2.4-3.54.2
libregistry-devel-4.2.4-3.54.2
libsmbconf-devel-4.2.4-3.54.2
libdcerpc-atsvc0-debuginfo-32bit-4.2.4-3.54.2
libsamba-credentials0-4.2.4-3.54.2
libwbclient-devel-4.2.4-3.54.2
samba-client-debuginfo-4.2.4-3.54.2
libndr-standard0-debuginfo-4.2.4-3.54.2
libdcerpc-samr-devel-4.2.4-3.54.2
libndr-krb5pac0-32bit-4.2.4-3.54.2
libdcerpc-atsvc0-32bit-4.2.4-3.54.2
libndr-krb5pac-devel-4.2.4-3.54.2
libsamba-credentials0-debuginfo-4.2.4-3.54.2
libregistry0-4.2.4-3.54.2
libdcerpc-samr0-debuginfo-32bit-4.2.4-3.54.2
samba-libs-4.2.4-3.54.2
ctdb-4.2.4-3.54.2
libsmbclient0-4.2.4-3.54.2
samba-core-devel-4.2.4-3.54.2

libndr-krb5pac0-4.2.4-3.54.2
ctdb-tests-4.2.4-3.54.2
libtevent-util0-32bit-4.2.4-3.54.2
samba-python-debuginfo-4.2.4-3.54.2
libtevent-util0-debuginfo-4.2.4-3.54.2
libsmbclient-devel-4.2.4-3.54.2
libtevent-util0-debuginfo-32bit-4.2.4-3.54.2
libndr-devel-4.2.4-3.54.2
libndr-krb5pac0-debuginfo-32bit-4.2.4-3.54.2
samba-debuginfo-32bit-4.2.4-3.54.2
libgensec0-debuginfo-4.2.4-3.54.2
libsmbldap0-debuginfo-32bit-4.2.4-3.54.2
libsamba-hostconfig-devel-4.2.4-3.54.2
libregistry0-debuginfo-4.2.4-3.54.2
libndr-standard-devel-4.2.4-3.54.2
libnetapi0-debuginfo-4.2.4-3.54.2
ctdb-pcp-pmda-4.2.4-3.54.2
libsmbldap0-32bit-4.2.4-3.54.2
libndr-nbt0-debuginfo-32bit-4.2.4-3.54.2
libndr-nbt-devel-4.2.4-3.54.2
libsamba-hostconfig0-debuginfo-32bit-4.2.4-3.54.2
samba-4.2.4-3.54.2
libsmbconf0-4.2.4-3.54.2
libndr0-32bit-4.2.4-3.54.2
libsamdb-devel-4.2.4-3.54.2
libsamba-util0-32bit-4.2.4-3.54.2
libsmbclient0-debuginfo-32bit-4.2.4-3.54.2
samba-winbind-debuginfo-4.2.4-3.54.2
libsamba-credentials-devel-4.2.4-3.54.2
ctdb-tests-debuginfo-4.2.4-3.54.2
libwbclient0-debuginfo-4.2.4-3.54.2
libdcerpc-samr0-4.2.4-3.54.2
libdcerpc0-debuginfo-32bit-4.2.4-3.54.2
libnetapi0-debuginfo-32bit-4.2.4-3.54.2
libsamdb0-debuginfo-32bit-4.2.4-3.54.2
libsamba-util0-debuginfo-4.2.4-3.54.2
libsamba-policy0-4.2.4-3.54.2
libsamba-credentials0-32bit-4.2.4-3.54.2
ctdb-pcp-pmda-debuginfo-4.2.4-3.54.2

144556 - SuSE Linux 13.1 openSUSE-SU-2016:1136-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1651, CVE-2016-1652, CVE-2016-1653, CVE-2016-1654, CVE-2016-1655, CVE-2016-1656, CVE-2016-1657, CVE-2016-1658, CVE-2016-1659

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1136-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-04/msg00092.html>

SuSE Linux 13.1

x86_64
chromium-50.0.2661.75-144.1
chromium-debugsource-50.0.2661.75-144.1
chromium-ffmpegsumo-50.0.2661.75-144.1
chromium-desktop-kde-50.0.2661.75-144.1
chromedriver-50.0.2661.75-144.1
chromium-debuginfo-50.0.2661.75-144.1
chromium-desktop-gnome-50.0.2661.75-144.1
chromedriver-debuginfo-50.0.2661.75-144.1
chromium-ffmpegsumo-debuginfo-50.0.2661.75-144.1

i586
chromium-50.0.2661.75-144.1
chromium-debugsource-50.0.2661.75-144.1
chromium-ffmpegsumo-50.0.2661.75-144.1
chromium-desktop-kde-50.0.2661.75-144.1
chromedriver-50.0.2661.75-144.1
chromium-debuginfo-50.0.2661.75-144.1
chromium-desktop-gnome-50.0.2661.75-144.1
chromedriver-debuginfo-50.0.2661.75-144.1
chromium-ffmpegsumo-debuginfo-50.0.2661.75-144.1

181927 - FreeBSD proftpd Vulnerability In Mod_tls (a733b5ca-06eb-11e6-817f-3085a9a4510d)

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

Risk Level: High

CVE: CVE-2016-3125

Description

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

proftpd -- vulnerability in mod_tls (a733b5ca-06eb-11e6-817f-3085a9a4510d)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/a733b5ca-06eb-11e6-817f-3085a9a4510d.html>

Affected packages:

proftpd < 1.3.5b

proftpd == 1.3.6.r1

185243 - Ubuntu Linux 12.04, 14.04, 15.10 USN-2953-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0639, CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0655, CVE-2016-0661, CVE-2016-0665, CVE-2016-0666, CVE-2016-0668, CVE-2016-2047

Description

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

USN-2953-1

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-April/003386.html>

Ubuntu 12.04

mysql-server-5.5_5.5.49-0ubuntu0.12.04.1

Ubuntu 15.10

mysql-server-5.6_5.6.30-0ubuntu0.15.10.1

Ubuntu 14.04

mysql-server-5.5_5.5.49-0ubuntu0.14.04.1

185244 - Ubuntu Linux 16.04 USN-2954-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0639, CVE-2016-0642, CVE-2016-0643, CVE-2016-0647, CVE-2016-0648, CVE-2016-0655, CVE-2016-0657, CVE-2016-0659, CVE-2016-0662, CVE-2016-0666, CVE-2016-0667, CVE-2016-2047

Description

The scan detected that the host is missing the following update:
USN-2954-1

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-April/003387.html>

Ubuntu 16.04

mysql-server-5.7_5.7.12-0ubuntu1

185245 - Ubuntu Linux 12.04, 14.04, 15.10 USN-2952-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9767, CVE-2015-8835, CVE-2015-8838, CVE-2016-1903, CVE-2016-2554, CVE-2016-3141, CVE-2016-3142, CVE-2016-3185

Description

The scan detected that the host is missing the following update:
USN-2952-1

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-April/003385.html>

Ubuntu 12.04

php5-snmp_5.3.10-1ubuntu3.22
php5-fpm_5.3.10-1ubuntu3.22
php5-cgi_5.3.10-1ubuntu3.22
libapache2-mod-php5_5.3.10-1ubuntu3.22
php5-gd_5.3.10-1ubuntu3.22
php5-mysqlnd_5.3.10-1ubuntu3.22
php5-cli_5.3.10-1ubuntu3.22

Ubuntu 15.10

php5-fpm_5.6.11+dfsg-1ubuntu3.2
php5-mysqlnd_5.6.11+dfsg-1ubuntu3.2
php5-gd_5.6.11+dfsg-1ubuntu3.2
php5-snmp_5.6.11+dfsg-1ubuntu3.2
php5-cli_5.6.11+dfsg-1ubuntu3.2
libapache2-mod-php5_5.6.11+dfsg-1ubuntu3.2
php5-cgi_5.6.11+dfsg-1ubuntu3.2

Ubuntu 14.04

libapache2-mod-php5_5.5.9+dfsg-1ubuntu4.16
php5-fpm_5.5.9+dfsg-1ubuntu4.16
php5-mysqlnd_5.5.9+dfsg-1ubuntu4.16
php5-gd_5.5.9+dfsg-1ubuntu4.16
php5-cli_5.5.9+dfsg-1ubuntu4.16
php5-cgi_5.5.9+dfsg-1ubuntu4.16
php5-snmp_5.5.9+dfsg-1ubuntu4.16

190557 - Fedora Linux 24 FEDORA-2016-8f164810c3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2315, CVE-2016-2324

Description

The scan detected that the host is missing the following update:
FEDORA-2016-8f164810c3

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183147.html>

Fedora Core 24

git-2.7.4-1.fc24

19953 - (APSB16-11) Vulnerability In Creative Cloud Desktop Application

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

Risk Level: High

CVE: CVE-2016-1034

Description

A vulnerability is present in some versions of Adobe Creative Cloud Desktop Application.

Observation

Adobe Creative Cloud Desktop Application is the desktop client used to access Adobe Creative Cloud.

A vulnerability is present in some versions of Adobe Creative Cloud Desktop Application. The flaw lies in JavaScript API for Creative Cloud Libraries. Successful exploitation could allow an attacker to read or write files on client's file system.

The update provided by Adobe bulletin APSB16-11 resolves this issue. The target system appears to be missing this update.

141161 - Red Hat Enterprise Linux RHSA-2016-0679 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3422, CVE-2016-3425, CVE-2016-3427, CVE-2016-3443, CVE-2016-3449

Description

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

RHSA-2016-0679

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0679.html>

RHEL7D

x86_64

java-1.6.0-sun-jdbc-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-src-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-devel-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-plugin-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-demo-1.6.0.115-1jpp.1.el7

RHEL7S

x86_64

java-1.6.0-sun-jdbc-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-src-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-devel-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-plugin-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-demo-1.6.0.115-1jpp.1.el7

RHEL7WS

x86_64

java-1.6.0-sun-jdbc-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-src-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-devel-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-plugin-1.6.0.115-1jpp.1.el7

java-1.6.0-sun-demo-1.6.0.115-1jpp.1.el7

141162 - Red Hat Enterprise Linux RHSA-2016-0677 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3422, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427, CVE-2016-3443, CVE-2016-3449

Description

The scan detected that the host is missing the following update:
RHSA-2016-0677

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-0677.html>

RHEL7D

x86_64

java-1.8.0-oracle-jdbc-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-devel-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-src-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-javafx-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-plugin-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-1.8.0.91-1jpp.1.el7

RHEL7S

x86_64

java-1.8.0-oracle-jdbc-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-devel-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-src-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-javafx-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-plugin-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-1.8.0.91-1jpp.1.el7

RHEL7WS

x86_64

java-1.8.0-oracle-jdbc-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-devel-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-src-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-javafx-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-plugin-1.8.0.91-1jpp.1.el7
java-1.8.0-oracle-1.8.0.91-1jpp.1.el7

141163 - Red Hat Enterprise Linux RHSA-2016-0651 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
RHSA-2016-0651

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-0651.html>

java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

RHEL6WS

x86_64

java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

i386

java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

141164 - Red Hat Enterprise Linux RHSA-2016-0675 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

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

RHSA-2016-0675

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0675.html>

RHEL6D

i386

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el6_7

noarch

java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el6_7

x86_64

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el6_7

RHEL6S

i386

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el6_7

noarch

java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el6_7

x86_64

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el6_7

RHEL6WS

x86_64

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el6_7

i386

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el6_7

141166 - Red Hat Enterprise Linux RHSA-2016-0695 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2805, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

Description

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

RHSA-2016-0695

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0695.html>

RHEL5S

i386

firefox-debuginfo-45.1.0-1.el5_11

firefox-45.1.0-1.el5_11

x86_64

firefox-debuginfo-45.1.0-1.el5_11

firefox-45.1.0-1.el5_11

RHEL7S

x86_64

firefox-debuginfo-45.1.0-1.el7_2

firefox-45.1.0-1.el7_2

RHEL6S

i386

firefox-45.1.0-1.el6_7

firefox-debuginfo-45.1.0-1.el6_7

x86_64

firefox-45.1.0-1.el6_7

firefox-debuginfo-45.1.0-1.el6_7

RHEL6WS
x86_64
firefox-45.1.0-1.el6_7
firefox-debuginfo-45.1.0-1.el6_7

i386
firefox-45.1.0-1.el6_7
firefox-debuginfo-45.1.0-1.el6_7

RHEL5D
x86_64
firefox-debuginfo-45.1.0-1.el5_11
firefox-45.1.0-1.el5_11

i386
firefox-debuginfo-45.1.0-1.el5_11
firefox-45.1.0-1.el5_11

RHEL7D
x86_64
firefox-debuginfo-45.1.0-1.el7_2
firefox-45.1.0-1.el7_2

RHEL6D
x86_64
firefox-45.1.0-1.el6_7
firefox-debuginfo-45.1.0-1.el6_7

i386
firefox-45.1.0-1.el6_7
firefox-debuginfo-45.1.0-1.el6_7

RHEL7WS
x86_64
firefox-debuginfo-45.1.0-1.el7_2
firefox-45.1.0-1.el7_2

141167 - Red Hat Enterprise Linux RHSA-2016-0676 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

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

RHSA-2016-0676

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0676.html>

RHEL5S
x86_64
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el5_11

java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el5_11

i386

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el5_11

RHEL7D

x86_64

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-accessibility-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-headless-1.7.0.101-2.6.6.1.el7_2

noarch

java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el7_2

RHEL7S

noarch

java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el7_2

RHEL7WS

x86_64

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-headless-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-accessibility-1.7.0.101-2.6.6.1.el7_2

noarch

java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el7_2

RHEL5D

x86_64

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el5_11

i386

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el5_11

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3422, CVE-2016-3425, CVE-2016-3427, CVE-2016-3443, CVE-2016-3449

Description

The scan detected that the host is missing the following update:
RHSA-2016-0678

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-0678.html>

RHEL7D

x86_64

java-1.7.0-oracle-javafx-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-jdbc-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-devel-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-src-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-plugin-1.7.0.101-1jpp.1.el7

RHEL7S

x86_64

java-1.7.0-oracle-javafx-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-jdbc-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-devel-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-src-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-plugin-1.7.0.101-1jpp.1.el7

RHEL7WS

x86_64

java-1.7.0-oracle-javafx-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-jdbc-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-devel-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-src-1.7.0.101-1jpp.1.el7
java-1.7.0-oracle-plugin-1.7.0.101-1jpp.1.el7

141169 - Red Hat Enterprise Linux RHSA-2016-0650 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
RHSA-2016-0650

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-0650.html>

RHEL7D

x86_64

java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-1.8.0.91-0.b14.el7_2

noarch

java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el7_2

RHEL7S

noarch

java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el7_2

RHEL7WS

x86_64

java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el7_2

noarch

java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el7_2

160087 - CentOS 7 CESA-2016-0650 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

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

CESA-2016-0650

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-April/021839.html>

CentOS 7

x86_64

java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el7_2

noarch

java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el7_2

160090 - CentOS 5, 7 CESA-2016-0676 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
CESA-2016-0676

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-April/021841.html>

<http://lists.centos.org/pipermail/centos-announce/2016-April/021840.html>

CentOS 5

x86_64

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el5_11

i386

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el5_11

CentOS 7

x86_64

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el7_2

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-accessibility-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-headless-1.7.0.101-2.6.6.1.el7_2

noarch
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el7_2

160091 - CentOS 6 CESA-2016-0675 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
CESA-2016-0675

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-April/021837.html>

CentOS 6

i686
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el6_7
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el6_7

noarch
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el6_7

x86_64
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el6_7
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el6_7

160092 - CentOS 6 CESA-2016-0651 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
CESA-2016-0651

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-April/021838.html>

CentOS 6

i686

java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

noarch

java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el6_7

x86_64

java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

160093 - CentOS 7 CESA-2016-0695 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2805, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

Description

The scan detected that the host is missing the following update:
CESA-2016-0695

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-April/021852.html>

CentOS 7

x86_64

firefox-45.1.0-1.el7.centos

i686

firefox-45.1.0-1.el7.centos

163064 - Oracle Enterprise Linux ELSA-2016-0650 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
ELSA-2016-0650

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-April/005954.html>

OEL7

x86_64

java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-1.8.0.91-0.b14.el7_2

163065 - Oracle Enterprise Linux ELSA-2016-0676 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
ELSA-2016-0676

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-April/005956.html>

<http://oss.oracle.com/pipermail/el-errata/2016-April/005958.html>

OEL7

x86_64

java-1.7.0-openjdk-headless-1.7.0.101-2.6.6.1.0.1.el7_2
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.0.1.el7_2
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.0.1.el7_2
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.0.1.el7_2
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.0.1.el7_2
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.0.1.el7_2
java-1.7.0-openjdk-accessibility-1.7.0.101-2.6.6.1.0.1.el7_2

OEL5

x86_64
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.0.1.el5_11
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.0.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.0.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.0.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.0.1.el5_11

i386
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.0.1.el5_11
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.0.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.0.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.0.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.0.1.el5_11

163066 - Oracle Enterprise Linux ELSA-2016-0675 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
ELSA-2016-0675

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-April/005957.html>

OEL6
x86_64
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.0.1.el6_7
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.0.1.el6_7
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.0.1.el6_7
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.0.1.el6_7
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.0.1.el6_7

i386
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.0.1.el6_7
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.0.1.el6_7
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.0.1.el6_7
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.0.1.el6_7
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.0.1.el6_7

163067 - Oracle Enterprise Linux ELSA-2016-0651 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
ELSA-2016-0651

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-April/005955.html>

OEL6

x86_64

java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

i386

java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

170667 - Amazon Linux AMI ALAS-2016-688 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

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

ALAS-2016-688

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2016-688.html>

Amazon Linux AMI

i686

java-1.8.0-openjdk-devel-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-src-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-headless-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.10.amzn1

noarch
java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.10.amzn1

x86_64
java-1.8.0-openjdk-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-src-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-headless-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.10.amzn1
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.10.amzn1

174944 - Scientific Linux Security ERRATA Critical: java-1.8.0-openjdk on SL7.x x86_64 (1604-12913)

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: java-1.8.0-openjdk on SL7.x x86_64 (1604-12913)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=12913>

SL7
x86_64
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-accessibility-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-1.8.0.91-0.b14.el7_2

noarch
java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el7_2
java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el7_2

174945 - Scientific Linux Security ERRATA Critical: java-1.7.0-openjdk on SL6.x i386/x86_64 (1604-13773)

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: java-1.7.0-openjdk on SL6.x i386/x86_64 (1604-13773)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=13773>

SL6

i386

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el6_7

noarch

java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el6_7

x86_64

java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el6_7

java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el6_7

174946 - Scientific Linux Security ERRATA Critical: java-1.8.0-openjdk on SL6.x i386/x86_64 (1604-12476)

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

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

Security ERRATA Critical: java-1.8.0-openjdk on SL6.x i386/x86_64 (1604-12476)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=12476>

SL6

i386

java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-src-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

noarch

java-1.8.0-openjdk-javadoc-debug-1.8.0.91-0.b14.el6_7

java-1.8.0-openjdk-javadoc-1.8.0.91-0.b14.el6_7

x86_64
java-1.8.0-openjdk-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-headless-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-debuginfo-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-src-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-demo-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-headless-debug-1.8.0.91-0.b14.el6_7
java-1.8.0-openjdk-devel-1.8.0.91-0.b14.el6_7

174947 - Scientific Linux Security ERRATA Critical: java-1.7.0-openjdk on SL5.x, SL7.x i386/x86_64 (1604-13345)

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

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

Security ERRATA Critical: java-1.7.0-openjdk on SL5.x, SL7.x i386/x86_64 (1604-13345)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=13345>

SL7

x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-accessibility-1.7.0.101-2.6.6.1.el7_2
java-1.7.0-openjdk-headless-1.7.0.101-2.6.6.1.el7_2

noarch

java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el7_2

SL5

x86_64
java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-src-1.7.0.101-2.6.6.1.el5_11

i386

java-1.7.0-openjdk-demo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.101-2.6.6.1.el5_11
java-1.7.0-openjdk-1.7.0.101-2.6.6.1.el5_11

174949 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1604-15448)

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

Risk Level: High

CVE: CVE-2016-2805, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

Description

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

Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1604-15448)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=15448>

SL5

x86_64

firefox-debuginfo-45.1.0-1.el5_11

firefox-45.1.0-1.el5_11

i386

firefox-debuginfo-45.1.0-1.el5_11

firefox-45.1.0-1.el5_11

SL7

x86_64

firefox-debuginfo-45.1.0-1.el7_2

firefox-45.1.0-1.el7_2

SL6

x86_64

firefox-45.1.0-1.el6_7

firefox-debuginfo-45.1.0-1.el6_7

i386

firefox-45.1.0-1.el6_7

firefox-debuginfo-45.1.0-1.el6_7

19946 - Pro-face GP-Pro EX HMI Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-7921, CVE-2016-2290, CVE-2016-2291, CVE-2016-2292

Description

Multiple vulnerabilities are present in some versions of Pro-face GP-Pro EX.

Observation

Pro-face GP-Pro EX is the development software for Pro-face HMI units.

Multiple vulnerabilities are present in some versions of Pro-face GP-Pro EX. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, to bypass security access restrictions or to remotely execute

arbitrary code.

19966 - (HT205771) Apple QuickTime Multiple Remote Code Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Apple QuickTime.

Observation

Apple QuickTime is a media player.

Multiple vulnerabilities are present in some versions of Apple QuickTime. The flaws are related with the Atom processing component. Successful exploitation could allow an attacker to remotely execute arbitrary code.

130473 - Debian Linux 8.0 DSA-3554-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3158, CVE-2016-3159, CVE-2016-3960

Description

The scan detected that the host is missing the following update:
DSA-3554-1

Observation

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

<http://www.debian.org/security/2016/dsa-3554>

Debian 8.0

all

xen-system-arm64_4.4.1-9+deb8u5

xen-utils-common_4.4.1-9+deb8u5

xen-system-amd64_4.4.1-9+deb8u5

libxen-dev_4.4.1-9+deb8u5

xen-hypervisor-4.4-armhf_4.4.1-9+deb8u5

xen-hypervisor-4.4-amd64_4.4.1-9+deb8u5

xen-utils-4.4_4.4.1-9+deb8u5

xenstore-utils_4.4.1-9+deb8u5

libxenstore3.0_4.4.1-9+deb8u5

xen-hypervisor-4.4-arm64_4.4.1-9+deb8u5

xen-system-armhf_4.4.1-9+deb8u5

libxen-4.4_4.4.1-9+deb8u5

144550 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1140-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3977

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1140-1

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-April/002025.html>

SuSE SLED 12 SP1

x86_64
giflib-debugsource-5.0.5-12.1
libgif6-debuginfo-32bit-5.0.5-12.1
libgif6-32bit-5.0.5-12.1
libgif6-debuginfo-5.0.5-12.1
libgif6-5.0.5-12.1

SuSE SLED 12

x86_64
giflib-debugsource-5.0.5-12.1
libgif6-debuginfo-32bit-5.0.5-12.1
libgif6-32bit-5.0.5-12.1
libgif6-debuginfo-5.0.5-12.1
libgif6-5.0.5-12.1

SuSE SLES 12 SP1

x86_64
giflib-progs-5.0.5-12.1
libgif6-debuginfo-5.0.5-12.1
libgif6-5.0.5-12.1
giflib-debugsource-5.0.5-12.1
libgif6-32bit-5.0.5-12.1
giflib-progs-debuginfo-5.0.5-12.1
libgif6-debuginfo-32bit-5.0.5-12.1

SuSE SLES 12

x86_64
giflib-progs-5.0.5-12.1
libgif6-debuginfo-5.0.5-12.1
libgif6-5.0.5-12.1
giflib-debugsource-5.0.5-12.1
libgif6-32bit-5.0.5-12.1
giflib-progs-debuginfo-5.0.5-12.1
libgif6-debuginfo-32bit-5.0.5-12.1

144552 - SuSE Linux 13.2 openSUSE-SU-2016:1111-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3977

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1111-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-04/msg00079.html>

SuSE Linux 13.2

x86_64

libgif6-debuginfo-5.0.5-4.6.1

giflib-devel-5.0.5-4.6.1

libgif6-5.0.5-4.6.1

giflib-devel-32bit-5.0.5-4.6.1

giflib-progs-5.0.5-4.6.1

giflib-progs-debuginfo-5.0.5-4.6.1

libgif6-debuginfo-5.0.5-4.6.1

libgif6-32bit-5.0.5-4.6.1

giflib-debugsource-5.0.5-4.6.1

i586

giflib-devel-5.0.5-4.6.1

libgif6-5.0.5-4.6.1

giflib-progs-5.0.5-4.6.1

giflib-progs-debuginfo-5.0.5-4.6.1

libgif6-debuginfo-5.0.5-4.6.1

giflib-debugsource-5.0.5-4.6.1

144555 - SuSE Linux 13.1 openSUSE-SU-2016:1108-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1108-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-04/msg00078.html>

SuSE Linux 13.1

i586

perl-apparmor-debuginfo-2.8.4-4.20.1

pam_apparmor-debuginfo-2.8.4-4.20.1

perl-apparmor-2.8.4-4.20.1

libapparmor1-debuginfo-2.8.4-4.20.1

pam_apparmor-2.8.4-4.20.1

python3-apparmor-2.8.4-4.20.1

ruby-apparmor-2.8.4-4.20.1

libapparmor1-2.8.4-4.20.1

apparmor-debugsource-2.8.4-4.20.1

python3-apparmor-debuginfo-2.8.4-4.20.1

ruby-apparmor-debuginfo-2.8.4-4.20.1

apache2-mod_apparmor-2.8.4-4.20.1

libapparmor-devel-2.8.4-4.20.1

apparmor-parser-2.8.4-4.20.1

apparmor-parser-debuginfo-2.8.4-4.20.1

apache2-mod_apparmor-debuginfo-2.8.4-4.20.1

noarch

apparmor-docs-2.8.4-4.20.1

apparmor-utils-lang-2.8.4-4.20.1

apparmor-profiles-2.8.4-4.20.1

apparmor-utils-2.8.4-4.20.1

apparmor-parser-lang-2.8.4-4.20.1

x86_64

pam_apparmor-32bit-2.8.4-4.20.1

libapparmor1-debuginfo-32bit-2.8.4-4.20.1

perl-apparmor-debuginfo-2.8.4-4.20.1

pam_apparmor-debuginfo-2.8.4-4.20.1

perl-apparmor-2.8.4-4.20.1

libapparmor1-debuginfo-2.8.4-4.20.1

pam_apparmor-2.8.4-4.20.1

python3-apparmor-2.8.4-4.20.1

pam_apparmor-debuginfo-32bit-2.8.4-4.20.1

ruby-apparmor-2.8.4-4.20.1

libapparmor1-2.8.4-4.20.1

libapparmor1-32bit-2.8.4-4.20.1

apparmor-debugsource-2.8.4-4.20.1

python3-apparmor-debuginfo-2.8.4-4.20.1

ruby-apparmor-debuginfo-2.8.4-4.20.1

apache2-mod_apparmor-2.8.4-4.20.1

libapparmor-devel-2.8.4-4.20.1

apparmor-parser-2.8.4-4.20.1

apparmor-parser-debuginfo-2.8.4-4.20.1

apache2-mod_apparmor-debuginfo-2.8.4-4.20.1

144557 - SuSE SLES 11 SP4 SUSE-SU-2016:1139-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3977

Description

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

SUSE-SU-2016:1139-1

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-April/002024.html>

SuSE SLES 11 SP4

i586

giflib-4.1.6-21.1

giflib-progs-4.1.6-21.1

x86_64

giflib-32bit-4.1.6-21.1

giflib-4.1.6-21.1

giflib-progs-4.1.6-21.1

144558 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1138-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1601

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1138-1

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-April/002023.html>

SuSE SLES 12 SP1

x86_64

yast2-users-debugsource-3.1.41.3-9.1

yast2-users-debuginfo-3.1.41.3-9.1

yast2-users-3.1.41.3-9.1

SuSE SLED 12 SP1

x86_64

yast2-users-debugsource-3.1.41.3-9.1

yast2-users-debuginfo-3.1.41.3-9.1

yast2-users-3.1.41.3-9.1

144559 - SuSE Linux 13.1 openSUSE-SU-2016:1118-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3977

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1118-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-04/msg00084.html>

SuSE Linux 13.1

x86_64

giflib-progs-5.0.5-2.9.1

giflib-devel-32bit-5.0.5-2.9.1

libgif6-5.0.5-2.9.1

giflib-debugsource-5.0.5-2.9.1

giflib-devel-5.0.5-2.9.1

libgif6-32bit-5.0.5-2.9.1

giflib-progs-debuginfo-5.0.5-2.9.1

libgif6-debuginfo-32bit-5.0.5-2.9.1

libgif6-debuginfo-5.0.5-2.9.1

i586
giflib-progs-5.0.5-2.9.1
libgif6-5.0.5-2.9.1
giflib-debugsource-5.0.5-2.9.1
giflib-devel-5.0.5-2.9.1
giflib-progs-debuginfo-5.0.5-2.9.1
libgif6-debuginfo-5.0.5-2.9.1

170665 - Amazon Linux AMI ALAS-2016-690 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-5325, CVE-2015-8560

Description

The scan detected that the host is missing the following update:
ALAS-2016-690

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-690.html>

Amazon Linux AMI
x86_64
foomatic-debuginfo-4.0.4-5.11.amzn1
foomatic-4.0.4-5.11.amzn1

i686
foomatic-4.0.4-5.11.amzn1
foomatic-debuginfo-4.0.4-5.11.amzn1

178174 - Gentoo Linux GLSA-201604-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8711, CVE-2015-8712, CVE-2015-8713, CVE-2015-8714, CVE-2015-8715, CVE-2015-8716, CVE-2015-8717, CVE-2015-8718, CVE-2015-8719, CVE-2015-8720, CVE-2015-8721, CVE-2015-8722, CVE-2015-8723, CVE-2015-8724, CVE-2015-8725, CVE-2015-8726, CVE-2015-8727, CVE-2015-8728, CVE-2015-8729, CVE-2015-8730, CVE-2015-8731, CVE-2015-8732, CVE-2015-8733, CVE-2015-8734, CVE-2015-8735, CVE-2015-8736, CVE-2015-8737, CVE-2015-8738, CVE-2015-8739, CVE-2015-8740, CVE-2015-8741, CVE-2015-8742, CVE-2016-2521, CVE-2016-2522, CVE-2016-2523, CVE-2016-2524, CVE-2016-2525, CVE-2016-2526, CVE-2016-2527, CVE-2016-2528, CVE-2016-2529, CVE-2016-2530, CVE-2016-2531, CVE-2016-2532

Description

The scan detected that the host is missing the following update:
GLSA-201604-05

Observation

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

<https://security.gentoo.org/glsa/201604-05>

Affected packages:
net-analyzer/wireshark < 2.0.2

19975 - Oracle Berkeley DB DataStore Critical Patch Update April 2016

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

Risk Level: Medium

CVE: CVE-2016-0682, CVE-2016-0689, CVE-2016-0692, CVE-2016-0694, CVE-2016-3418

Description

Multiple vulnerabilities are present in some versions of Oracle Berkeley DB.

Observation

Berkeley DB is a family of open source, embedded key-value database.

Multiple vulnerabilities are present in some versions of Oracle Berkeley DB. The flaws are caused due to unspecified errors in the DataStore component. Successful exploitation could allow local attackers to affect confidentiality, integrity, and availability.

37520 - IBM AIX IV81278 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8704

Description

The scan detected that the host is missing the following update:
IV81278

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=swg1IV81278>

5300-12

bos.net.tcp.client < 5.3.12.11

37521 - IBM AIX IV81279 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8704

Description

The scan detected that the host is missing the following update:
IV81279

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=swg1IV81279>

6100-09

bos.net.tcp.client < 6.1.9.102

37522 - IBM AIX IV81280 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8704

Description

The scan detected that the host is missing the following update:
IV81280

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=swg1IV81280>

7100-03

bos.net.tcp.client < 7.1.3.47

37523 - IBM AIX IV81281 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8704

Description

The scan detected that the host is missing the following update:
IV81281

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=swg1IV81281>

7100-04

bos.net.tcp.client < 7.1.4.1

37524 - IBM AIX IV81282 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8704

Description

The scan detected that the host is missing the following update:
IV81282

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=swg1IV81282>

7200-00
bos.net.tcp.client < 7.2.0.1

141165 - Red Hat Enterprise Linux RHSA-2016-0685 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1978, CVE-2016-1979

Description

The scan detected that the host is missing the following update:
RHSA-2016-0685

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-0685.html>

RHEL7D

x86_64
nss-tools-3.21.0-9.el7_2
nss-softokn-3.16.2.3-14.2.el7_2
nss-devel-3.21.0-9.el7_2
nss-3.21.0-9.el7_2
nss-debuginfo-3.21.0-9.el7_2
nspr-devel-4.11.0-1.el7_2
nss-softokn-debuginfo-3.16.2.3-14.2.el7_2
nspr-4.11.0-1.el7_2
nss-util-debuginfo-3.21.0-2.2.el7_2
nspr-debuginfo-4.11.0-1.el7_2
nss-util-devel-3.21.0-2.2.el7_2
nss-softokn-freebl-devel-3.16.2.3-14.2.el7_2
nss-softokn-devel-3.16.2.3-14.2.el7_2
nss-pkcs11-devel-3.21.0-9.el7_2
nss-util-3.21.0-2.2.el7_2
nss-sysinit-3.21.0-9.el7_2
nss-softokn-freebl-3.16.2.3-14.2.el7_2

RHEL7S

ppc64
nss-tools-3.21.0-9.el7_2
nss-softokn-3.16.2.3-14.2.el7_2
nss-devel-3.21.0-9.el7_2
nss-3.21.0-9.el7_2
nss-debuginfo-3.21.0-9.el7_2
nspr-devel-4.11.0-1.el7_2
nss-softokn-debuginfo-3.16.2.3-14.2.el7_2
nspr-4.11.0-1.el7_2
nss-util-debuginfo-3.21.0-2.2.el7_2
nspr-debuginfo-4.11.0-1.el7_2
nss-util-devel-3.21.0-2.2.el7_2
nss-softokn-freebl-devel-3.16.2.3-14.2.el7_2
nss-softokn-devel-3.16.2.3-14.2.el7_2
nss-pkcs11-devel-3.21.0-9.el7_2
nss-util-3.21.0-2.2.el7_2
nss-sysinit-3.21.0-9.el7_2

nss-softokn-freebl-3.16.2.3-14.2.el7_2

RHEL7WS

x86_64

nss-tools-3.21.0-9.el7_2

nss-softokn-3.16.2.3-14.2.el7_2

nss-devel-3.21.0-9.el7_2

nss-3.21.0-9.el7_2

nss-debuginfo-3.21.0-9.el7_2

nspr-devel-4.11.0-1.el7_2

nss-softokn-debuginfo-3.16.2.3-14.2.el7_2

nspr-4.11.0-1.el7_2

nss-util-debuginfo-3.21.0-2.2.el7_2

nspr-debuginfo-4.11.0-1.el7_2

nss-util-devel-3.21.0-2.2.el7_2

nss-softokn-freebl-devel-3.16.2.3-14.2.el7_2

nss-softokn-devel-3.16.2.3-14.2.el7_2

nss-pkcs11-devel-3.21.0-9.el7_2

nss-util-3.21.0-2.2.el7_2

nss-sysinit-3.21.0-9.el7_2

nss-softokn-freebl-3.16.2.3-14.2.el7_2

141170 - Red Hat Enterprise Linux RHSA-2016-0684 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1978, CVE-2016-1979

Description

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

RHSA-2016-0684

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-0684.html>

RHEL5D

x86_64

nss-tools-3.21.0-6.el5_11

nss-3.21.0-6.el5_11

nspr-4.11.0-1.el5_11

nss-debuginfo-3.21.0-6.el5_11

nspr-debuginfo-4.11.0-1.el5_11

i386

nss-tools-3.21.0-6.el5_11

nss-3.21.0-6.el5_11

nspr-4.11.0-1.el5_11

nss-debuginfo-3.21.0-6.el5_11

nspr-debuginfo-4.11.0-1.el5_11

RHEL5S

i386

nss-debuginfo-3.21.0-6.el5_11

nspr-devel-4.11.0-1.el5_11

nss-tools-3.21.0-6.el5_11

nspr-debuginfo-4.11.0-1.el5_11
nss-devel-3.21.0-6.el5_11
nss-3.21.0-6.el5_11
nss-pkcs11-devel-3.21.0-6.el5_11
nspr-4.11.0-1.el5_11

x86_64
nss-debuginfo-3.21.0-6.el5_11
nspr-devel-4.11.0-1.el5_11
nss-tools-3.21.0-6.el5_11
nspr-debuginfo-4.11.0-1.el5_11
nss-devel-3.21.0-6.el5_11
nss-3.21.0-6.el5_11
nss-pkcs11-devel-3.21.0-6.el5_11
nspr-4.11.0-1.el5_11

160088 - CentOS 7 CESA-2016-0685 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1978, CVE-2016-1979

Description

The scan detected that the host is missing the following update:
CESA-2016-0685

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-April/021851.html>
<http://lists.centos.org/pipermail/centos-announce/2016-April/021849.html>
<http://lists.centos.org/pipermail/centos-announce/2016-April/021850.html>
<http://lists.centos.org/pipermail/centos-announce/2016-April/021848.html>

CentOS 7

x86_64
nss-tools-3.21.0-9.el7_2
nss-softokn-3.16.2.3-14.2.el7_2
nss-devel-3.21.0-9.el7_2
nss-3.21.0-9.el7_2
nspr-4.11.0-1.el7_2
nss-softokn-freebl-devel-3.16.2.3-14.2.el7_2
nspr-devel-4.11.0-1.el7_2
nss-pkcs11-devel-3.21.0-9.el7_2
nss-util-devel-3.21.0-2.2.el7_2
nss-softokn-devel-3.16.2.3-14.2.el7_2
nss-util-3.21.0-2.2.el7_2
nss-sysinit-3.21.0-9.el7_2
nss-softokn-freebl-3.16.2.3-14.2.el7_2

i686

nss-util-3.21.0-2.2.el7_2
nss-3.21.0-9.el7_2
nspr-4.11.0-1.el7_2
nss-pkcs11-devel-3.21.0-9.el7_2
nss-devel-3.21.0-9.el7_2
nss-util-devel-3.21.0-2.2.el7_2

nspr-devel-4.11.0-1.el7_2
nss-softokn-3.16.2.3-14.2.el7_2
nss-softokn-freebl-devel-3.16.2.3-14.2.el7_2
nss-softokn-devel-3.16.2.3-14.2.el7_2
nss-softokn-freebl-3.16.2.3-14.2.el7_2

160089 - CentOS 5 CESA-2016-0684 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1978, CVE-2016-1979

Description

The scan detected that the host is missing the following update:
CESA-2016-0684

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-April/021846.html>

<http://lists.centos.org/pipermail/centos-announce/2016-April/021847.html>

CentOS 5

x86_64

nss-devel-3.21.0-6.el5_11
nss-tools-3.21.0-6.el5_11
nspr-devel-4.11.0-1.el5_11
nss-3.21.0-6.el5_11
nss-pkcs11-devel-3.21.0-6.el5_11
nspr-4.11.0-1.el5_11

i386

nss-devel-3.21.0-6.el5_11
nss-tools-3.21.0-6.el5_11
nspr-devel-4.11.0-1.el5_11
nss-3.21.0-6.el5_11
nss-pkcs11-devel-3.21.0-6.el5_11
nspr-4.11.0-1.el5_11

163063 - Oracle Enterprise Linux ELSA-2016-0684 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1978, CVE-2016-1979

Description

The scan detected that the host is missing the following update:
ELSA-2016-0684

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-April/005963.html>

OEL5
i386
nss-devel-3.21.0-6.el5_11
nss-tools-3.21.0-6.el5_11
nspr-devel-4.11.0-1.el5_11
nss-3.21.0-6.el5_11
nss-pkcs11-devel-3.21.0-6.el5_11
nspr-4.11.0-1.el5_11

x86_64
nss-devel-3.21.0-6.el5_11
nss-tools-3.21.0-6.el5_11
nspr-devel-4.11.0-1.el5_11
nss-3.21.0-6.el5_11
nss-pkcs11-devel-3.21.0-6.el5_11
nspr-4.11.0-1.el5_11

163068 - Oracle Enterprise Linux ELSA-2016-0685 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2730, CVE-2016-1978, CVE-2016-1979

Description

The scan detected that the host is missing the following update:
ELSA-2016-0685

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-April/005964.html>

OEL7
x86_64
nss-softokn-3.16.2.3-14.2.el7_2
nss-sysinit-3.21.0-9.0.1.el7_2
nss-tools-3.21.0-9.0.1.el7_2
nss-softokn-freebl-devel-3.16.2.3-14.2.el7_2
nspr-devel-4.11.0-1.el7_2
nspr-4.11.0-1.el7_2
nss-util-devel-3.21.0-2.2.el7_2
nss-devel-3.21.0-9.0.1.el7_2
nss-softokn-devel-3.16.2.3-14.2.el7_2
nss-pkcs11-devel-3.21.0-9.0.1.el7_2
nss-util-3.21.0-2.2.el7_2
nss-softokn-freebl-3.16.2.3-14.2.el7_2
nss-3.21.0-9.0.1.el7_2

170664 - Amazon Linux AMI ALAS-2016-691 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8629, CVE-2015-8630, CVE-2015-8631

Description

The scan detected that the host is missing the following update:
ALAS-2016-691

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-691.html>

Amazon Linux AMI

x86_64
krb5-libs-1.13.2-12.40.amzn1
krb5-server-ldap-1.13.2-12.40.amzn1
krb5-debuginfo-1.13.2-12.40.amzn1
krb5-pkinit-openssl-1.13.2-12.40.amzn1
krb5-workstation-1.13.2-12.40.amzn1
krb5-server-1.13.2-12.40.amzn1
krb5-devel-1.13.2-12.40.amzn1

i686

krb5-server-ldap-1.13.2-12.40.amzn1
krb5-libs-1.13.2-12.40.amzn1
krb5-devel-1.13.2-12.40.amzn1
krb5-debuginfo-1.13.2-12.40.amzn1
krb5-pkinit-openssl-1.13.2-12.40.amzn1
krb5-workstation-1.13.2-12.40.amzn1
krb5-server-1.13.2-12.40.amzn1

174948 - Scientific Linux Security ERRATA Moderate: nss, nspr, nss-softokn, and nss-util on SL7.x x86_64 (1604-14559)

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

Risk Level: Medium

CVE: CVE-2016-1978, CVE-2016-1979

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: nss, nspr, nss-softokn, and nss-util on SL7.x x86_64 (1604-14559)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=14559>

SL7

x86_64
nss-tools-3.21.0-9.el7_2
nss-softokn-3.16.2.3-14.2.el7_2
nss-devel-3.21.0-9.el7_2
nss-3.21.0-9.el7_2
nss-debuginfo-3.21.0-9.el7_2
nspr-devel-4.11.0-1.el7_2
nss-softokn-debuginfo-3.16.2.3-14.2.el7_2
nspr-4.11.0-1.el7_2
nss-util-debuginfo-3.21.0-2.2.el7_2
nspr-debuginfo-4.11.0-1.el7_2
nss-util-devel-3.21.0-2.2.el7_2

nss-softokn-freebl-devel-3.16.2.3-14.2.el7_2
nss-softokn-devel-3.16.2.3-14.2.el7_2
nss-pkcs11-devel-3.21.0-9.el7_2
nss-util-3.21.0-2.2.el7_2
nss-sysinit-3.21.0-9.el7_2
nss-softokn-freebl-3.16.2.3-14.2.el7_2

174950 - Scientific Linux Security ERRATA Moderate: nss and nspr on SL5.x i386/x86_64 (1604-14194)

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

Risk Level: Medium

CVE: CVE-2016-1978, CVE-2016-1979

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: nss and nspr on SL5.x i386/x86_64 (1604-14194)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=14194>

SL5
x86_64
nss-debuginfo-3.21.0-6.el5_11
nspr-devel-4.11.0-1.el5_11
nss-tools-3.21.0-6.el5_11
nspr-debuginfo-4.11.0-1.el5_11
nss-devel-3.21.0-6.el5_11
nss-3.21.0-6.el5_11
nss-pkcs11-devel-3.21.0-6.el5_11
nspr-4.11.0-1.el5_11

i386
nss-debuginfo-3.21.0-6.el5_11
nspr-devel-4.11.0-1.el5_11
nss-tools-3.21.0-6.el5_11
nspr-debuginfo-4.11.0-1.el5_11
nss-devel-3.21.0-6.el5_11
nss-3.21.0-6.el5_11
nss-pkcs11-devel-3.21.0-6.el5_11
nspr-4.11.0-1.el5_11

190565 - Fedora Linux 24 FEDORA-2016-74f9a65b3a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3068, CVE-2016-3069, CVE-2016-3630

Description

The scan detected that the host is missing the following update:
FEDORA-2016-74f9a65b3a

Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182833.html>

Fedora Core 24

mercurial-3.7.3-1.fc24

19954 - Cisco Catalyst Switches Network Mobility Services Protocol Port Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-1378

Description

An information disclosure vulnerability is present in some versions of the Cisco IOS used in Cisco Catalyst Switches.

Observation

Cisco IOS is an operating system used in Cisco device.

An information disclosure vulnerability is present in some versions of the Cisco IOS used in Cisco Catalyst Switches. The vulnerability is due to a failure to properly secure NMSP with authentication which allows a remote unauthenticated attacker to access Network Mobility Services Protocol (NMSP) port and retrieve version information about the software release running on the device.

19976 - Oracle VM VirtualBox Critical Patch Update April 2016

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

Risk Level: Medium

CVE: CVE-2015-3195, CVE-2015-3197, CVE-2016-0678

Description

Multiple vulnerabilities are present in some versions of Oracle VirtualBox.

Observation

Oracle VirtualBox is a virtualization software.

Multiple vulnerabilities are present in some versions of Oracle VirtualBox. The flaws exist in multiple components including OpenSSL. Successful exploitation by a remote attacker could affect confidentiality, integrity, and availability.

19977 - Wireshark Denial of Service Vulnerability Prior To 1.12.11

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

A denial of service vulnerability is present in some versions of Wireshark.

Observation

Wireshark is a popular network traffic analysis software.

A denial of service vulnerability is present in some versions of Wireshark. The flaw lies in the NCP dissector component. Successful exploitation could allow an attacker to cause a denial of service condition.

19981 - Wireshark Multiple Vulnerabilities Prior To 2.0.3

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

Risk Level: Medium

CVE: CVE-2016-4006, CVE-2016-4076, CVE-2016-4077, CVE-2016-4078, CVE-2016-4079, CVE-2016-4080, CVE-2016-4081, CVE-2016-4082, CVE-2016-4083, CVE-2016-4084

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a popular network traffic analysis software.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause denial of service condition.

144549 - SuSE SLES 11 SP4 SUSE-SU-2016:1149-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9745, CVE-2014-9747

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1149-1

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-April/002028.html>

SuSE SLES 11 SP4
i586
freetype2-2.3.7-25.41.4
ft2demos-2.3.7-25.41.4

x86_64
freetype2-2.3.7-25.41.4
freetype2-32bit-2.3.7-25.41.4
ft2demos-2.3.7-25.41.4

170666 - Amazon Linux AMI ALAS-2016-689 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0773

Description

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

ALAS-2016-689

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-689.html>

Amazon Linux AMI

x86_64

postgresql8-devel-8.4.20-5.52.amzn1
postgresql8-plperl-8.4.20-5.52.amzn1
postgresql8-contrib-8.4.20-5.52.amzn1
postgresql8-8.4.20-5.52.amzn1
postgresql8-debuginfo-8.4.20-5.52.amzn1
postgresql8-pltcl-8.4.20-5.52.amzn1
postgresql8-docs-8.4.20-5.52.amzn1
postgresql8-libs-8.4.20-5.52.amzn1
postgresql8-plpython-8.4.20-5.52.amzn1
postgresql8-server-8.4.20-5.52.amzn1
postgresql8-test-8.4.20-5.52.amzn1

i686

postgresql8-devel-8.4.20-5.52.amzn1
postgresql8-plperl-8.4.20-5.52.amzn1
postgresql8-pltcl-8.4.20-5.52.amzn1
postgresql8-8.4.20-5.52.amzn1
postgresql8-contrib-8.4.20-5.52.amzn1
postgresql8-debuginfo-8.4.20-5.52.amzn1
postgresql8-docs-8.4.20-5.52.amzn1
postgresql8-test-8.4.20-5.52.amzn1
postgresql8-libs-8.4.20-5.52.amzn1
postgresql8-plpython-8.4.20-5.52.amzn1
postgresql8-server-8.4.20-5.52.amzn1

170668 - Amazon Linux AMI ALAS-2016-687 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3959

Description

The scan detected that the host is missing the following update:
ALAS-2016-687

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-687.html>

Amazon Linux AMI

i686

golang-1.5.3-1.21.amzn1
golang-bin-1.5.3-1.21.amzn1

noarch

golang-tests-1.5.3-1.21.amzn1
golang-misc-1.5.3-1.21.amzn1
golang-docs-1.5.3-1.21.amzn1
golang-src-1.5.3-1.21.amzn1

x86_64
golang-1.5.3-1.21.amzn1
golang-bin-1.5.3-1.21.amzn1

178173 - Gentoo Linux GLSA-201604-04 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201604-04

Observation

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

<https://security.gentoo.org/glsa/201604-04>

Affected packages:
dev-libs/libksba < 1.3.3

190553 - Fedora Linux 23 FEDORA-2016-188267b485 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-3115

Description

The scan detected that the host is missing the following update:
FEDORA-2016-188267b485

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183122.html>

Fedora Core 23

gsi-openssh-7.2p2-1.fc23

190561 - Fedora Linux 22 FEDORA-2016-fc1cc33e05 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-3115

Description

The scan detected that the host is missing the following update:
FEDORA-2016-fc1cc33e05

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183101.html>

Fedora Core 22

gsi-openssh-6.9p1-8.fc22

130475 - Debian Linux 8.0 DSA-3557-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0666, CVE-2016-2047

Description

The scan detected that the host is missing the following update:
DSA-3557-1

Observation

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

<http://www.debian.org/security/2016/dsa-3557>

Debian 8.0

all

libmysqld-dev_5.5.49-0+deb8u1

libmysqlclient-dev_5.5.49-0+deb8u1

mysql-common_5.5.49-0+deb8u1

mysql-server_5.5.49-0+deb8u1

libmysqld-pic_5.5.49-0+deb8u1

mysql-server-5.5_5.5.49-0+deb8u1

mysql-source-5.5_5.5.49-0+deb8u1

mysql-client-5.5_5.5.49-0+deb8u1

mysql-testsuite_5.5.49-0+deb8u1

libmysqlclient18_5.5.49-0+deb8u1

mysql-server-core-5.5_5.5.49-0+deb8u1

mysql-client_5.5.49-0+deb8u1

mysql-testsuite-5.5_5.5.49-0+deb8u1

19967 - IBM WebSphere Application Server Information Disclosure Vulnerability (swg21979231)

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

Risk Level: Low

CVE: CVE-2016-0306

Description

A vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a Java application server.

A vulnerability is present in some versions of IBM WebSphere Application Server. The flaws lie in the TLS configuration. Successful exploitation could allow an attacker to obtain sensitive information. Exploitation requires FIPS 140-2 to be enabled.

33342 - Oracle Solaris 152252-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152252-01

Observation

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

<https://getupdates.oracle.com/readme/152252-01>

SunOS 5.10: sudo Patch

SOLARIS_10

SUNWsudo:11.10.0,REV=2013.04.29.14.39

SUNWsdor:11.10.0,REV=2013.04.29.14.39

33343 - Oracle Solaris 152253-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152253-01

Observation

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

<https://getupdates.oracle.com/readme/152253-01>

SunOS 5.10(x86): sudo Patch

SOLARIS_10_x86

SUNWsdor:11.10.0,REV=2013.04.29.10.28

SUNWsudo:11.10.0,REV=2013.04.29.10.28

33344 - Oracle Solaris 152255-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152255-01

Observation

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

<https://getupdates.oracle.com/readme/152255-01>

SunOS 5.10(x86): sudo Source Patch

SOLARIS_10_x86

SUNWsudoS:11.10.0,REV=2013.04.29.10.28

33345 - Oracle Solaris 152254-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152254-01

Observation

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

<https://getupdates.oracle.com/readme/152254-01>

SunOS 5.10: sudo Source Patch

SOLARIS_10

SUNWsudoS:11.10.0,REV=2013.04.29.14.39

130471 - Debian Linux 7.0, 8.0 DSA-3556-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3074

Description

The scan detected that the host is missing the following update:
DSA-3556-1

Observation

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

<http://www.debian.org/security/2016/dsa-3556>

Debian 8.0

all
libgd-tools_2.1.0-5+deb8u1
libgd-dbg_2.1.0-5+deb8u1
libgd2-xpm-dev_2.1.0-5+deb8u1
libgd2-noxpm-dev_2.1.0-5+deb8u1
libgd3_2.1.0-5+deb8u1
libgd-dev_2.1.0-5+deb8u1

Debian 7.0

all
libgd2-xpm-dev_2.0.36~rc1~dfsg-6.1+deb7u2
libgd-tools_2.0.36~rc1~dfsg-6.1+deb7u2
libgd2-noxpm_2.0.36~rc1~dfsg-6.1+deb7u2
libgd2-xpm_2.0.36~rc1~dfsg-6.1+deb7u2
libgd2-noxpm-dev_2.0.36~rc1~dfsg-6.1+deb7u2

130472 - Debian Linux 7.0 DSA-3553-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8852

Description

The scan detected that the host is missing the following update:
DSA-3553-1

Observation

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

<http://www.debian.org/security/2016/dsa-3553>

Debian 7.0

all
varnish_3.0.2-2+deb7u2

130474 - Debian Linux 7.0, 8.0 DSA-3555-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2011-5326, CVE-2014-9771, CVE-2016-3993, CVE-2016-3994, CVE-2016-4024

Description

The scan detected that the host is missing the following update:
DSA-3555-1

Observation

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

For more information see:

<http://www.debian.org/security/2016/dsa-3555>

Debian 8.0

all

libimlib2_1.4.6-2+deb8u2

libimlib2-dev_1.4.6-2+deb8u2

Debian 7.0

all

libimlib2-dev_1.4.5-1+deb7u2

libimlib2_1.4.5-1+deb7u2

181924 - FreeBSD mozilla Multiple Vulnerabilities (92d44f83-a7bf-41cf-91ee-3d1b8ecf579f)

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

Risk Level: Low

CVE: CVE-2016-2804, CVE-2016-2805, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2811, CVE-2016-2812, CVE-2016-2814, CVE-2016-2816, CVE-2016-2817, CVE-2016-2820

Description

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

mozilla -- multiple vulnerabilities (92d44f83-a7bf-41cf-91ee-3d1b8ecf579f)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/92d44f83-a7bf-41cf-91ee-3d1b8ecf579f.html>

Affected packages:

firefox < 46.0,1

linux-firefox < 46.0,1

seamonkey < 2.43

linux-seamonkey < 2.43

39.0,1 <= firefox-esr < 45.1.0,1

firefox-esr < 38.8.0,1

39.0 <= libxul < 45.1.0

39.0 <= thunderbird < 45.1.0

39.0 <= linux-thunderbird < 45.1.0

libxul < 38.8.0

thunderbird < 38.8.0

linux-thunderbird < 38.8.0

181925 - FreeBSD libtasn1 Denial Of Service Parsing Malicious DER Certificates (1b0d2938-0766-11e6-94fa-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-4008

Description

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

libtasn1 -- denial of service parsing malicious DER certificates (1b0d2938-0766-11e6-94fa-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/1b0d2938-0766-11e6-94fa-002590263bf5.html>

Affected packages:
libtasn1 < 4.8

181926 - FreeBSD ansible Use Of Predictable Paths In Lxc_container (253c6889-06f0-11e6-925f-6805ca0b3d42)

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

Risk Level: Low

CVE: CVE-2016-3096

Description

The scan detected that the host is missing the following update:
ansible -- use of predictable paths in lxc_container (253c6889-06f0-11e6-925f-6805ca0b3d42)

Observation

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

<http://www.vuxml.org/freebsd/253c6889-06f0-11e6-925f-6805ca0b3d42.html>

Affected packages:
2.0.0.0 <= ansible < 2.0.2.0
ansible1 < 1.9.6

181928 - FreeBSD squid Multiple Vulnerabilities (e05bfc92-0763-11e6-94fa-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054

Description

The scan detected that the host is missing the following update:
squid -- multiple vulnerabilities (e05bfc92-0763-11e6-94fa-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/e05bfc92-0763-11e6-94fa-002590263bf5.html>

Affected packages:
squid < 3.5.17

181929 - FreeBSD phpmyfaq Cross-site Request Forgery Vulnerability (f87a9376-0943-11e6-8fc4-00a0986f28c4)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
phpmyfaq -- cross-site request forgery vulnerability (f87a9376-0943-11e6-8fc4-00a0986f28c4)

Observation

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

<http://www.vuxml.org/freebsd/f87a9376-0943-11e6-8fc4-00a0986f28c4.html>

Affected packages:
phpmyfaq < 2.8.27

190537 - Fedora Linux 22 FEDORA-2016-ac1dff014c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-ac1dff014c

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183100.html>

Fedora Core 22

webkitgtk4-2.12.1-1.fc22

190538 - Fedora Linux 22 FEDORA-2016-59c5e405e3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3959

Description

The scan detected that the host is missing the following update:
FEDORA-2016-59c5e405e3

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183106.html>

Fedora Core 22

golang-1.5.4-1.fc22

190539 - Fedora Linux 22 FEDORA-2016-3c4e438fc8 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8868

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3c4e438fc8

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183107.html>

Fedora Core 22

mingw-poppler-0.30.0-4.fc22

190540 - Fedora Linux 22 FEDORA-2016-8d983eeb13 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3144

Description

The scan detected that the host is missing the following update:
FEDORA-2016-8d983eeb13

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182953.html>

Fedora Core 22

drupal7-block_class-2.3-1.fc22

190541 - Fedora Linux 23 FEDORA-2016-cb7a73c82e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-cb7a73c82e

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183056.html>

Fedora Core 23

webkitgtk4-2.12.1-1.fc23

190542 - Fedora Linux 23 FEDORA-2016-2fcfc7670f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3959

Description

The scan detected that the host is missing the following update:
FEDORA-2016-2fcfc7670f

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183137.html>

Fedora Core 23

golang-1.5.4-1.fc23

190543 - Fedora Linux 23 FEDORA-2016-80c07fbb6c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-80c07fbb6c

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183058.html>

Fedora Core 23

w3m-0.5.3-24.fc23

190544 - Fedora Linux 23 FEDORA-2016-a099d11840 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a099d11840

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182895.html>

Fedora Core 23

glpi-0.90.3-1.fc23

190545 - Fedora Linux 22 FEDORA-2016-5f44e89fe0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2016-5f44e89fe0

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183075.html>

Fedora Core 22

python-tgcaptcha2-0.3.1-1.fc22

190546 - Fedora Linux 23 FEDORA-2016-73eb29f890 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2016-73eb29f890

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183096.html>

Fedora Core 23

parallel-20160222-1.fc23

190547 - Fedora Linux 22 FEDORA-2016-657a4a658e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-657a4a658e

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182961.html>

Fedora Core 22

glpi-0.90.3-1.fc22

190548 - Fedora Linux 22 FEDORA-2016-6cf17ad0df Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2173

Description

The scan detected that the host is missing the following update:
FEDORA-2016-6cf17ad0df

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182959.html>

Fedora Core 22

springframework-amqp-1.3.9-4.fc22

190549 - Fedora Linux 23 FEDORA-2016-65519440f5 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3096

Description

The scan detected that the host is missing the following update:
FEDORA-2016-65519440f5

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183132.html>

Fedora Core 23

ansible1.9-1.9.6-1.fc23

190550 - Fedora Linux 22 FEDORA-2016-28ff51a3f5 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3096

Description

The scan detected that the host is missing the following update:
FEDORA-2016-28ff51a3f5

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183103.html>

Fedora Core 22

ansible1.9-1.9.6-1.fc22

190551 - Fedora Linux 23 FEDORA-2016-d5c26081f3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d5c26081f3

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183077.html>

Fedora Core 23

thunderbird-45.0-2.fc23

190552 - Fedora Linux 22 FEDORA-2016-7eb5caa94d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-7eb5caa94d

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183074.html>

Fedora Core 22

parallel-20160222-1.fc22

190554 - Fedora Linux 23 FEDORA-2016-33ccc205e7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-33ccc205e7

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183050.html>

Fedora Core 23

java-1.8.0-openjdk-1.8.0.91-1.b14.fc23

190555 - Fedora Linux 23 FEDORA-2016-383b8250e6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4008

Description

The scan detected that the host is missing the following update:
FEDORA-2016-383b8250e6

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182907.html>

Fedora Core 23

libtasn1-4.8-1.fc23

190556 - Fedora Linux 23 FEDORA-2016-c3d9a9c0c4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2016-c3d9a9c0c4

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183150.html>

Fedora Core 23

rpm-4.13.0-0.rc1.13.fc23

190558 - Fedora Linux 22 FEDORA-2016-85e9f2e3cd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3099

Description

The scan detected that the host is missing the following update:
FEDORA-2016-85e9f2e3cd

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183102.html>

Fedora Core 22

mod_nss-1.0.11-7.fc22

190559 - Fedora Linux 23 FEDORA-2016-de909cc333 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3674

Description

The scan detected that the host is missing the following update:
FEDORA-2016-de909cc333

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183180.html>

Fedora Core 23

xstream-1.4.9-1.fc23

190560 - Fedora Linux 22 FEDORA-2016-250042b8a6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3674

Description

The scan detected that the host is missing the following update:
FEDORA-2016-250042b8a6

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183208.html>

Fedora Core 22

xstream-1.4.9-1.fc22

190562 - Fedora Linux 23 FEDORA-2016-7f5004093e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8325

Description

The scan detected that the host is missing the following update:
FEDORA-2016-7f5004093e

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183076.html>

Fedora Core 23

openssh-7.2p2-3.fc23

190563 - Fedora Linux 23 FEDORA-2016-d7dafbf27f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d7dafbf27f

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183097.html>

Fedora Core 23

python-tgcaptcha2-0.3.1-1.fc23

190564 - Fedora Linux 23 FEDORA-2016-0d82b3eb5d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3144

Description

The scan detected that the host is missing the following update:
FEDORA-2016-0d82b3eb5d

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182886.html>

Fedora Core 23

drupal7-block_class-2.3-1.fc23

190567 - Fedora Linux 23 FEDORA-2016-c848d48286 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8868

Description

The scan detected that the host is missing the following update:
FEDORA-2016-c848d48286

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183142.html>

Fedora Core 23

mingw-poppler-0.34.0-2.fc23

190568 - Fedora Linux 24 FEDORA-2016-73c0897e5e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-73c0897e5e

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182819.html>

Fedora Core 24

webkitgtk4-2.12.1-1.fc24

190569 - Fedora Linux 23 FEDORA-2016-8b28358b72 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3099

Description

The scan detected that the host is missing the following update:
FEDORA-2016-8b28358b72

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183129.html>

Fedora Core 23

mod_nss-1.0.12-3.fc23

190570 - Fedora Linux 23 FEDORA-2016-f099190fee Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2173

Description

The scan detected that the host is missing the following update:
FEDORA-2016-f099190fee

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182850.html>

Fedora Core 23

springframework-amqp-1.3.9-4.fc23

190566 - Fedora Linux 24 FEDORA-2016-7f37d42add Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3955, CVE-2016-3961

Description

The scan detected that the host is missing the following update:
FEDORA-2016-7f37d42add

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183042.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2016-April/183041.html>

Fedora Core 24

binutils-2.26-18.fc24

kernel-4.5.2-301.fc24

19968 - Update to Improve Wireless Mouse Input Filtering (3152550)

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

A vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is popular operating system for desktop and servers.

A vulnerability is present in some versions of Microsoft Windows. The flaw is due to improper filtering packets received from USB wireless dongles. Successful exploitation could allow a local attacker to inject keyboard HID packets into Microsoft wireless mouse devices through USB dongles.

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.

9743 - FutureSoft TFTP Server 2000 Remote Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

16628 - FrameFlow Server Monitor Unspecified Defect Denial Of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

1371 - Poll It CGI Script Arbitrary File Disclosure

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

Risk Level: High

CVE: CVE-2000-0590

[Update Details](#)

FASLScript is updated

19445 - (SOL17515) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7855

[Update Details](#)

FASLScript is updated

19446 - (SOL17517) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7701

[Update Details](#)

FASLScript is updated

70002 - http-helpers.fasI3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

70048 - adobe.fasI3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

70088 - ibm.fasI3.inc

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

Risk Level: Informational
CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

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

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

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2016 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates