

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

20841 - (HT207272) Apple Safari Multiple Vulnerabilities Prior To 10.0.1

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

Risk Level: High

CVE: CVE-2016-4613, CVE-2016-4666, CVE-2016-4677, CVE-2016-7578

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

Multiple vulnerabilities are present in some versions of Apple Safari. The flaws lie in Webkit component. Successful exploitation could allow an attacker to obtain sensitive information or execute arbitrary code.

20855 - (HT207271) Apple iOS Multiple Vulnerabilities Prior To 10.1

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2016-4660, CVE-2016-4664, CVE-2016-4665, CVE-2016-4666, CVE-2016-4669, CVE-2016-4670, CVE-2016-4673, CVE-2016-4675, CVE-2016-4677, CVE-2016-4679, CVE-2016-4680, CVE-2016-4686, CVE-2016-4721, CVE-2016-7577, CVE-2016-7578, CVE-2016-7579, CVE-2016-7613

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

Apple iOS is the operating system used by Apple iPhone, iPad and iPod touch.

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

141322 - Red Hat Enterprise Linux RHSA-2016-2595 Update Is Not Installed

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

Risk Level: High

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

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2595.html>

RHEL7D

x86_64

mariadb-debuginfo-5.5.52-1.el7
mariadb-server-5.5.52-1.el7
mariadb-test-5.5.52-1.el7
mariadb-embedded-devel-5.5.52-1.el7
mariadb-embedded-5.5.52-1.el7
mariadb-devel-5.5.52-1.el7
mariadb-5.5.52-1.el7
mariadb-bench-5.5.52-1.el7
mariadb-libs-5.5.52-1.el7

RHEL7WS

x86_64

mariadb-debuginfo-5.5.52-1.el7
mariadb-server-5.5.52-1.el7
mariadb-test-5.5.52-1.el7
mariadb-libs-5.5.52-1.el7
mariadb-embedded-5.5.52-1.el7
mariadb-embedded-devel-5.5.52-1.el7
mariadb-5.5.52-1.el7
mariadb-bench-5.5.52-1.el7
mariadb-devel-5.5.52-1.el7

141331 - Red Hat Enterprise Linux RHSA-2016-2574 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2015-8956, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-3841, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2574.html>

RHEL7D

x86_64

python-perf-debuginfo-3.10.0-514.el7
python-perf-3.10.0-514.el7
kernel-debuginfo-common-x86_64-3.10.0-514.el7
kernel-debug-debuginfo-3.10.0-514.el7
kernel-debug-devel-3.10.0-514.el7
perf-3.10.0-514.el7

kernel-tools-debuginfo-3.10.0-514.el7
kernel-headers-3.10.0-514.el7
kernel-devel-3.10.0-514.el7
kernel-tools-libs-devel-3.10.0-514.el7
kernel-debuginfo-3.10.0-514.el7
kernel-debug-3.10.0-514.el7
perf-debuginfo-3.10.0-514.el7
kernel-tools-3.10.0-514.el7
kernel-tools-libs-3.10.0-514.el7
kernel-3.10.0-514.el7

noarch
kernel-abi-whitelists-3.10.0-514.el7
kernel-doc-3.10.0-514.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-514.el7
kernel-doc-3.10.0-514.el7

RHEL7WS
x86_64
python-perf-debuginfo-3.10.0-514.el7
python-perf-3.10.0-514.el7
kernel-debuginfo-common-x86_64-3.10.0-514.el7
kernel-debug-debuginfo-3.10.0-514.el7
kernel-debug-devel-3.10.0-514.el7
perf-3.10.0-514.el7
kernel-tools-debuginfo-3.10.0-514.el7
kernel-headers-3.10.0-514.el7
kernel-devel-3.10.0-514.el7
kernel-tools-libs-devel-3.10.0-514.el7
kernel-debuginfo-3.10.0-514.el7
kernel-debug-3.10.0-514.el7
perf-debuginfo-3.10.0-514.el7
kernel-tools-3.10.0-514.el7
kernel-tools-libs-3.10.0-514.el7
kernel-3.10.0-514.el7

noarch
kernel-abi-whitelists-3.10.0-514.el7
kernel-doc-3.10.0-514.el7

141344 - Red Hat Enterprise Linux RHSA-2016-2607 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8165

Description

The scan detected that the host is missing the following update:
RHSA-2016-2607

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2607.html>

RHEL7S
noarch
powerpc-utils-python-1.2.1-9.el7

141349 - Red Hat Enterprise Linux RHSA-2016-2586 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5636

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2586.html>

RHEL7D
x86_64
python-tools-2.7.5-48.el7
python-2.7.5-48.el7
tkinter-2.7.5-48.el7
python-test-2.7.5-48.el7
python-devel-2.7.5-48.el7
python-debug-2.7.5-48.el7
python-debuginfo-2.7.5-48.el7
python-libs-2.7.5-48.el7

RHEL7WS
x86_64
python-tools-2.7.5-48.el7
python-2.7.5-48.el7
tkinter-2.7.5-48.el7
python-test-2.7.5-48.el7
python-devel-2.7.5-48.el7
python-debug-2.7.5-48.el7
python-debuginfo-2.7.5-48.el7
python-libs-2.7.5-48.el7

144975 - SuSE Linux 13.1 openSUSE-SU-2016:2737-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-3522, CVE-2011-4516, CVE-2011-4517, CVE-2014-8137, CVE-2014-8138, CVE-2014-8157, CVE-2014-8158, CVE-2014-9029, CVE-2015-5203, CVE-2015-5221, CVE-2016-1577, CVE-2016-1867, CVE-2016-2089, CVE-2016-2116, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8880, CVE-2016-8881, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2737-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00018.html>

SuSE Linux 13.1

x86_64

libjasper1-32bit-1.900.14-160.25.1

libjasper1-1.900.14-160.25.1

libjasper1-debuginfo-1.900.14-160.25.1

jasper-1.900.14-160.25.1

libjasper-devel-1.900.14-160.25.1

jasper-debugsource-1.900.14-160.25.1

jasper-debuginfo-1.900.14-160.25.1

libjasper1-debuginfo-32bit-1.900.14-160.25.1

i586

libjasper1-1.900.14-160.25.1

libjasper1-debuginfo-1.900.14-160.25.1

jasper-1.900.14-160.25.1

libjasper-devel-1.900.14-160.25.1

jasper-debugsource-1.900.14-160.25.1

jasper-debuginfo-1.900.14-160.25.1

144981 - SuSE Linux 13.2 openSUSE-SU-2016:2730-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4658

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2730-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00012.html>

SuSE Linux 13.2

i586

python-libxml2-debuginfo-2.9.4-7.20.1

libxml2-2-debuginfo-2.9.4-7.20.1

libxml2-2-2.9.4-7.20.1

python-libxml2-2.9.4-7.20.1

libxml2-debugsource-2.9.4-7.20.1

libxml2-tools-debuginfo-2.9.4-7.20.1

libxml2-tools-2.9.4-7.20.1

libxml2-devel-2.9.4-7.20.1

python-libxml2-debugsource-2.9.4-7.20.1

noarch

libxml2-doc-2.9.4-7.20.1

x86_64

python-libxml2-debuginfo-2.9.4-7.20.1

libxml2-2-debuginfo-2.9.4-7.20.1

libxml2-2-2.9.4-7.20.1
python-libxml2-2.9.4-7.20.1
libxml2-debugsource-2.9.4-7.20.1
libxml2-tools-debuginfo-2.9.4-7.20.1
libxml2-tools-2.9.4-7.20.1
libxml2-devel-2.9.4-7.20.1
libxml2-2-debuginfo-32bit-2.9.4-7.20.1
libxml2-2-32bit-2.9.4-7.20.1
python-libxml2-debugsource-2.9.4-7.20.1
libxml2-devel-32bit-2.9.4-7.20.1

144983 - SuSE Linux 13.2 openSUSE-SU-2016:2722-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2722-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00010.html>

SuSE Linux 13.2

x86_64

libjasper1-1.900.14-163.24.1
libjasper1-32bit-1.900.14-163.24.1
jasper-1.900.14-163.24.1
jasper-debugsource-1.900.14-163.24.1
libjasper1-debuginfo-32bit-1.900.14-163.24.1
libjasper1-debuginfo-1.900.14-163.24.1
libjasper-devel-1.900.14-163.24.1
jasper-debuginfo-1.900.14-163.24.1

i586

libjasper1-1.900.14-163.24.1
jasper-1.900.14-163.24.1
jasper-debugsource-1.900.14-163.24.1
libjasper1-debuginfo-1.900.14-163.24.1
libjasper-devel-1.900.14-163.24.1
jasper-debuginfo-1.900.14-163.24.1

144986 - SuSE Linux 13.2 openSUSE-SU-2016:2746-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440, CVE-2016-5612, CVE-2016-5630, CVE-2016-6662

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2746-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00021.html>

SuSE Linux 13.2

x86_64

mariadb-debuginfo-10.0.27-2.27.1
libmysqlclient18-debuginfo-32bit-10.0.27-2.27.1
mariadb-debugsource-10.0.27-2.27.1
libmysqlclient18-32bit-10.0.27-2.27.1
libmysqlclient_r18-10.0.27-2.27.1
libmysqlclient_r18-32bit-10.0.27-2.27.1
libmysqld18-debuginfo-10.0.27-2.27.1
libmysqld-devel-10.0.27-2.27.1
libmysqlclient18-debuginfo-10.0.27-2.27.1
mariadb-bench-10.0.27-2.27.1
mariadb-errormessages-10.0.27-2.27.1
mariadb-tools-10.0.27-2.27.1
libmysqld18-10.0.27-2.27.1
mariadb-client-10.0.27-2.27.1
mariadb-client-debuginfo-10.0.27-2.27.1
mariadb-test-debuginfo-10.0.27-2.27.1
libmysqlclient-devel-10.0.27-2.27.1
mariadb-bench-debuginfo-10.0.27-2.27.1
mariadb-10.0.27-2.27.1
libmysqlclient18-10.0.27-2.27.1
mariadb-tools-debuginfo-10.0.27-2.27.1
mariadb-test-10.0.27-2.27.1

i586

mariadb-debuginfo-10.0.27-2.27.1
mariadb-debugsource-10.0.27-2.27.1
libmysqlclient_r18-10.0.27-2.27.1
libmysqld18-debuginfo-10.0.27-2.27.1
libmysqld-devel-10.0.27-2.27.1
libmysqlclient18-debuginfo-10.0.27-2.27.1
mariadb-bench-10.0.27-2.27.1
mariadb-errormessages-10.0.27-2.27.1
mariadb-tools-10.0.27-2.27.1
libmysqld18-10.0.27-2.27.1
mariadb-client-10.0.27-2.27.1
mariadb-client-debuginfo-10.0.27-2.27.1
mariadb-test-debuginfo-10.0.27-2.27.1
libmysqlclient-devel-10.0.27-2.27.1
mariadb-bench-debuginfo-10.0.27-2.27.1
mariadb-10.0.27-2.27.1
libmysqlclient18-10.0.27-2.27.1
mariadb-tools-debuginfo-10.0.27-2.27.1
mariadb-test-10.0.27-2.27.1

20844 - IBM AIX Lquerylv Privilege Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2016-6079

Description

A vulnerability is present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

A vulnerability is present in some versions of IBM AIX. The flaw lies in lquerylv in LVM. Successful exploitation could allow an attacker to obtain root privileges.

20846 - (HPSBGN03648) HPE LoadRunner Remote Denial of Service Vulnerability

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

Risk Level: High

CVE: CVE-2016-4384

Description

A denial of service vulnerability is present in some versions of HP LoadRunner.

Observation

HP LoadRunner is a test automation software.

A denial of service vulnerability is present in some versions of HP LoadRunner. The affected component is unspecified. Successful exploitation could allow a remote attacker to cause a denial of service.

20847 - (HPSBMU03653) HPE System Management Homepage Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-3739, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4342, CVE-2016-4343, CVE-2016-4393, CVE-2016-4394, CVE-2016-4395, CVE-2016-4396, CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-5385, CVE-2016-5387, CVE-2016-5388

Description

Multiple vulnerabilities are present in some versions of HPE System Management Homepage.

Observation

HPE System Management Homepage is a web-based interface that consolidates and simplifies the management of individual ProLiant and Integrity servers.

Multiple vulnerabilities are present in some versions of HPE System Management Homepage. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, execute remote code, disclose or modify sensitive information.

20848 - (HT207268) Apple Xcode Multiple Vulnerabilities Prior To 8.1

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

Risk Level: High

CVE: CVE-2015-3193, CVE-2015-3194, CVE-2015-6764, CVE-2015-8027, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-1669, CVE-2016-2086, CVE-2016-2216

Description

Multiple vulnerabilities are present in some versions of Apple Xcode.

Observation

Apple Xcode is an integrated development environment.

Multiple vulnerabilities are present in some versions of Apple Xcode. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose private information, execute remote code or cause unexpected application termination.

130619 - Debian Linux 8.0 DSA-3707-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
DSA-3707-1

Observation

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

<http://www.debian.org/security/2016/dsa-3707>

Debian 8.0

all

openjdk-7-jre-zero_7u111-2.6.7-2~deb8u1

openjdk-7-doc_7u111-2.6.7-2~deb8u1

openjdk-7-jre-headless_7u111-2.6.7-2~deb8u1

openjdk-7-dbg_7u111-2.6.7-2~deb8u1

openjdk-7-source_7u111-2.6.7-2~deb8u1

icedtea-7-jre-jamvm_7u111-2.6.7-2~deb8u1

openjdk-7-jdk_7u111-2.6.7-2~deb8u1

openjdk-7-jre-lib_7u111-2.6.7-2~deb8u1

openjdk-7-demo_7u111-2.6.7-2~deb8u1

openjdk-7-jre_7u111-2.6.7-2~deb8u1

130624 - Debian Linux 8.0 DSA-3709-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4738

Description

The scan detected that the host is missing the following update:
DSA-3709-1

Observation

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

<http://www.debian.org/security/2016/dsa-3709>

Debian 8.0

all

libxslt1-dev_1.1.28-2+deb8u2
xsltproc_1.1.28-2+deb8u2
libxslt1.1_1.1.28-2+deb8u2
python-libxslt1_1.1.28-2+deb8u2
python-libxslt1-dbg_1.1.28-2+deb8u2
libxslt1-dbg_1.1.28-2+deb8u2

141325 - Red Hat Enterprise Linux RHSA-2016-2580 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8868

Description

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

RHSA-2016-2580

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2580.html>

RHEL7D

x86_64

poppler-qt-devel-0.26.5-16.el7
poppler-cpp-0.26.5-16.el7
poppler-0.26.5-16.el7
poppler-devel-0.26.5-16.el7
poppler-cpp-devel-0.26.5-16.el7
poppler-glib-devel-0.26.5-16.el7
poppler-demos-0.26.5-16.el7
poppler-qt-0.26.5-16.el7
poppler-utils-0.26.5-16.el7
poppler-debuginfo-0.26.5-16.el7
poppler-glib-0.26.5-16.el7

RHEL7WS

x86_64

poppler-qt-devel-0.26.5-16.el7
poppler-cpp-0.26.5-16.el7
poppler-0.26.5-16.el7
poppler-devel-0.26.5-16.el7
poppler-cpp-devel-0.26.5-16.el7
poppler-glib-devel-0.26.5-16.el7
poppler-demos-0.26.5-16.el7
poppler-qt-0.26.5-16.el7
poppler-utils-0.26.5-16.el7
poppler-debuginfo-0.26.5-16.el7
poppler-glib-0.26.5-16.el7

141339 - Red Hat Enterprise Linux RHSA-2016-2659 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5573, CVE-2016-5597

Description

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

RHSA-2016-2659

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2659.html>

RHEL5S

i386

java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-accessibility-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el5_11

x86_64

java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-accessibility-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el5_11

RHEL6D

x86_64

java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el6_8

i386

java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el6_8

RHEL6S

i386

java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el6_8

x86_64
java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el6_8

RHEL6WS

x86_64
java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el6_8

i386
java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el6_8
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el6_8

RHEL5D

x86_64
java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-accessibility-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el5_11

i386
java-1.6.0-ibm-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-javacomm-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-demo-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-jdbc-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-devel-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-accessibility-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-plugin-1.6.0.16.35-1jpp.1.el5_11
java-1.6.0-ibm-src-1.6.0.16.35-1jpp.1.el5_11

141355 - Red Hat Enterprise Linux RHSA-2016-2579 Update Is Not Installed

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

Risk Level: High

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

Description

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

RHSA-2016-2579

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2579.html>

RHEL7D

x86_64

libreoffice-langpack-ta-5.0.6.2-3.el7

libreoffice-xsltfilter-5.0.6.2-3.el7

libreoffice-langpack-th-5.0.6.2-3.el7

libcmis-devel-0.5.1-2.el7

libreoffice-langpack-de-5.0.6.2-3.el7

libreoffice-langpack-mai-5.0.6.2-3.el7

libreoffice-langpack-ts-5.0.6.2-3.el7

libreoffice-langpack-fi-5.0.6.2-3.el7

libreoffice-langpack-pl-5.0.6.2-3.el7

libpagemaker-tools-0.0.3-1.el7

libreoffice-rhino-5.0.6.2-3.el7

libreoffice-langpack-sl-5.0.6.2-3.el7

libreoffice-langpack-si-5.0.6.2-3.el7

libreoffice-gdb-debug-support-5.0.6.2-3.el7

libreoffice-langpack-sr-5.0.6.2-3.el7

libreoffice-langpack-ve-5.0.6.2-3.el7

libreoffice-langpack-zh-Hans-5.0.6.2-3.el7

libreoffice-calc-5.0.6.2-3.el7

libreoffice-emailmerge-5.0.6.2-3.el7

libreoffice-langpack-gu-5.0.6.2-3.el7

libreoffice-langpack-tr-5.0.6.2-3.el7

libreoffice-langpack-ar-5.0.6.2-3.el7

libreoffice-langpack-nb-5.0.6.2-3.el7

libreoffice-filters-5.0.6.2-3.el7

libreoffice-debuginfo-5.0.6.2-3.el7

libreoffice-langpack-kn-5.0.6.2-3.el7

libreoffice-langpack-kk-5.0.6.2-3.el7

libreoffice-langpack-nn-5.0.6.2-3.el7

libreoffice-langpack-lt-5.0.6.2-3.el7

libreoffice-writer-5.0.6.2-3.el7

libreoffice-langpack-en-5.0.6.2-3.el7

libreoffice-langpack-nl-5.0.6.2-3.el7

libreoffice-officebean-5.0.6.2-3.el7

libreoffice-langpack-nr-5.0.6.2-3.el7

libreoffice-langpack-el-5.0.6.2-3.el7

libreoffice-langpack-it-5.0.6.2-3.el7

libreoffice-langpack-ro-5.0.6.2-3.el7

libreoffice-langpack-ca-5.0.6.2-3.el7

libreoffice-langpack-he-5.0.6.2-3.el7

libreoffice-langpack-fa-5.0.6.2-3.el7

libreoffice-langpack-pt-PT-5.0.6.2-3.el7

libreoffice-langpack-te-5.0.6.2-3.el7

libreoffice-langpack-bn-5.0.6.2-3.el7

libreoffice-langpack-dz-5.0.6.2-3.el7

libreoffice-langpack-cs-5.0.6.2-3.el7

libpagemaker-debuginfo-0.0.3-1.el7

libreoffice-bsh-5.0.6.2-3.el7

libreoffice-sdk-5.0.6.2-3.el7

libreoffice-langpack-or-5.0.6.2-3.el7

libreoffice-pdfimport-5.0.6.2-3.el7

libreoffice-langpack-br-5.0.6.2-3.el7

libreoffice-graphicfilter-5.0.6.2-3.el7

libreoffice-langpack-af-5.0.6.2-3.el7
libreoffice-langpack-hi-5.0.6.2-3.el7
libreoffice-langpack-ga-5.0.6.2-3.el7
libreoffice-langpack-hr-5.0.6.2-3.el7
libreoffice-postgresql-5.0.6.2-3.el7
libreoffice-math-5.0.6.2-3.el7
libreoffice-core-5.0.6.2-3.el7
libpagemaker-devel-0.0.3-1.el7
libreoffice-pyuno-5.0.6.2-3.el7
libreoffice-langpack-bg-5.0.6.2-3.el7
libreoffice-langpack-es-5.0.6.2-3.el7
libreoffice-langpack-sk-5.0.6.2-3.el7
libreoffice-impress-5.0.6.2-3.el7
libreoffice-langpack-ru-5.0.6.2-3.el7
libreoffice-langpack-eu-5.0.6.2-3.el7
libreoffice-langpack-pt-BR-5.0.6.2-3.el7
libreoffice-langpack-uk-5.0.6.2-3.el7
libreoffice-ogltrans-5.0.6.2-3.el7
libreoffice-ure-5.0.6.2-3.el7
libreoffice-langpack-zh-Hant-5.0.6.2-3.el7
libreoffice-nlpsolver-5.0.6.2-3.el7
libreoffice-wiki-publisher-5.0.6.2-3.el7
libreoffice-langpack-xh-5.0.6.2-3.el7
libreoffice-langpack-da-5.0.6.2-3.el7
libreoffice-base-5.0.6.2-3.el7
libreoffice-langpack-ja-5.0.6.2-3.el7
libpagemaker-0.0.3-1.el7
libreoffice-librelogo-5.0.6.2-3.el7
libreoffice-langpack-hu-5.0.6.2-3.el7
libreoffice-langpack-zu-5.0.6.2-3.el7
libreoffice-langpack-ss-5.0.6.2-3.el7
libreoffice-draw-5.0.6.2-3.el7
libreoffice-langpack-st-5.0.6.2-3.el7
libreoffice-langpack-as-5.0.6.2-3.el7
libreoffice-langpack-ml-5.0.6.2-3.el7
libreoffice-langpack-fr-5.0.6.2-3.el7
libreoffice-langpack-mr-5.0.6.2-3.el7
libreoffice-langpack-ko-5.0.6.2-3.el7
libcmis-tools-0.5.1-2.el7
libcmis-debuginfo-0.5.1-2.el7
libreoffice-langpack-pa-5.0.6.2-3.el7
libcmis-0.5.1-2.el7
libreoffice-langpack-cy-5.0.6.2-3.el7
libreoffice-glade-5.0.6.2-3.el7
libreoffice-langpack-gl-5.0.6.2-3.el7
libreoffice-langpack-tn-5.0.6.2-3.el7
libreoffice-langpack-nso-5.0.6.2-3.el7
libreoffice-5.0.6.2-3.el7
libreoffice-langpack-et-5.0.6.2-3.el7
libreoffice-langpack-sv-5.0.6.2-3.el7
libreoffice-sdk-doc-5.0.6.2-3.el7
libreoffice-langpack-lv-5.0.6.2-3.el7

noarch

autocorr-ca-5.0.6.2-3.el7
autocorr-da-5.0.6.2-3.el7
autocorr-en-5.0.6.2-3.el7
autocorr-de-5.0.6.2-3.el7
autocorr-ro-5.0.6.2-3.el7
autocorr-ja-5.0.6.2-3.el7

autocorr-is-5.0.6.2-3.el7
autocorr-af-5.0.6.2-3.el7
autocorr-ru-5.0.6.2-3.el7
autocorr-zh-5.0.6.2-3.el7
autocorr-hu-5.0.6.2-3.el7
autocorr-sl-5.0.6.2-3.el7
mdds-devel-0.12.1-1.el7
autocorr-sk-5.0.6.2-3.el7
libreoffice-opensymbol-fonts-5.0.6.2-3.el7
autocorr-lb-5.0.6.2-3.el7
autocorr-sr-5.0.6.2-3.el7
autocorr-fa-5.0.6.2-3.el7
autocorr-pl-5.0.6.2-3.el7
autocorr-cs-5.0.6.2-3.el7
autocorr-fr-5.0.6.2-3.el7
autocorr-es-5.0.6.2-3.el7
libpagemaker-doc-0.0.3-1.el7
autocorr-fi-5.0.6.2-3.el7
autocorr-pt-5.0.6.2-3.el7
autocorr-sv-5.0.6.2-3.el7
autocorr-ga-5.0.6.2-3.el7
autocorr-mn-5.0.6.2-3.el7
autocorr-bg-5.0.6.2-3.el7
autocorr-ko-5.0.6.2-3.el7
autocorr-vi-5.0.6.2-3.el7
autocorr-lt-5.0.6.2-3.el7
autocorr-tr-5.0.6.2-3.el7
autocorr-nl-5.0.6.2-3.el7
autocorr-it-5.0.6.2-3.el7
autocorr-hr-5.0.6.2-3.el7

RHEL7WS

x86_64

libreoffice-langpack-ta-5.0.6.2-3.el7
libreoffice-xsltfilter-5.0.6.2-3.el7
libreoffice-langpack-th-5.0.6.2-3.el7
libcmis-devel-0.5.1-2.el7
libreoffice-langpack-de-5.0.6.2-3.el7
libreoffice-langpack-mai-5.0.6.2-3.el7
libreoffice-langpack-ts-5.0.6.2-3.el7
libreoffice-langpack-fi-5.0.6.2-3.el7
libreoffice-langpack-pl-5.0.6.2-3.el7
libpagemaker-tools-0.0.3-1.el7
libreoffice-rhino-5.0.6.2-3.el7
libreoffice-langpack-sl-5.0.6.2-3.el7
libreoffice-langpack-si-5.0.6.2-3.el7
libreoffice-gdb-debug-support-5.0.6.2-3.el7
libreoffice-langpack-sr-5.0.6.2-3.el7
libreoffice-langpack-ve-5.0.6.2-3.el7
libreoffice-langpack-zh-Hans-5.0.6.2-3.el7
libreoffice-calc-5.0.6.2-3.el7
libreoffice-emailmerge-5.0.6.2-3.el7
libreoffice-langpack-gu-5.0.6.2-3.el7
libreoffice-langpack-tr-5.0.6.2-3.el7
libreoffice-langpack-ar-5.0.6.2-3.el7
libreoffice-langpack-nb-5.0.6.2-3.el7
libreoffice-filters-5.0.6.2-3.el7
libreoffice-debuginfo-5.0.6.2-3.el7
libreoffice-langpack-kn-5.0.6.2-3.el7
libreoffice-langpack-kk-5.0.6.2-3.el7

libreoffice-langpack-nn-5.0.6.2-3.el7
libreoffice-langpack-lt-5.0.6.2-3.el7
libreoffice-writer-5.0.6.2-3.el7
libreoffice-langpack-en-5.0.6.2-3.el7
libreoffice-langpack-nl-5.0.6.2-3.el7
libreoffice-officebean-5.0.6.2-3.el7
libreoffice-langpack-nr-5.0.6.2-3.el7
libreoffice-langpack-el-5.0.6.2-3.el7
libreoffice-langpack-it-5.0.6.2-3.el7
libreoffice-langpack-ro-5.0.6.2-3.el7
libreoffice-langpack-ca-5.0.6.2-3.el7
libreoffice-langpack-he-5.0.6.2-3.el7
libreoffice-langpack-fa-5.0.6.2-3.el7
libreoffice-langpack-pt-PT-5.0.6.2-3.el7
libreoffice-langpack-te-5.0.6.2-3.el7
libreoffice-langpack-bn-5.0.6.2-3.el7
libreoffice-langpack-dz-5.0.6.2-3.el7
libreoffice-langpack-cs-5.0.6.2-3.el7
libpagemaker-debuginfo-0.0.3-1.el7
libreoffice-bsh-5.0.6.2-3.el7
libreoffice-sdk-5.0.6.2-3.el7
libreoffice-langpack-or-5.0.6.2-3.el7
libreoffice-pdfimport-5.0.6.2-3.el7
libreoffice-langpack-br-5.0.6.2-3.el7
libreoffice-graphicfilter-5.0.6.2-3.el7
libreoffice-langpack-af-5.0.6.2-3.el7
libreoffice-langpack-hi-5.0.6.2-3.el7
libreoffice-langpack-ga-5.0.6.2-3.el7

141359 - Red Hat Enterprise Linux RHSA-2016-2658 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2658

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2658.html>

RHEL5S

x86_64

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el5_11

i386

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el5_11

RHEL6S

i386

java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el6_8

noarch

java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el6_8

x86_64

java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el6_8

RHEL6WS

x86_64

java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8

i386

java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8

RHEL5D

x86_64

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el5_11

i386

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el5_11
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el5_11

RHEL7D

x86_64

java-1.7.0-openjdk-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-src-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-accessibility-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-headless-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.0.el7_3

noarch
java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.0.el7_3

RHEL6D
i386
java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el6_8

noarch
java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el6_8

x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el6_8
java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el6_8

RHEL7WS
x86_64
java-1.7.0-openjdk-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-src-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-headless-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-accessibility-1.7.0.121-2.6.8.0.el7_3
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.0.el7_3

noarch
java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.0.el7_3

144988 - SuSE SLES 12 SP1 SUSE-SU-2016:2726-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3485, CVE-2016-3511, CVE-2016-3598

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2726-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-November/002395.html>

SuSE SLES 12 SP1
x86_64
java-1_8_0-ibm-1.8.0_sr3.10-15.1
java-1_8_0-ibm-alsa-1.8.0_sr3.10-15.1
java-1_8_0-ibm-plugin-1.8.0_sr3.10-15.1

163185 - Oracle Enterprise Linux ELSA-2016-2658 Update Is Not Installed

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

Risk Level: High

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

Description

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

ELSA-2016-2658

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-November/006462.html>

<http://oss.oracle.com/pipermail/el-errata/2016-November/006461.html>

OEL5

x86_64

java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.0.1.el5_11

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.0.1.el5_11

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.0.1.el5_11

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.0.1.el5_11

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.0.1.el5_11

i386

java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.0.1.el5_11

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.0.1.el5_11

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.0.1.el5_11

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.0.1.el5_11

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.0.1.el5_11

OEL6

x86_64

java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.0.1.el6_8

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.0.1.el6_8

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.0.1.el6_8

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.0.1.el6_8

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.0.1.el6_8

i386

java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.0.1.el6_8

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.0.1.el6_8

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.0.1.el6_8

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.0.1.el6_8

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.0.1.el6_8

175031 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL5.x, SL6.x i386/x86_64 (1611-736)

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

Risk Level: High

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

Description

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

Security ERRATA Important: java-1.7.0-openjdk on SL5.x, SL6.x i386/x86_64 (1611-736)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind16111&L=scientific-linux-errata&F=&S=&P=736>

SL6

i386

java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el6_8

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el6_8

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el6_8

noarch

java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el6_8

x86_64

java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el6_8

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el6_8

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el6_8

SL5

x86_64

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el5_11

i386

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-debuginfo-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el5_11

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el5_11

178234 - Gentoo Linux GLSA-201611-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Description

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

GLSA-201611-04

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201611-04>

Affected packages:

dev-java/oracle-jre-bin < 1.8.0.111

dev-java/oracle-jdk-bin < 1.8.0.111

185471 - Ubuntu Linux 16.04, 16.10 USN-3121-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
USN-3121-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003618.html>

Ubuntu 16.10

openjdk-8-jdk-headless_8u111-b14-2ubuntu0.16.10.2
openjdk-8-jre-zero_8u111-b14-2ubuntu0.16.10.2
openjdk-8-jdk_8u111-b14-2ubuntu0.16.10.2
openjdk-8-jre-headless_8u111-b14-2ubuntu0.16.10.2
openjdk-8-jre_8u111-b14-2ubuntu0.16.10.2
openjdk-8-jre-jamvm_8u111-b14-2ubuntu0.16.10.2

Ubuntu 16.04

openjdk-8-jre-zero_8u111-b14-2ubuntu0.16.04.2
openjdk-8-jdk-headless_8u111-b14-2ubuntu0.16.04.2
openjdk-8-jdk_8u111-b14-2ubuntu0.16.04.2
openjdk-8-jre_8u111-b14-2ubuntu0.16.04.2
openjdk-8-jre-jamvm_8u111-b14-2ubuntu0.16.04.2
openjdk-8-jre-headless_8u111-b14-2ubuntu0.16.04.2

20730 - Cisco NX-OS Software Crafted DHCPv4 Packet Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-6392

Description

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

Observation

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

A denial of service vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the implementation of the DHCPv4 relay agent and smart relay agent in Cisco NX-OS Software. Successful exploitation could allow an attacker to cause a denial of service condition.

20723 - Oracle GlassFish Server Critical Patch Update October 2016

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

Risk Level: High

CVE: CVE-2016-1950, CVE-2016-5519

Description

Multiple vulnerabilities are present in some versions of Oracle GlassFish.

Observation

Oracle GlassFish Server supports lightweight Java EE 6 Web Profile and the Java EE 6 platform.

Multiple vulnerabilities are present in some versions of Oracle GlassFish Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to remotely execute arbitrary code.

20732 - Novell Sentinel Vulnerability Prior To 7.4.3.0

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1000031

Description

A java deserialization vulnerability is present in some versions of NetIQ Sentinel.

Observation

NetIQ Sentinel is a SIEM software that provides monitoring and management on real-time.

A java deserialization vulnerability is present in some versions of NetIQ Sentinel. The flaw lies in the Apache Commons component. Successful exploitation could allow an attacker to remotely execute arbitrary code.

20737 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 45.4

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

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

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source Email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or execute arbitrary code.

20738 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 45.4

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

Risk Level: High

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

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source Email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or execute arbitrary code.

20842 - Cisco ASA Software Local Certificate Authority Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-6431

Description

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

Observation

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

A denial of service vulnerability is present in some versions of Cisco ASA Software. The flaw lies in local Certificate Authority (CA) feature. Successful exploitation could allow an attacker to cause a reload of the affected system.

20843 - (HPSBUX03664) HP-UX BIND Service Named Remote Denial of Service Vulnerability

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

Risk Level: High

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

Description

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

Observation

HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP HP-UX. The flaws lie in BIND service. Successful exploitation could allow an attacker to cause denial of service.

20850 - (APSB16-34) Vulnerability In Creative Cloud Desktop Application

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

Risk Level: High

CVE: CVE-2016-6935

Description

A privilege escalation 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 privilege escalation vulnerability is present in some versions of Adobe Creative Cloud Desktop Application. The flaw is due to an unquoted Windows search path vulnerability. Successful exploitation could allow an attacker to gain privileges by executing malicious

binary files placed in the %SYSTEMDRIVE% directory.

The update provided by Adobe bulletin APSPB16-34 resolves these issues. The target system appears to be missing this update.

132294 - Oracle VM OVMSA-2016-0154 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0154

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000576.html>

OVM3.4
x86_64
kernel-uek-4.1.12-61.1.17.el6uek
kernel-uek-firmware-4.1.12-61.1.17.el6uek

132295 - Oracle VM OVMSA-2016-0155 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0155

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000577.html>

OVM3.3
x86_64
kernel-uek-firmware-3.8.13-118.14.1.el6uek
kernel-uek-3.8.13-118.14.1.el6uek

135165 - Oracle Solaris 11.3.11.6.0 Update Is Not Installed (CVE-2016-5544)

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

Risk Level: High

CVE: CVE-2016-5544

Description

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

SRU 11.3.11.6.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

141323 - Red Hat Enterprise Linux RHSA-2016-2582 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2582

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2582.html>

RHEL7D

x86_64

nettle-2.7.1-8.el7

nettle-debuginfo-2.7.1-8.el7

nettle-devel-2.7.1-8.el7

RHEL7WS

x86_64

nettle-2.7.1-8.el7

nettle-debuginfo-2.7.1-8.el7

nettle-devel-2.7.1-8.el7

141328 - Red Hat Enterprise Linux RHSA-2016-2672 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5198

Description

The scan detected that the host is missing the following update:
RHSA-2016-2672

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2672.html>

RHEL6D

x86_64

chromium-browser-54.0.2840.90-1.el6

chromium-browser-debuginfo-54.0.2840.90-1.el6

i386

chromium-browser-54.0.2840.90-1.el6

chromium-browser-debuginfo-54.0.2840.90-1.el6

RHEL6S

x86_64

chromium-browser-54.0.2840.90-1.el6

chromium-browser-debuginfo-54.0.2840.90-1.el6

i386

chromium-browser-54.0.2840.90-1.el6

chromium-browser-debuginfo-54.0.2840.90-1.el6

RHEL6WS

x86_64

chromium-browser-54.0.2840.90-1.el6

chromium-browser-debuginfo-54.0.2840.90-1.el6

i386

chromium-browser-54.0.2840.90-1.el6

chromium-browser-debuginfo-54.0.2840.90-1.el6

141337 - Red Hat Enterprise Linux RHSA-2016-2588 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325

Description

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

RHSA-2016-2588

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2588.html>

RHEL7D

x86_64

openssh-server-sysvinit-6.6.1p1-31.el7

openssh-clients-6.6.1p1-31.el7

openssh-askpass-6.6.1p1-31.el7

openssh-server-6.6.1p1-31.el7

openssh-debuginfo-6.6.1p1-31.el7

openssh-keycat-6.6.1p1-31.el7

openssh-6.6.1p1-31.el7

pam_ssh_agent_auth-0.9.3-9.31.el7

openssh-ldap-6.6.1p1-31.el7

RHEL7WS

x86_64

openssh-server-sysvinit-6.6.1p1-31.el7

openssh-clients-6.6.1p1-31.el7

openssh-askpass-6.6.1p1-31.el7

openssh-server-6.6.1p1-31.el7

openssh-debuginfo-6.6.1p1-31.el7
openssh-keycat-6.6.1p1-31.el7
openssh-6.6.1p1-31.el7
pam_ssh_agent_auth-0.9.3-9.31.el7
openssh-ldap-6.6.1p1-31.el7

141338 - Red Hat Enterprise Linux RHSA-2016-2598 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2598

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2598.html>

RHEL7D

x86_64
php-bcmath-5.4.16-42.el7
php-devel-5.4.16-42.el7
php-odbc-5.4.16-42.el7
php-intl-5.4.16-42.el7
php-xml-5.4.16-42.el7
php-recode-5.4.16-42.el7
php-pdo-5.4.16-42.el7
php-embedded-5.4.16-42.el7
php-pspell-5.4.16-42.el7
php-debuginfo-5.4.16-42.el7
php-enchant-5.4.16-42.el7
php-ldap-5.4.16-42.el7
php-soap-5.4.16-42.el7
php-dba-5.4.16-42.el7
php-5.4.16-42.el7
php-gd-5.4.16-42.el7
php-cli-5.4.16-42.el7
php-mysqlnd-5.4.16-42.el7
php-mbstring-5.4.16-42.el7
php-fpm-5.4.16-42.el7
php-common-5.4.16-42.el7
php-xmlrpc-5.4.16-42.el7
php-pgsql-5.4.16-42.el7
php-mysql-5.4.16-42.el7
php-snmp-5.4.16-42.el7
php-process-5.4.16-42.el7

RHEL7WS

x86_64
php-bcmath-5.4.16-42.el7
php-mbstring-5.4.16-42.el7
php-devel-5.4.16-42.el7
php-odbc-5.4.16-42.el7
php-intl-5.4.16-42.el7

php-xml-5.4.16-42.el7
php-recode-5.4.16-42.el7
php-enchanted-5.4.16-42.el7
php-embedded-5.4.16-42.el7
php-pspell-5.4.16-42.el7
php-debuginfo-5.4.16-42.el7
php-pdo-5.4.16-42.el7
php-ldap-5.4.16-42.el7
php-soap-5.4.16-42.el7
php-dba-5.4.16-42.el7
php-common-5.4.16-42.el7
php-gd-5.4.16-42.el7
php-cli-5.4.16-42.el7
php-mysqlnd-5.4.16-42.el7
php-process-5.4.16-42.el7
php-fpm-5.4.16-42.el7
php-pgsql-5.4.16-42.el7
php-xmlrpc-5.4.16-42.el7
php-mysql-5.4.16-42.el7
php-snmp-5.4.16-42.el7
php-5.4.16-42.el7

141340 - Red Hat Enterprise Linux RHSA-2016-2604 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7050

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2604.html>

RHEL7D

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

RHEL7S

noarch
resteasy-base-jaxrs-api-3.0.6-4.el7
resteasy-base-tjws-3.0.6-4.el7

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

RHEL7WS

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

141341 - Red Hat Enterprise Linux RHSA-2016-2599 Update Is Not Installed

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

Risk Level: High

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

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2599.html>

RHEL7D

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

RHEL7S

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

RHEL7WS

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

141342 - Red Hat Enterprise Linux RHSA-2016-2590 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2774

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2590.html>

RHEL7D

x86_64
dhcp-common-4.2.5-47.el7
dhcp-debuginfo-4.2.5-47.el7
dhcp-4.2.5-47.el7
dhclient-4.2.5-47.el7
dhcp-libs-4.2.5-47.el7
dhcp-devel-4.2.5-47.el7

RHEL7WS

x86_64
dhcp-common-4.2.5-47.el7
dhcp-debuginfo-4.2.5-47.el7
dhcp-4.2.5-47.el7
dhclient-4.2.5-47.el7
dhcp-libs-4.2.5-47.el7
dhcp-devel-4.2.5-47.el7

141351 - Red Hat Enterprise Linux RHSA-2016-2573 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5229, CVE-2015-5277, CVE-2016-3075

Description

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

RHSA-2016-2573

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2573.html>

RHEL7D

x86_64

glibc-utils-2.17-157.el7

glibc-debuginfo-2.17-157.el7

glibc-devel-2.17-157.el7

glibc-static-2.17-157.el7

glibc-headers-2.17-157.el7

glibc-debuginfo-common-2.17-157.el7

glibc-2.17-157.el7

nscd-2.17-157.el7

glibc-common-2.17-157.el7

RHEL7WS

x86_64

glibc-utils-2.17-157.el7

glibc-debuginfo-2.17-157.el7

glibc-devel-2.17-157.el7

glibc-static-2.17-157.el7

glibc-headers-2.17-157.el7

glibc-debuginfo-common-2.17-157.el7

glibc-2.17-157.el7

nscd-2.17-157.el7

glibc-common-2.17-157.el7

144977 - SuSE Linux 13.1 openSUSE-SU-2016:2735-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5287, CVE-2016-5288

Description

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

openSUSE-SU-2016:2735-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00016.html>

SuSE Linux 13.1

x86_64

MozillaFirefox-buildsymbols-49.0.2-128.1
MozillaFirefox-debuginfo-49.0.2-128.1
MozillaFirefox-branding-upstream-49.0.2-128.1
MozillaFirefox-devel-49.0.2-128.1
MozillaFirefox-translations-other-49.0.2-128.1
MozillaFirefox-debugsource-49.0.2-128.1
MozillaFirefox-translations-common-49.0.2-128.1
MozillaFirefox-49.0.2-128.1

i586

MozillaFirefox-buildsymbols-49.0.2-128.1
MozillaFirefox-debuginfo-49.0.2-128.1
MozillaFirefox-branding-upstream-49.0.2-128.1
MozillaFirefox-devel-49.0.2-128.1
MozillaFirefox-translations-other-49.0.2-128.1
MozillaFirefox-debugsource-49.0.2-128.1
MozillaFirefox-translations-common-49.0.2-128.1
MozillaFirefox-49.0.2-128.1

144978 - SuSE SLES 11 SP4 SUSE-SU-2016:2723-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8602

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2723-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-November/002392.html>

SuSE SLES 11 SP4

i586

libgimpprint-4.2.7-32.41.1
ghostscript-fonts-std-8.62-32.41.1
ghostscript-omni-8.62-32.41.1
ghostscript-fonts-rus-8.62-32.41.1
ghostscript-x11-8.62-32.41.1
ghostscript-fonts-other-8.62-32.41.1
ghostscript-library-8.62-32.41.1

x86_64

libgimpprint-4.2.7-32.41.1
ghostscript-fonts-std-8.62-32.41.1
ghostscript-omni-8.62-32.41.1
ghostscript-fonts-rus-8.62-32.41.1
ghostscript-x11-8.62-32.41.1
ghostscript-fonts-other-8.62-32.41.1
ghostscript-library-8.62-32.41.1

144979 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2699-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2699-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-November/002386.html>

SuSE SLES 12 SP1

x86_64

curl-7.37.0-31.1

libcurl4-7.37.0-31.1

libcurl4-debuginfo-7.37.0-31.1

libcurl4-debuginfo-32bit-7.37.0-31.1

curl-debugsource-7.37.0-31.1

libcurl4-32bit-7.37.0-31.1

curl-debuginfo-7.37.0-31.1

SuSE SLED 12 SP1

x86_64

libcurl4-32bit-7.37.0-31.1

libcurl4-7.37.0-31.1

libcurl4-debuginfo-7.37.0-31.1

libcurl4-debuginfo-32bit-7.37.0-31.1

curl-debugsource-7.37.0-31.1

curl-7.37.0-31.1

curl-debuginfo-7.37.0-31.1

144980 - SuSE SLES 11 SP4 SUSE-SU-2016:2714-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2714-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-November/002391.html>

SuSE SLES 11 SP4

i586

curl-7.19.7-1.64.1

libcurl4-7.19.7-1.64.1

x86_64
curl-7.19.7-1.64.1
libcurl4-7.19.7-1.64.1
libcurl4-32bit-7.19.7-1.64.1

144984 - SuSE Linux 13.2 openSUSE-SU-2016:2733-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5198

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2733-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00014.html>

SuSE Linux 13.2

x86_64
chromedriver-54.0.2840.90-134.1
chromedriver-debuginfo-54.0.2840.90-134.1
chromium-54.0.2840.90-134.1
chromium-debugsource-54.0.2840.90-134.1
chromium-debuginfo-54.0.2840.90-134.1
chromium-ffmpegsumo-debuginfo-54.0.2840.90-134.1
chromium-ffmpegsumo-54.0.2840.90-134.1

i586

chromedriver-54.0.2840.90-134.1
chromedriver-debuginfo-54.0.2840.90-134.1
chromium-54.0.2840.90-134.1
chromium-debugsource-54.0.2840.90-134.1
chromium-debuginfo-54.0.2840.90-134.1
chromium-ffmpegsumo-debuginfo-54.0.2840.90-134.1
chromium-ffmpegsumo-54.0.2840.90-134.1

144987 - SuSE Linux 13.2 openSUSE-SU-2016:2715-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0634, CVE-2016-7543

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2715-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00007.html>

SuSE Linux 13.2
i586
bash-devel-4.2-75.5.1
bash-debuginfo-4.2-75.5.1
libreadline6-6.2-75.5.1
bash-debugsource-4.2-75.5.1
libreadline6-debuginfo-6.2-75.5.1
bash-loadables-4.2-75.5.1
bash-4.2-75.5.1
bash-loadables-debuginfo-4.2-75.5.1
readline-devel-6.2-75.5.1

noarch
readline-doc-6.2-75.5.1
bash-doc-4.2-75.5.1
bash-lang-4.2-75.5.1

x86_64
bash-debuginfo-32bit-4.2-75.5.1
bash-loadables-4.2-75.5.1
readline-devel-6.2-75.5.1
libreadline6-debuginfo-32bit-6.2-75.5.1
readline-devel-32bit-6.2-75.5.1
libreadline6-debuginfo-6.2-75.5.1
bash-4.2-75.5.1
libreadline6-32bit-6.2-75.5.1
bash-devel-4.2-75.5.1
libreadline6-6.2-75.5.1
bash-debugsource-4.2-75.5.1
bash-debuginfo-4.2-75.5.1
bash-loadables-debuginfo-4.2-75.5.1

163182 - Oracle Enterprise Linux ELSA-2016-3635 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583

Description

The scan detected that the host is missing the following update:
ELSA-2016-3635

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006455.html>

<http://oss.oracle.com/pipermail/el-errata/2016-November/006454.html>

OEL7

x86_64
kernel-uek-debug-devel-4.1.12-61.1.17.el7uek
dtrace-modules-4.1.12-61.1.17.el7uek-0.5.3-2.el7
kernel-uek-4.1.12-61.1.17.el7uek
kernel-uek-doc-4.1.12-61.1.17.el7uek
kernel-uek-debug-4.1.12-61.1.17.el7uek
kernel-uek-devel-4.1.12-61.1.17.el7uek
kernel-uek-firmware-4.1.12-61.1.17.el7uek

OEL6
x86_64
dtrace-modules-4.1.12-61.1.17.el6uek-0.5.3-2.el6
kernel-uek-firmware-4.1.12-61.1.17.el6uek
kernel-uek-4.1.12-61.1.17.el6uek
kernel-uek-debug-4.1.12-61.1.17.el6uek
kernel-uek-devel-4.1.12-61.1.17.el6uek
kernel-uek-debug-devel-4.1.12-61.1.17.el6uek
kernel-uek-doc-4.1.12-61.1.17.el6uek

163183 - Oracle Enterprise Linux ELSA-2016-3636 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583

Description

The scan detected that the host is missing the following update:
ELSA-2016-3636

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006456.html>
<http://oss.oracle.com/pipermail/el-errata/2016-November/006457.html>

OEL7
x86_64
kernel-uek-devel-3.8.13-118.14.1.el7uek
kernel-uek-doc-3.8.13-118.14.1.el7uek
kernel-uek-debug-3.8.13-118.14.1.el7uek
kernel-uek-debug-devel-3.8.13-118.14.1.el7uek
kernel-uek-3.8.13-118.14.1.el7uek
dtrace-modules-3.8.13-118.14.1.el7uek-0.4.5-3.el7
kernel-uek-firmware-3.8.13-118.14.1.el7uek

OEL6
x86_64
kernel-uek-firmware-3.8.13-118.14.1.el6uek
kernel-uek-doc-3.8.13-118.14.1.el6uek
kernel-uek-debug-3.8.13-118.14.1.el6uek
kernel-uek-3.8.13-118.14.1.el6uek
dtrace-modules-3.8.13-118.14.1.el6uek-0.4.5-3.el6
kernel-uek-devel-3.8.13-118.14.1.el6uek
kernel-uek-debug-devel-3.8.13-118.14.1.el6uek

175030 - Scientific Linux Security ERRATA Important: pacemaker on SL6.x i386/x86_64 (1611-1159)

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

Risk Level: High

CVE: CVE-2016-7035

Description

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

Security ERRATA Important: pacemaker on SL6.x i386/x86_64 (1611-1159)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1611&L=scientific-linux-errata&F=&S=&P=1159>

SL6

x86_64

pacemaker-libs-1.1.14-8.el6_8.2
pacemaker-remote-1.1.14-8.el6_8.2
pacemaker-1.1.14-8.el6_8.2
pacemaker-libs-devel-1.1.14-8.el6_8.2
pacemaker-doc-1.1.14-8.el6_8.2
pacemaker-cli-1.1.14-8.el6_8.2
pacemaker-debuginfo-1.1.14-8.el6_8.2
pacemaker-cluster-libs-1.1.14-8.el6_8.2
pacemaker-cts-1.1.14-8.el6_8.2

i386

pacemaker-libs-1.1.14-8.el6_8.2
pacemaker-remote-1.1.14-8.el6_8.2
pacemaker-1.1.14-8.el6_8.2
pacemaker-libs-devel-1.1.14-8.el6_8.2
pacemaker-doc-1.1.14-8.el6_8.2
pacemaker-cli-1.1.14-8.el6_8.2
pacemaker-debuginfo-1.1.14-8.el6_8.2
pacemaker-cluster-libs-1.1.14-8.el6_8.2
pacemaker-cts-1.1.14-8.el6_8.2

185470 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3123-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624

Description

The scan detected that the host is missing the following update:
USN-3123-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003620.html>

Ubuntu 12.04

libcurl3_7.22.0-3ubuntu4.17
libcurl3-gnutls_7.22.0-3ubuntu4.17
libcurl3-nss_7.22.0-3ubuntu4.17

Ubuntu 16.04

libcurl3-gnutls_7.47.0-1ubuntu2.2

libcurl3_7.47.0-1ubuntu2.2
libcurl3-nss_7.47.0-1ubuntu2.2

Ubuntu 14.04

libcurl3-nss_7.35.0-1ubuntu2.10
libcurl3-gnutls_7.35.0-1ubuntu2.10
libcurl3_7.35.0-1ubuntu2.10

Ubuntu 16.10

libcurl3-gnutls_7.50.1-1ubuntu1.1
libcurl3_7.50.1-1ubuntu1.1
libcurl3-nss_7.50.1-1ubuntu1.1

185472 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3122-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7382, CVE-2016-7389

Description

The scan detected that the host is missing the following update:
USN-3122-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003619.html>

Ubuntu 12.04

nvidia-current_304.132-0ubuntu0.12.04.1
nvidia-340-updates_340.98-0ubuntu0.12.04.1
nvidia-304-updates_304.132-0ubuntu0.12.04.1
nvidia-331_340.98-0ubuntu0.12.04.1
nvidia-304_304.132-0ubuntu0.12.04.1
nvidia-340_340.98-0ubuntu0.12.04.1
nvidia-331-updates_340.98-0ubuntu0.12.04.1

Ubuntu 16.04

nvidia-340_340.98-0ubuntu0.16.04.1
nvidia-331_340.98-0ubuntu0.16.04.1
nvidia-current_304.132-0ubuntu0.16.04.2
nvidia-304-updates_304.132-0ubuntu0.16.04.2
nvidia-361_367.57-0ubuntu0.16.04.1
nvidia-304_304.132-0ubuntu0.16.04.2
nvidia-340-updates_340.98-0ubuntu0.16.04.1
nvidia-331-updates_340.98-0ubuntu0.16.04.1
nvidia-367_367.57-0ubuntu0.16.04.1

Ubuntu 14.04

nvidia-340_340.98-0ubuntu0.14.04.1
nvidia-367_367.57-0ubuntu0.14.04.1
nvidia-304_304.132-0ubuntu0.14.04.2

nvidia-331_340.98-0ubuntu0.14.04.1
nvidia-current_304.132-0ubuntu0.14.04.2
nvidia-352_367.57-0ubuntu0.14.04.1
nvidia-352-updates_367.57-0ubuntu0.14.04.1
nvidia-340-updates_340.98-0ubuntu0.14.04.1
nvidia-331-updates_340.98-0ubuntu0.14.04.1
nvidia-304-updates_304.132-0ubuntu0.14.04.2

191331 - Fedora Linux 24 FEDORA-2016-cae6456f63 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1245, CVE-2016-2342, CVE-2016-4049

Description

The scan detected that the host is missing the following update:
FEDORA-2016-cae6456f63

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

quagga-0.99.24.1-4.fc24

191339 - Fedora Linux 23 FEDORA-2016-568c7ff4f6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1245, CVE-2016-2342, CVE-2016-4049

Description

The scan detected that the host is missing the following update:
FEDORA-2016-568c7ff4f6

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 23

quagga-0.99.24.1-3.fc23

191341 - Fedora Linux 24 FEDORA-2016-a2b9adcd5c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6293

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a2b9adcd5c

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

icu-56.1-5.fc24

20743 - (VMSA-2016-0016) VMware vRealize Operations Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-7457

Description

A privilege escalation vulnerability is present in some versions of VMware vRealize Operations.

Observation

VMware vRealize Operations is the VMware's IT operations management software.

A privilege escalation vulnerability is present in some versions of VMware vRealize Operations. The flaw lies in an unknown component of the product. Successful exploitation could allow an attacker to escalate its privileges.

20745 - IBM AIX Lsmcode Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-3053

Description

A vulnerability is present in some versions of IBM AIX.

Observation

IBM AIX is an Unix-like operating system.

A vulnerability is present in some versions of IBM AIX. The flaw lies in lsmcode. Successful exploitation could allow a local attacker to gain root privileges.

20747 - Oracle iPlanet Web Server Critical Patch Update October 2016

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

Risk Level: Medium

CVE: CVE-2016-1950

Description

A vulnerability is present in some versions of Oracle iPlanet Web Server.

Observation

Oracle iPlanet Web Server is an enterprise web application server.

A vulnerability is present in some versions of Oracle iPlanet Web Server. The flaw lies in NSS. Successful exploitation could allow an attacker to execute arbitrary code.

20748 - Oracle iPlanet Web Server Critical Patch Update October 2016

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

Risk Level: Medium

CVE: CVE-2016-1950

Description

A vulnerability is present in some versions of Oracle iPlanet Web Server.

Observation

Oracle iPlanet Web Server is an enterprise web application server.

A vulnerability is present in some versions of Oracle iPlanet Web Server. The flaw lies in NSS. Successful exploitation could allow an attacker to execute arbitrary code.

20750 - Oracle iPlanet Web Proxy Server Critical Patch Update October 2016

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

Risk Level: Medium

CVE: CVE-2016-1950

Description

A vulnerability is present in some versions of Oracle iPlanet Web Proxy Server.

Observation

Oracle iPlanet Web Proxy Server is a product used to solve network congestion issues.

A vulnerability is present in some versions of Oracle iPlanet Web Proxy Server. The flaw lies in the embedded NSS component. Successful exploitation could allow an attacker to execute remote code or to cause a denial of service.

141347 - Red Hat Enterprise Linux RHSA-2016-2576 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8869

Description

The scan detected that the host is missing the following update:
RHSA-2016-2576

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2576.html>

RHEL7D

x86_64

lua-guestfs-1.32.7-3.el7
ocaml-libguestfs-devel-1.32.7-3.el7
libguestfs-gobject-1.32.7-3.el7
libguestfs-xfstools-1.32.7-3.el7
ocaml-libguestfs-1.32.7-3.el7
libguestfs-devel-1.32.7-3.el7
libguestfs-tools-c-1.32.7-3.el7
ruby-libguestfs-1.32.7-3.el7
python-libguestfs-1.32.7-3.el7
virt-dib-1.32.7-3.el7
libguestfs-rescue-1.32.7-3.el7
libguestfs-gobject-devel-1.32.7-3.el7
perl-Sys-Guestfs-1.32.7-3.el7
libguestfs-rsync-1.32.7-3.el7
libguestfs-1.32.7-3.el7
libguestfs-java-1.32.7-3.el7
libguestfs-debuginfo-1.32.7-3.el7
libguestfs-gfs2-1.32.7-3.el7
libguestfs-java-devel-1.32.7-3.el7

noarch

libguestfs-man-pages-ja-1.32.7-3.el7
libguestfs-man-pages-uk-1.32.7-3.el7
libguestfs-inspect-icons-1.32.7-3.el7
libguestfs-bash-completion-1.32.7-3.el7
libguestfs-javadoc-1.32.7-3.el7
libguestfs-tools-1.32.7-3.el7
libguestfs-gobject-doc-1.32.7-3.el7

RHEL7S

x86_64

lua-guestfs-1.32.7-3.el7
ocaml-libguestfs-devel-1.32.7-3.el7
libguestfs-gobject-1.32.7-3.el7
libguestfs-xfstools-1.32.7-3.el7
ocaml-libguestfs-1.32.7-3.el7
libguestfs-devel-1.32.7-3.el7
libguestfs-tools-c-1.32.7-3.el7
ruby-libguestfs-1.32.7-3.el7
python-libguestfs-1.32.7-3.el7
virt-dib-1.32.7-3.el7
libguestfs-rescue-1.32.7-3.el7
libguestfs-gobject-devel-1.32.7-3.el7
perl-Sys-Guestfs-1.32.7-3.el7
libguestfs-rsync-1.32.7-3.el7
libguestfs-1.32.7-3.el7
libguestfs-java-1.32.7-3.el7
virt-v2v-1.32.7-3.el7
libguestfs-debuginfo-1.32.7-3.el7
libguestfs-gfs2-1.32.7-3.el7
libguestfs-java-devel-1.32.7-3.el7

noarch

libguestfs-man-pages-ja-1.32.7-3.el7
virt-p2v-1.32.7-2.el7
libguestfs-man-pages-uk-1.32.7-3.el7
libguestfs-inspect-icons-1.32.7-3.el7
libguestfs-bash-completion-1.32.7-3.el7

libguestfs-javadoc-1.32.7-3.el7
libguestfs-tools-1.32.7-3.el7
libguestfs-gobject-doc-1.32.7-3.el7

RHEL7WS

x86_64
lua-guestfs-1.32.7-3.el7
ocaml-libguestfs-devel-1.32.7-3.el7
libguestfs-gobject-1.32.7-3.el7
libguestfs-xfstools-1.32.7-3.el7
ocaml-libguestfs-1.32.7-3.el7
libguestfs-devel-1.32.7-3.el7
libguestfs-tools-c-1.32.7-3.el7
ruby-libguestfs-1.32.7-3.el7
python-libguestfs-1.32.7-3.el7
virt-dib-1.32.7-3.el7
libguestfs-rescue-1.32.7-3.el7
libguestfs-gobject-devel-1.32.7-3.el7
perl-Sys-Guestfs-1.32.7-3.el7
libguestfs-rsync-1.32.7-3.el7
libguestfs-1.32.7-3.el7
libguestfs-java-1.32.7-3.el7
libguestfs-debuginfo-1.32.7-3.el7
libguestfs-gfs2-1.32.7-3.el7
libguestfs-java-devel-1.32.7-3.el7

noarch

libguestfs-man-pages-ja-1.32.7-3.el7
libguestfs-man-pages-uk-1.32.7-3.el7
libguestfs-inspect-icons-1.32.7-3.el7
libguestfs-bash-completion-1.32.7-3.el7
libguestfs-javadoc-1.32.7-3.el7
libguestfs-tools-1.32.7-3.el7
libguestfs-gobject-doc-1.32.7-3.el7

141357 - Red Hat Enterprise Linux RHSA-2016-2589 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4994

Description

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

RHSA-2016-2589

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2589.html>

RHEL7D

x86_64
gimp-devel-tools-2.8.16-3.el7
gimp-debuginfo-2.8.16-3.el7
gimp-2.8.16-3.el7
gimp-libs-2.8.16-3.el7
gimp-devel-2.8.16-3.el7

noarch
gimp-help-ja-2.8.2-1.el7
gimp-help-es-2.8.2-1.el7
gimp-help-ru-2.8.2-1.el7
gimp-help-ca-2.8.2-1.el7
gimp-help-fr-2.8.2-1.el7
gimp-help-en_GB-2.8.2-1.el7
gimp-help-2.8.2-1.el7
gimp-help-de-2.8.2-1.el7
gimp-help-it-2.8.2-1.el7
gimp-help-ko-2.8.2-1.el7
gimp-help-nl-2.8.2-1.el7
gimp-help-da-2.8.2-1.el7
gimp-help-nn-2.8.2-1.el7
gimp-help-sl-2.8.2-1.el7
gimp-help-zh_CN-2.8.2-1.el7
gimp-help-pt_BR-2.8.2-1.el7
gimp-help-el-2.8.2-1.el7
gimp-help-sv-2.8.2-1.el7

RHEL7WS

x86_64
gimp-devel-tools-2.8.16-3.el7
gimp-debuginfo-2.8.16-3.el7
gimp-2.8.16-3.el7
gimp-libs-2.8.16-3.el7
gimp-devel-2.8.16-3.el7

noarch
gimp-help-ja-2.8.2-1.el7
gimp-help-es-2.8.2-1.el7
gimp-help-ru-2.8.2-1.el7
gimp-help-ca-2.8.2-1.el7
gimp-help-fr-2.8.2-1.el7
gimp-help-en_GB-2.8.2-1.el7
gimp-help-2.8.2-1.el7
gimp-help-de-2.8.2-1.el7
gimp-help-it-2.8.2-1.el7
gimp-help-ko-2.8.2-1.el7
gimp-help-nl-2.8.2-1.el7
gimp-help-da-2.8.2-1.el7
gimp-help-nn-2.8.2-1.el7
gimp-help-sl-2.8.2-1.el7
gimp-help-zh_CN-2.8.2-1.el7
gimp-help-pt_BR-2.8.2-1.el7
gimp-help-el-2.8.2-1.el7
gimp-help-sv-2.8.2-1.el7

178233 - Gentoo Linux GLSA-201611-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214, CVE-2016-4324

Description

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

GLSA-201611-03

Observation

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

<https://security.gentoo.org/glsa/201611-03>

Affected packages:

app-office/libreoffice < 5.1.4.2
app-office/libreoffice-bin < 5.1.4.2
app-office/openoffice-bin < 4.1.2

20744 - Oracle Secure Global Desktop Critical Patch Update October 2016

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-5580

Description

A vulnerability is present in some versions of Oracle Secure Global Desktop.

Observation

Oracle Secure Global Desktop is a secure remote access solution.

A vulnerability is present in some versions of Oracle Secure Global Desktop. The flaw lies in Web Services component. Successful exploitation could allow an attacker to execute arbitrary code.

20849 - Apache Tomcat Multiple Vulnerabilities (October 27th 2016)

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

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in several components. Successful exploitation could allow an attacker to retrieve sensitive data or escalate privileges.

20856 - (SYM16-017) Symantec Web Gateway Management Console Interface Command Injection Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-5313

Description

A vulnerability is present in some versions of Symantec Web Gateway.

Observation

Symantec Web Gateway is a flexible Web content filtering and provides protection against data loss.

A vulnerability is present in some versions of Symantec Web Gateway. The flaw lies in the Management Console. Successful exploitation could allow an authorized management console user to bypass security measures by modifying whitelist without validation.

88821 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-308-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
SSA:2016-308-02

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.571846>

Slackware 14.0
x86_64
bind-9.9.9_P4-x86_64-1

Slackware 13.37
x86_64
bind-9.9.9_P4-x86_64-1

Slackware 14.1
x86_64
bind-9.9.9_P4-x86_64-1

Slackware 13.1
x86_64
bind-9.9.9_P4-x86_64-1

Slackware 14.2
x86_64
bind-9.10.4_P4-x86_64-1

i586
bind-9.10.4_P4-i586-1

Slackware 13.0
x86_64
bind-9.9.9_P4-x86_64-1

132293 - Oracle VM OVMSA-2016-0156 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0156

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000579.html>
<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000578.html>

OVM3.3
x86_64
libcrypt-1.4.5-12.el6_8

OVM3.4
x86_64
libcrypt-1.4.5-12.el6_8

132296 - Oracle VM OVMSA-2016-0152 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0152

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000573.html>
<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000574.html>

OVM3.3
x86_64
bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3

OVM3.4
x86_64
bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3

132297 - Oracle VM OVMSA-2016-0153 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0153

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000575.html>

OVM3.2
x86_64
bind-utils-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11

135169 - Oracle Solaris 11.3.12.4.0 Update Is Not Installed (CVE-2016-5566)

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

Risk Level: Medium

CVE: CVE-2016-5566

Description

The scan detected that the host is missing the following update:
SRU 11.3.12.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

135171 - Oracle Solaris 11.3.13.4.0 Update Is Not Installed (CVE-2016-5606)

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

Risk Level: Medium

CVE: CVE-2016-5606

Description

The scan detected that the host is missing the following update:
SRU 11.3.13.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

141320 - Red Hat Enterprise Linux RHSA-2016-2575 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-2575

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2575.html>

RHEL7D

x86_64
libcurl-7.29.0-35.el7
libcurl-devel-7.29.0-35.el7
curl-7.29.0-35.el7
curl-debuginfo-7.29.0-35.el7

RHEL7WS

x86_64
libcurl-7.29.0-35.el7
libcurl-devel-7.29.0-35.el7
curl-7.29.0-35.el7
curl-debuginfo-7.29.0-35.el7

141324 - Red Hat Enterprise Linux RHSA-2016-2592 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4455

Description

The scan detected that the host is missing the following update:
RHSA-2016-2592

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2592.html>

RHEL7D

x86_64
subscription-manager-gui-1.17.15-1.el7
subscription-manager-initial-setup-addon-1.17.15-1.el7
subscription-manager-plugin-ostree-1.17.15-1.el7
python-rhsm-certificates-1.17.9-1.el7
python-rhsm-debuginfo-1.17.9-1.el7
subscription-manager-migration-1.17.15-1.el7
subscription-manager-plugin-container-1.17.15-1.el7
subscription-manager-1.17.15-1.el7
subscription-manager-debuginfo-1.17.15-1.el7
python-rhsm-1.17.9-1.el7

noarch

subscription-manager-migration-data-2.0.31-1.el7

RHEL7WS

x86_64
subscription-manager-gui-1.17.15-1.el7
subscription-manager-initial-setup-addon-1.17.15-1.el7
subscription-manager-plugin-ostree-1.17.15-1.el7
python-rhsm-certificates-1.17.9-1.el7
python-rhsm-debuginfo-1.17.9-1.el7
subscription-manager-migration-1.17.15-1.el7
subscription-manager-plugin-container-1.17.15-1.el7
subscription-manager-1.17.15-1.el7

subscription-manager-debuginfo-1.17.15-1.el7
python-rhsm-1.17.9-1.el7

noarch
subscription-manager-migration-data-2.0.31-1.el7

141326 - Red Hat Enterprise Linux RHSA-2016-2674 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2674.html>

RHEL6S

i386
libgcrypt-debuginfo-1.4.5-12.el6_8
libgcrypt-1.4.5-12.el6_8
libgcrypt-devel-1.4.5-12.el6_8

x86_64

libgcrypt-debuginfo-1.4.5-12.el6_8
libgcrypt-1.4.5-12.el6_8
libgcrypt-devel-1.4.5-12.el6_8

RHEL6WS

x86_64
libgcrypt-debuginfo-1.4.5-12.el6_8
libgcrypt-1.4.5-12.el6_8
libgcrypt-devel-1.4.5-12.el6_8

i386

libgcrypt-debuginfo-1.4.5-12.el6_8
libgcrypt-1.4.5-12.el6_8
libgcrypt-devel-1.4.5-12.el6_8

RHEL7D

x86_64
libgcrypt-1.5.3-13.el7_3.1
libgcrypt-debuginfo-1.5.3-13.el7_3.1
libgcrypt-devel-1.5.3-13.el7_3.1

RHEL6D

x86_64
libgcrypt-debuginfo-1.4.5-12.el6_8
libgcrypt-1.4.5-12.el6_8
libgcrypt-devel-1.4.5-12.el6_8

i386

libgcrypt-debuginfo-1.4.5-12.el6_8

libgrypt-1.4.5-12.el6_8
libgrypt-devel-1.4.5-12.el6_8

RHEL7WS

x86_64
libgrypt-1.5.3-13.el7_3.1
libgrypt-debuginfo-1.5.3-13.el7_3.1
libgrypt-devel-1.5.3-13.el7_3.1

141327 - Red Hat Enterprise Linux RHSA-2016-2141 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

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

RHSA-2016-2141

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2141.html>

RHEL5S

i386
bind-utils-9.3.6-25.P1.el5_11.11
bind-devel-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11
bind-libbind-devel-9.3.6-25.P1.el5_11.11
caching-nameserver-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11
bind-chroot-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-debuginfo-9.3.6-25.P1.el5_11.11

x86_64

bind-utils-9.3.6-25.P1.el5_11.11
bind-devel-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11
bind-libbind-devel-9.3.6-25.P1.el5_11.11
caching-nameserver-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11
bind-chroot-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-debuginfo-9.3.6-25.P1.el5_11.11

RHEL6D

x86_64
bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-debuginfo-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

i386
bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-debuginfo-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

RHEL6S

i386
bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-debuginfo-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

x86_64

bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-debuginfo-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

RHEL6WS

x86_64
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-debuginfo-9.8.2-0.47.rc1.el6_8.3
bind-utils-9.8.2-0.47.rc1.el6_8.3

i386

bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-debuginfo-9.8.2-0.47.rc1.el6_8.3
bind-utils-9.8.2-0.47.rc1.el6_8.3

RHEL5D

x86_64
bind-libs-9.3.6-25.P1.el5_11.11
bind-utils-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-debuginfo-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11

i386

bind-libs-9.3.6-25.P1.el5_11.11
bind-utils-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-debuginfo-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11

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

Risk Level: Medium

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

Description

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

RHSA-2016-2594

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2594.html>

RHEL7D

x86_64

389-ds-base-1.3.5.10-11.el7

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

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

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

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

RHEL7WS

x86_64

389-ds-base-1.3.5.10-11.el7

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

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

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

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

141334 - Red Hat Enterprise Linux RHSA-2016-2615 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

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

RHSA-2016-2615

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2615.html>

RHEL7D

x86_64

bind-lite-devel-9.9.4-38.el7_3

bind-sdb-9.9.4-38.el7_3

bind-pkcs11-utils-9.9.4-38.el7_3

bind-debuginfo-9.9.4-38.el7_3

bind-chroot-9.9.4-38.el7_3

bind-devel-9.9.4-38.el7_3

bind-pkcs11-devel-9.9.4-38.el7_3

bind-pkcs11-libs-9.9.4-38.el7_3

bind-9.9.4-38.el7_3
bind-libs-9.9.4-38.el7_3
bind-utils-9.9.4-38.el7_3
bind-libs-lite-9.9.4-38.el7_3
bind-sdb-chroot-9.9.4-38.el7_3
bind-pkcs11-9.9.4-38.el7_3

noarch
bind-license-9.9.4-38.el7_3

RHEL7WS

x86_64
bind-devel-9.9.4-38.el7_3
bind-pkcs11-libs-9.9.4-38.el7_3
bind-sdb-9.9.4-38.el7_3
bind-pkcs11-utils-9.9.4-38.el7_3
bind-debuginfo-9.9.4-38.el7_3
bind-chroot-9.9.4-38.el7_3
bind-pkcs11-9.9.4-38.el7_3
bind-sdb-chroot-9.9.4-38.el7_3
bind-lite-devel-9.9.4-38.el7_3
bind-9.9.4-38.el7_3
bind-libs-9.9.4-38.el7_3
bind-pkcs11-devel-9.9.4-38.el7_3
bind-libs-lite-9.9.4-38.el7_3
bind-utils-9.9.4-38.el7_3

noarch
bind-license-9.9.4-38.el7_3

141335 - Red Hat Enterprise Linux RHSA-2016-2606 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2606.html>

RHEL7D

x86_64
postgresql-plpython-9.2.18-1.el7
postgresql-server-9.2.18-1.el7
postgresql-devel-9.2.18-1.el7
postgresql-9.2.18-1.el7
postgresql-contrib-9.2.18-1.el7
postgresql-pltcl-9.2.18-1.el7
postgresql-docs-9.2.18-1.el7
postgresql-upgrade-9.2.18-1.el7
postgresql-debuginfo-9.2.18-1.el7
postgresql-libs-9.2.18-1.el7

postgresql-plperl-9.2.18-1.el7
postgresql-test-9.2.18-1.el7

RHEL7WS

x86_64

postgresql-plpython-9.2.18-1.el7
postgresql-server-9.2.18-1.el7
postgresql-devel-9.2.18-1.el7
postgresql-9.2.18-1.el7
postgresql-contrib-9.2.18-1.el7
postgresql-pltcl-9.2.18-1.el7
postgresql-docs-9.2.18-1.el7
postgresql-upgrade-9.2.18-1.el7
postgresql-debuginfo-9.2.18-1.el7
postgresql-libs-9.2.18-1.el7
postgresql-plperl-9.2.18-1.el7
postgresql-test-9.2.18-1.el7

141336 - Red Hat Enterprise Linux RHSA-2016-2603 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5361

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2603.html>

RHEL7D

x86_64

libreswan-debuginfo-3.15-8.el7
libreswan-3.15-8.el7

RHEL7WS

x86_64

libreswan-debuginfo-3.15-8.el7
libreswan-3.15-8.el7

141348 - Red Hat Enterprise Linux RHSA-2016-2583 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2015-5194, CVE-2015-5195, CVE-2015-5196, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7974, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8158

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2583.html>

RHEL7D

x86_64
ntpdate-4.2.6p5-25.el7
ntp-debuginfo-4.2.6p5-25.el7
snmp-4.2.6p5-25.el7
ntp-4.2.6p5-25.el7

noarch

ntp-doc-4.2.6p5-25.el7
ntp-perl-4.2.6p5-25.el7

RHEL7WS

x86_64
ntpdate-4.2.6p5-25.el7
ntp-debuginfo-4.2.6p5-25.el7
snmp-4.2.6p5-25.el7
ntp-4.2.6p5-25.el7

noarch

ntp-doc-4.2.6p5-25.el7
ntp-perl-4.2.6p5-25.el7

141352 - Red Hat Enterprise Linux RHSA-2016-2597 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5410

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2597.html>

RHEL7D

noarch
python-firewall-0.4.3.2-8.el7
firewall-applet-0.4.3.2-8.el7
firewalld-filesystem-0.4.3.2-8.el7
firewalld-0.4.3.2-8.el7
firewall-config-0.4.3.2-8.el7

RHEL7S

noarch
python-firewall-0.4.3.2-8.el7
firewall-applet-0.4.3.2-8.el7
firewalld-filesystem-0.4.3.2-8.el7
firewalld-0.4.3.2-8.el7

firewall-config-0.4.3.2-8.el7

RHEL7WS

noarch

python-firewall-0.4.3.2-8.el7

firewall-applet-0.4.3.2-8.el7

firewalld-filesystem-0.4.3.2-8.el7

firewalld-0.4.3.2-8.el7

firewall-config-0.4.3.2-8.el7

141356 - Red Hat Enterprise Linux RHSA-2016-2600 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2569, CVE-2016-2570, CVE-2016-2571, CVE-2016-2572, CVE-2016-3948

Description

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

RHSA-2016-2600

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2600.html>

RHEL7WS

x86_64

squid-sysvinit-3.5.20-2.el7

squid-migration-script-3.5.20-2.el7

squid-3.5.20-2.el7

squid-debuginfo-3.5.20-2.el7

141358 - Red Hat Enterprise Linux RHSA-2016-2142 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

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

RHSA-2016-2142

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2142.html>

RHEL5S

i386

bind97-chroot-9.7.0-21.P2.el5_11.9

bind97-debuginfo-9.7.0-21.P2.el5_11.9

bind97-libs-9.7.0-21.P2.el5_11.9

bind97-9.7.0-21.P2.el5_11.9

bind97-utils-9.7.0-21.P2.el5_11.9

bind97-devel-9.7.0-21.P2.el5_11.9

x86_64

bind97-chroot-9.7.0-21.P2.el5_11.9

bind97-debuginfo-9.7.0-21.P2.el5_11.9

bind97-libs-9.7.0-21.P2.el5_11.9

bind97-9.7.0-21.P2.el5_11.9

bind97-utils-9.7.0-21.P2.el5_11.9

bind97-devel-9.7.0-21.P2.el5_11.9

144982 - SuSE Linux 13.2 openSUSE-SU-2016:2738-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2738-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00019.html>

SuSE Linux 13.2

i586

bind-utils-debuginfo-9.9.6P1-2.25.1

bind-utils-9.9.6P1-2.25.1

bind-debugsource-9.9.6P1-2.25.1

bind-debuginfo-9.9.6P1-2.25.1

bind-chrootenv-9.9.6P1-2.25.1

bind-devel-9.9.6P1-2.25.1

bind-libs-9.9.6P1-2.25.1

bind-libs-debuginfo-9.9.6P1-2.25.1

bind-lwresd-9.9.6P1-2.25.1

bind-9.9.6P1-2.25.1

bind-lwresd-debuginfo-9.9.6P1-2.25.1

noarch

bind-doc-9.9.6P1-2.25.1

x86_64

bind-libs-32bit-9.9.6P1-2.25.1

bind-devel-9.9.6P1-2.25.1

bind-libs-9.9.6P1-2.25.1

bind-9.9.6P1-2.25.1

bind-libs-debuginfo-32bit-9.9.6P1-2.25.1

bind-debugsource-9.9.6P1-2.25.1

bind-debuginfo-9.9.6P1-2.25.1

bind-utils-debuginfo-9.9.6P1-2.25.1

bind-libs-debuginfo-9.9.6P1-2.25.1

bind-lwresd-9.9.6P1-2.25.1

bind-chrootenv-9.9.6P1-2.25.1

bind-lwresd-debuginfo-9.9.6P1-2.25.1

bind-utils-9.9.6P1-2.25.1

144985 - SuSE SLES 11 SP4 SUSE-SU-2016:2706-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2706-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-November/002389.html>

SuSE SLES 11 SP4

i586

bind-utils-9.9.6P1-0.33.1

bind-doc-9.9.6P1-0.33.1

bind-chrootenv-9.9.6P1-0.33.1

bind-libs-9.9.6P1-0.33.1

bind-9.9.6P1-0.33.1

x86_64

bind-chrootenv-9.9.6P1-0.33.1

bind-utils-9.9.6P1-0.33.1

bind-libs-32bit-9.9.6P1-0.33.1

bind-libs-9.9.6P1-0.33.1

bind-9.9.6P1-0.33.1

bind-doc-9.9.6P1-0.33.1

160163 - CentOS 5 CESA-2016-2142 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
CESA-2016-2142

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-November/022138.html>

CentOS 5

x86_64

bind97-utils-9.7.0-21.P2.el5_11.9

bind97-libs-9.7.0-21.P2.el5_11.9

bind97-devel-9.7.0-21.P2.el5_11.9

bind97-chroot-9.7.0-21.P2.el5_11.9

bind97-9.7.0-21.P2.el5_11.9

i386
bind97-utils-9.7.0-21.P2.el5_11.9
bind97-libs-9.7.0-21.P2.el5_11.9
bind97-devel-9.7.0-21.P2.el5_11.9
bind97-chroot-9.7.0-21.P2.el5_11.9
bind97-9.7.0-21.P2.el5_11.9

160164 - CentOS 5, 6 CESA-2016-2141 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

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

CESA-2016-2141

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-November/022136.html>

<http://lists.centos.org/pipermail/centos-announce/2016-November/022137.html>

CentOS 5

x86_64

bind-devel-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11
bind-libbind-devel-9.3.6-25.P1.el5_11.11
caching-nameserver-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11
bind-chroot-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-utils-9.3.6-25.P1.el5_11.11

i386

bind-devel-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11
bind-libbind-devel-9.3.6-25.P1.el5_11.11
caching-nameserver-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11
bind-chroot-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-utils-9.3.6-25.P1.el5_11.11

CentOS 6

x86_64

bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

i686

bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3

bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

163184 - Oracle Enterprise Linux ELSA-2016-2141 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
ELSA-2016-2141

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006452.html>

<http://oss.oracle.com/pipermail/el-errata/2016-November/006451.html>

OEL5

i386

bind-devel-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11
bind-libbind-devel-9.3.6-25.P1.el5_11.11
caching-nameserver-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11
bind-chroot-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-utils-9.3.6-25.P1.el5_11.11

x86_64

bind-devel-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11
bind-libbind-devel-9.3.6-25.P1.el5_11.11
caching-nameserver-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11
bind-chroot-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-utils-9.3.6-25.P1.el5_11.11

OEL6

x86_64

bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

i386

bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

163186 - Oracle Enterprise Linux ELSA-2016-2674 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

Description

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

ELSA-2016-2674

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-November/006464.html>

OEL6

x86_64

libgcrypt-devel-1.4.5-12.el6_8

libgcrypt-1.4.5-12.el6_8

i386

libgcrypt-devel-1.4.5-12.el6_8

libgcrypt-1.4.5-12.el6_8

163187 - Oracle Enterprise Linux ELSA-2016-2142 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

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

ELSA-2016-2142

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-November/006453.html>

OEL5

i386

bind97-utils-9.7.0-21.P2.el5_11.9

bind97-libs-9.7.0-21.P2.el5_11.9

bind97-devel-9.7.0-21.P2.el5_11.9

bind97-chroot-9.7.0-21.P2.el5_11.9

bind97-9.7.0-21.P2.el5_11.9

x86_64

bind97-utils-9.7.0-21.P2.el5_11.9

bind97-libs-9.7.0-21.P2.el5_11.9

bind97-devel-9.7.0-21.P2.el5_11.9

bind97-chroot-9.7.0-21.P2.el5_11.9

bind97-9.7.0-21.P2.el5_11.9

175029 - Scientific Linux Security ERRATA Moderate: libgcrypt on SL6.x i386/x86_64 (1611-1490)

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

Risk Level: Medium

CVE: CVE-2016-6313

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libgcrypt on SL6.x i386/x86_64 (1611-1490)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1611&L=scientific-linux-errata&F=&S=&P=1490>

SL6
x86_64
libgcrypt-debuginfo-1.4.5-12.el6_8
libgcrypt-1.4.5-12.el6_8
libgcrypt-devel-1.4.5-12.el6_8

i386
libgcrypt-debuginfo-1.4.5-12.el6_8
libgcrypt-1.4.5-12.el6_8
libgcrypt-devel-1.4.5-12.el6_8

175032 - Scientific Linux Security ERRATA Important: bind on SL5.x, SL6.x i386/x86_64 (1611-79)

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL5.x, SL6.x i386/x86_64 (1611-79)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1611&L=scientific-linux-errata&F=&S=&P=79>

SL6
x86_64
bind-utils-9.8.2-0.47.rc1.el6_8.3
bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-debuginfo-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

i386
bind-utils-9.8.2-0.47.rc1.el6_8.3

bind-9.8.2-0.47.rc1.el6_8.3
bind-chroot-9.8.2-0.47.rc1.el6_8.3
bind-debuginfo-9.8.2-0.47.rc1.el6_8.3
bind-sdb-9.8.2-0.47.rc1.el6_8.3
bind-libs-9.8.2-0.47.rc1.el6_8.3
bind-devel-9.8.2-0.47.rc1.el6_8.3

SL5

x86_64

bind-utils-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11
bind-devel-9.3.6-25.P1.el5_11.11
bind-libbind-devel-9.3.6-25.P1.el5_11.11
bind-chroot-9.3.6-25.P1.el5_11.11
caching-nameserver-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-debuginfo-9.3.6-25.P1.el5_11.11

i386

bind-utils-9.3.6-25.P1.el5_11.11
bind-libs-9.3.6-25.P1.el5_11.11
bind-devel-9.3.6-25.P1.el5_11.11
bind-libbind-devel-9.3.6-25.P1.el5_11.11
bind-chroot-9.3.6-25.P1.el5_11.11
caching-nameserver-9.3.6-25.P1.el5_11.11
bind-9.3.6-25.P1.el5_11.11
bind-sdb-9.3.6-25.P1.el5_11.11
bind-debuginfo-9.3.6-25.P1.el5_11.11

175033 - Scientific Linux Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1611-409)

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1611-409)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1611&L=scientific-linux-errata&F=&S=&P=409>

SL5

x86_64

bind97-chroot-9.7.0-21.P2.el5_11.9
bind97-debuginfo-9.7.0-21.P2.el5_11.9
bind97-libs-9.7.0-21.P2.el5_11.9
bind97-9.7.0-21.P2.el5_11.9
bind97-utils-9.7.0-21.P2.el5_11.9
bind97-devel-9.7.0-21.P2.el5_11.9

i386

bind97-chroot-9.7.0-21.P2.el5_11.9
bind97-debuginfo-9.7.0-21.P2.el5_11.9

bind97-libs-9.7.0-21.P2.el5_11.9
bind97-9.7.0-21.P2.el5_11.9
bind97-utils-9.7.0-21.P2.el5_11.9
bind97-devel-9.7.0-21.P2.el5_11.9

20752 - Oracle Application Express Critical Patch Update October 2016

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

Risk Level: Medium

CVE: CVE-2010-5312

Description

Multiple vulnerabilities are present in some versions of Oracle Application Express.

Observation

Oracle Application Express is an Oracle web-based software development environment that runs on an Oracle database.

Multiple vulnerabilities are present in some versions of Oracle Application Express. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code.

20753 - Oracle Business Intelligence Publisher Edition Critical Patch Update October 2016

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

Risk Level: Medium

CVE: CVE-2016-3473

Description

An information disclosure vulnerability is present in some versions of Oracle Business Intelligence Publisher.

Observation

Oracle Business Intelligence Publisher is the Oracle Business Intelligence reporting tool.

An information disclosure vulnerability is present in some versions of Oracle Business Intelligence Publisher. The flaw lies in an unknown Oracle Business Intelligence Publisher component. Successful exploitation by a remote authenticated attacker could affect confidentiality.

135164 - Oracle Solaris 11.3.12.4.0 Update Is Not Installed (CVE-2016-5487)

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

Risk Level: Medium

CVE: CVE-2016-5487

Description

The scan detected that the host is missing the following update:
SRU 11.3.12.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

135166 - Oracle Solaris 11.3.12.4.0 Update Is Not Installed (CVE-2016-5553)

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

Risk Level: Medium

CVE: CVE-2016-5553

Description

The scan detected that the host is missing the following update:
SRU 11.3.12.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

135167 - Oracle Solaris 11.3.11.6.0 Update Is Not Installed (CVE-2016-5559)

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

Risk Level: Medium

CVE: CVE-2016-5559

Description

The scan detected that the host is missing the following update:
SRU 11.3.11.6.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

135170 - Oracle Solaris 11.3.12.4.0 Update Is Not Installed (CVE-2016-5576)

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

Risk Level: Medium

CVE: CVE-2016-5576

Description

The scan detected that the host is missing the following update:
SRU 11.3.12.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

141329 - Red Hat Enterprise Linux RHSA-2016-2577 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2577.html>

RHEL7D

x86_64

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

RHEL7S

ppc64

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

RHEL7WS

x86_64

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

141330 - Red Hat Enterprise Linux RHSA-2016-2587 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4971

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2587.html>

RHEL7D

x86_64

wget-debuginfo-1.14-13.el7

wget-1.14-13.el7

RHEL7WS

x86_64

wget-debuginfo-1.14-13.el7

wget-1.14-13.el7

141343 - Red Hat Enterprise Linux RHSA-2016-2601 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5384

Description

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

RHSA-2016-2601

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2601.html>

RHEL7D

x86_64

fontconfig-2.10.95-10.el7

fontconfig-devel-2.10.95-10.el7

fontconfig-debuginfo-2.10.95-10.el7

noarch

fontconfig-devel-doc-2.10.95-10.el7

RHEL7S

noarch

fontconfig-devel-doc-2.10.95-10.el7

RHEL7WS

x86_64

fontconfig-2.10.95-10.el7

fontconfig-devel-2.10.95-10.el7

fontconfig-debuginfo-2.10.95-10.el7

noarch

fontconfig-devel-doc-2.10.95-10.el7

141346 - Red Hat Enterprise Linux RHSA-2016-2591 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2591.html>

RHEL7D

x86_64

libkadm5-1.14.1-26.el7

krb5-devel-1.14.1-26.el7

krb5-debuginfo-1.14.1-26.el7

krb5-libs-1.14.1-26.el7

krb5-server-ldap-1.14.1-26.el7

krb5-pkinit-1.14.1-26.el7

krb5-workstation-1.14.1-26.el7

krb5-server-1.14.1-26.el7

RHEL7WS
x86_64
libkadm5-1.14.1-26.el7
krb5-server-1.14.1-26.el7
krb5-debuginfo-1.14.1-26.el7
krb5-libs-1.14.1-26.el7
krb5-server-ldap-1.14.1-26.el7
krb5-pkinit-1.14.1-26.el7
krb5-workstation-1.14.1-26.el7
krb5-devel-1.14.1-26.el7

141354 - Red Hat Enterprise Linux RHSA-2016-2610 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7795

Description

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

RHSA-2016-2610

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2610.html>

RHEL7D
x86_64
systemd-219-30.el7_3.3
systemd-debuginfo-219-30.el7_3.3
systemd-sysv-219-30.el7_3.3
systemd-libs-219-30.el7_3.3
systemd-networkd-219-30.el7_3.3
systemd-journal-gateway-219-30.el7_3.3
systemd-python-219-30.el7_3.3
systemd-resolved-219-30.el7_3.3
libgudev1-devel-219-30.el7_3.3
systemd-devel-219-30.el7_3.3
libgudev1-219-30.el7_3.3

RHEL7WS
x86_64
libgudev1-devel-219-30.el7_3.3
systemd-debuginfo-219-30.el7_3.3
systemd-devel-219-30.el7_3.3
systemd-libs-219-30.el7_3.3
systemd-sysv-219-30.el7_3.3
systemd-journal-gateway-219-30.el7_3.3
systemd-python-219-30.el7_3.3
systemd-networkd-219-30.el7_3.3
systemd-resolved-219-30.el7_3.3
systemd-219-30.el7_3.3
libgudev1-219-30.el7_3.3

20845 - IBM WebSphere MQ Invalid Client Protocol Flows Denial Of Service Vulnerability

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0379

Description

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

Observation

IBM WebSphere MQ is a messaging solution.

A vulnerability is present in some versions of IBM WebSphere MQ. The flaw is due to incorrect handling of MQ protocol flows. Successful exploitation could allow an attacker to cause a denial of service.

88822 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-308-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-8625

Description

The scan detected that the host is missing the following update:
SSA:2016-308-01

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.661139>

Slackware 14.0
x86_64
curl-7.51.0-x86_64-1

Slackware 13.37
x86_64
curl-7.51.0-x86_64-1

Slackware 14.1
x86_64
curl-7.51.0-x86_64-1

Slackware 13.1
x86_64
curl-7.51.0-x86_64-1

Slackware 14.2
x86_64
curl-7.51.0-x86_64-1

i586
curl-7.51.0-i586-1

Slackware 13.0
x86_64
curl-7.51.0-x86_64-1

130620 - Debian Linux 8.0 DSA-3706-1 Update Is Not Installed

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

Risk Level: Low

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

Description

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

DSA-3706-1

Observation

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

For more information see:

<http://www.debian.org/security/2016/dsa-3706>

Debian 8.0

all

mysql-source-5.5_5.5.53-0+deb8u1

mysql-server_5.5.53-0+deb8u1

libmysqld-pic_5.5.53-0+deb8u1

libmysqld-dev_5.5.53-0+deb8u1

mysql-common_5.5.53-0+deb8u1

mysql-testsuite-5.5_5.5.53-0+deb8u1

mysql-server-core-5.5_5.5.53-0+deb8u1

mysql-client_5.5.53-0+deb8u1

mysql-client-5.5_5.5.53-0+deb8u1

mysql-server-5.5_5.5.53-0+deb8u1

mysql-testsuite_5.5.53-0+deb8u1

libmysqlclient18_5.5.53-0+deb8u1

libmysqlclient-dev_5.5.53-0+deb8u1

130621 - Debian Linux 8.0 DSA-3704-1 Update Is Not Installed

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

Risk Level: Low

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

Description

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

DSA-3704-1

Observation

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

For more information see:

<http://www.debian.org/security/2016/dsa-3704>

Debian 8.0

all

memcached_1.4.21-1.1+deb8u1

130622 - Debian Linux 8.0 DSA-3705-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
DSA-3705-1

Observation

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

<http://www.debian.org/security/2016/dsa-3705>

Debian 8.0
all
curl_7.38.0-4+deb8u5

130623 - Debian Linux 8.0 DSA-3708-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-3708-1

Observation

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

<http://www.debian.org/security/2016/dsa-3708>

Debian 8.0
all
mat_0.5.2-3+deb8u1

141333 - Red Hat Enterprise Linux RHSA-2016-2605 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5011

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2605.html>

RHEL7D
x86_64
libmount-2.23.2-33.el7
libuuid-2.23.2-33.el7
libmount-devel-2.23.2-33.el7
uuid-2.23.2-33.el7
libblkid-devel-2.23.2-33.el7
util-linux-debuginfo-2.23.2-33.el7
libblkid-2.23.2-33.el7
libuuid-devel-2.23.2-33.el7
util-linux-2.23.2-33.el7

RHEL7WS
x86_64
libmount-2.23.2-33.el7
libuuid-2.23.2-33.el7
libmount-devel-2.23.2-33.el7
util-linux-debuginfo-2.23.2-33.el7
libblkid-2.23.2-33.el7
uuid-2.23.2-33.el7
libblkid-devel-2.23.2-33.el7
libuuid-devel-2.23.2-33.el7
util-linux-2.23.2-33.el7

141345 - Red Hat Enterprise Linux RHSA-2016-2602 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3099

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2602.html>

RHEL7D
x86_64
mod_nss-debuginfo-1.0.14-7.el7
mod_nss-1.0.14-7.el7

RHEL7WS
x86_64
mod_nss-debuginfo-1.0.14-7.el7
mod_nss-1.0.14-7.el7

141350 - Red Hat Enterprise Linux RHSA-2016-2581 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-0764

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2581.html>

RHEL7D

x86_64

NetworkManager-libnm-devel-1.4.0-12.el7
NetworkManager-adsl-1.4.0-12.el7
network-manager-applet-1.4.0-2.el7
NetworkManager-wwan-1.4.0-12.el7
NetworkManager-wifi-1.4.0-12.el7
libnma-devel-1.4.0-2.el7
libnl3-devel-3.2.28-2.el7
libnl3-doc-3.2.28-2.el7
NetworkManager-tui-1.4.0-12.el7
NetworkManager-1.4.0-12.el7
libnl3-cli-3.2.28-2.el7
NetworkManager-libreswan-gnome-1.2.4-1.el7
NetworkManager-libreswan-1.2.4-1.el7
NetworkManager-team-1.4.0-12.el7
NetworkManager-debuginfo-1.4.0-12.el7
libnl3-debuginfo-3.2.28-2.el7
NetworkManager-bluetooth-1.4.0-12.el7
NetworkManager-glib-devel-1.4.0-12.el7
NetworkManager-glib-1.4.0-12.el7
libnm-gtk-devel-1.4.0-2.el7
libnm-gtk-1.4.0-2.el7
NetworkManager-libreswan-debuginfo-1.2.4-1.el7
network-manager-applet-debuginfo-1.4.0-2.el7
NetworkManager-config-server-1.4.0-12.el7
nm-connection-editor-1.4.0-2.el7
NetworkManager-libnm-1.4.0-12.el7
libnma-1.4.0-2.el7
libnl3-3.2.28-2.el7

noarch

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

RHEL7WS

x86_64

NetworkManager-libnm-devel-1.4.0-12.el7
NetworkManager-adsl-1.4.0-12.el7
network-manager-applet-1.4.0-2.el7
NetworkManager-wwan-1.4.0-12.el7
NetworkManager-wifi-1.4.0-12.el7
libnma-devel-1.4.0-2.el7
libnl3-devel-3.2.28-2.el7
libnl3-doc-3.2.28-2.el7
NetworkManager-tui-1.4.0-12.el7
NetworkManager-1.4.0-12.el7
libnl3-cli-3.2.28-2.el7
NetworkManager-libreswan-gnome-1.2.4-1.el7
NetworkManager-libreswan-1.2.4-1.el7
NetworkManager-team-1.4.0-12.el7
NetworkManager-debuginfo-1.4.0-12.el7

libnl3-debuginfo-3.2.28-2.el7
NetworkManager-bluetooth-1.4.0-12.el7
NetworkManager-glib-devel-1.4.0-12.el7
NetworkManager-glib-1.4.0-12.el7
libnm-gtk-devel-1.4.0-2.el7
libnm-gtk-1.4.0-2.el7
NetworkManager-libreswan-debuginfo-1.2.4-1.el7
network-manager-applet-debuginfo-1.4.0-2.el7
NetworkManager-config-server-1.4.0-12.el7
nm-connection-editor-1.4.0-2.el7
NetworkManager-libnm-1.4.0-12.el7
libnma-1.4.0-2.el7
libnl3-3.2.28-2.el7

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

141353 - Red Hat Enterprise Linux RHSA-2016-2593 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7091

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2593.html>

RHEL7D
x86_64
sudo-1.8.6p7-20.el7
sudo-debuginfo-1.8.6p7-20.el7
sudo-devel-1.8.6p7-20.el7

RHEL7WS
x86_64
sudo-1.8.6p7-20.el7
sudo-debuginfo-1.8.6p7-20.el7
sudo-devel-1.8.6p7-20.el7

182166 - FreeBSD chromium Out-of-bounds Memory Access (ae9cb9b8-a203-11e6-a265-3065ec8fd3ec)

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

Risk Level: Low

CVE: CVE-2016-5198

Description

The scan detected that the host is missing the following update:
chromium -- out-of-bounds memory access (ae9cb9b8-a203-11e6-a265-3065ec8fd3ec)

Observation

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

<http://www.vuxml.org/freebsd/ae9cb9b8-a203-11e6-a265-3065ec8fd3ec.html>

Affected packages:

chromium < 54.0.2840.90
chromium-npapi < 54.0.2840.90
chromium-pulse < 54.0.2840.90

185469 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3113-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1586, CVE-2016-5181, CVE-2016-5182, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5192, CVE-2016-5194

Description

The scan detected that the host is missing the following update:
USN-3113-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003616.html>

Ubuntu 16.04

liboxideqtcore0_1.18.3-0ubuntu0.16.04.1

Ubuntu 14.04

liboxideqtcore0_1.18.3-0ubuntu0.14.04.1

Ubuntu 16.10

liboxideqtcore0_1.18.3-0ubuntu0.16.10.1

185473 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3120-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
USN-3120-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003617.html>

Ubuntu 12.04

memcached_1.4.13-0ubuntu2.2

Ubuntu 16.04

memcached_1.4.25-2ubuntu1.2

Ubuntu 14.04

memcached_1.4.14-0ubuntu9.1

Ubuntu 16.10

memcached_1.4.25-2ubuntu2.1

191327 - Fedora Linux 24 FEDORA-2016-3dad5dfd03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7977, CVE-2016-8602

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3dad5dfd03

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

ghostscript-9.20-5.fc24

191328 - Fedora Linux 24 FEDORA-2016-3113e71193 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8614, CVE-2016-8628

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3113e71193

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

ansible-2.2.0.0-3.fc24

191329 - Fedora Linux 24 FEDORA-2016-fa03795843 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5287, CVE-2016-5288

Description

The scan detected that the host is missing the following update:
FEDORA-2016-fa03795843

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

firefox-49.0.2-1.fc24

191330 - Fedora Linux 24 FEDORA-2016-160ec6525e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9085

Description

The scan detected that the host is missing the following update:
FEDORA-2016-160ec6525e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

libwebp-0.5.1-2.fc24

191332 - Fedora Linux 24 FEDORA-2016-96d276367e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9083, CVE-2016-9084

Description

The scan detected that the host is missing the following update:
FEDORA-2016-96d276367e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

kernel-4.8.6-201.fc24

191333 - Fedora Linux 24 FEDORA-2016-e8e8cdb4ed Update Is Not Installed

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

Risk Level: Low

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

Description

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

FEDORA-2016-e8e8cdb4ed

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

curl-7.47.1-9.fc24

191334 - Fedora Linux 24 FEDORA-2016-8660c7656f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5416

Description

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

FEDORA-2016-8660c7656f

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

389-ds-base-1.3.5.15-1.fc24

191335 - Fedora Linux 23 FEDORA-2016-3f235e39d0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5287, CVE-2016-5288

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3f235e39d0

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 23

firefox-49.0.2-1.fc23

191336 - Fedora Linux 24 FEDORA-2016-c9d15bbcbb Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
FEDORA-2016-c9d15bbcbb

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

kdepimlibs-4.14.10-15.fc24

191337 - Fedora Linux 23 FEDORA-2016-c1bb366e5b 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-c1bb366e5b

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 23

dbus-1.10.12-1.fc23

191338 - Fedora Linux 24 FEDORA-2016-73054cfeeb 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-2016-73054cfeeb

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

java-1.8.0-openjdk-aarch32-1.8.0.102-7.160812.fc24

191340 - Fedora Linux 23 FEDORA-2016-2a159ef513 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7035

Description

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

FEDORA-2016-2a159ef513

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 23

pacemaker-1.1.15-2.fc23

191342 - Fedora Linux 24 FEDORA-2016-242ff9a2fa Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7035

Description

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

FEDORA-2016-242ff9a2fa

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/11/?count=200&page=1>

Fedora Core 24

pacemaker-1.1.15-2.fc24

20751 - Oracle Sun Ray Software Critical Patch Update October 2016

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2016-2107

Description

An information disclosure vulnerability is present in some versions of Oracle Sun Ray Operating Software.

Observation

Sun Ray Operating Software is a popular secure platform that delivers rich virtual desktop experience.

An information disclosure vulnerability is present in some versions of Oracle Sun Ray Operating Software. The flaw lies in the OpenSSL component. Successful exploitation could allow an attacker to affect confidentiality.

135168 - Oracle Solaris 11.3.11.6.0 Update Is Not Installed (CVE-2016-5561)

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

Risk Level: Low

CVE: CVE-2016-5561

Description

The scan detected that the host is missing the following update:
SRU 11.3.11.6.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

135172 - Oracle Solaris 11.3.12.4.0 Update Is Not Installed (CVE-2016-5615)

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

Risk Level: Low

CVE: CVE-2016-5615

Description

The scan detected that the host is missing the following update:
SRU 11.3.12.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

141321 - Red Hat Enterprise Linux RHSA-2016-2585 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1981, CVE-2016-3712

Description

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

RHSA-2016-2585

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2585.html>

RHEL7D

x86_64

qemu-kvm-1.5.3-126.el7

qemu-kvm-debuginfo-1.5.3-126.el7

qemu-img-1.5.3-126.el7

qemu-kvm-tools-1.5.3-126.el7

qemu-kvm-common-1.5.3-126.el7

RHEL7S

ppc64

qemu-img-1.5.3-126.el7

qemu-kvm-debuginfo-1.5.3-126.el7

RHEL7WS

x86_64

qemu-kvm-1.5.3-126.el7

qemu-kvm-debuginfo-1.5.3-126.el7

qemu-img-1.5.3-126.el7

qemu-kvm-tools-1.5.3-126.el7

qemu-kvm-common-1.5.3-126.el7

135163 - Oracle Solaris 11.2.9.5.0 Update Is Not Installed (CVE-2016-5480)

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

Risk Level: Low

CVE: CVE-2016-5480

Description

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

SRU 11.2.9.5.0

Observation

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

For more information see:

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2189657.1&_adf.ctrl-state=170qipjygn_4&_afLoop=450729204826508

144976 - SuSE Linux 13.1 openSUSE-SU-2016:2736-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-0245

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2736-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00017.html>

SuSE Linux 13.1

i586

libdbus-1-3-1.8.22-4.39.1

dbus-1-1.8.22-4.39.1

dbus-1-debuginfo-1.8.22-4.39.1

dbus-1-debugsource-1.8.22-4.39.1

dbus-1-x11-debugsource-1.8.22-4.39.1

libdbus-1-3-debuginfo-1.8.22-4.39.1

dbus-1-devel-1.8.22-4.39.1

dbus-1-x11-1.8.22-4.39.1

dbus-1-x11-debuginfo-1.8.22-4.39.1

noarch

dbus-1-devel-doc-1.8.22-4.39.1

x86_64

libdbus-1-3-debuginfo-1.8.22-4.39.1

dbus-1-debuginfo-1.8.22-4.39.1

dbus-1-x11-debuginfo-1.8.22-4.39.1

dbus-1-devel-1.8.22-4.39.1

libdbus-1-3-32bit-1.8.22-4.39.1

dbus-1-debugsource-1.8.22-4.39.1

dbus-1-1.8.22-4.39.1

dbus-1-devel-32bit-1.8.22-4.39.1

dbus-1-x11-debugsource-1.8.22-4.39.1

libdbus-1-3-1.8.22-4.39.1

libdbus-1-3-debuginfo-32bit-1.8.22-4.39.1

dbus-1-x11-1.8.22-4.39.1

dbus-1-debuginfo-32bit-1.8.22-4.39.1

ENHANCED CHECKS

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

11024 - Microsoft IIS ODBC Tool Files Security Bypass Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

19945 - IBM AIX Openssl Multiple Vulnerabilities (openssl_advisory18)

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

Risk Level: High

CVE: CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800

Update Details

FASLScript is updated

19970 - IBM AIX OpenSSL Denial of Service Vulnerability

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

Risk Level: High

CVE: CVE-2016-2842

Update Details

FASLScript is updated

20645 - (MS16-123) Microsoft Windows Win32k Privilege Escalation I (3192892)

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

Risk Level: High

CVE: CVE-2016-3266

Update Details

Risk is updated

20680 - (MS16-120) Microsoft Windows Graphics Win32k Privilege Escalation (3192884)

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

Risk Level: High

CVE: CVE-2016-3270

Update Details

Risk is updated

20681 - (MS16-120) Microsoft Windows Graphics True Type Font Parsing Privilege Escalation (3192884)

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

Risk Level: High

CVE: CVE-2016-7182

Update Details

Risk is updated

33001 - Oracle Solaris 126547-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-3410, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-

2016-5480

[Update Details](#)

CVE is updated

33002 - Oracle Solaris 126546-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-3410, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2016-5480

[Update Details](#)

CVE is updated

11528 - (MS11-016) Vulnerability In Microsoft Office Groove Could Allow Remote Code Execution (2494047)

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

Risk Level: High

CVE: CVE-2010-3146

[Update Details](#)

Description is updated Observation is updated CVE is updated

20637 - (MS16-121) Security Update for Microsoft Office (3194063)

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

Risk Level: High

CVE: CVE-2016-7193

[Update Details](#)

Risk is updated

20638 - (MS16-121) Security Update for Microsoft Office (3194063)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7193

[Update Details](#)

Risk is updated

20639 - (MS16-121) Microsoft Office Memory Corruption Remote Code Execution (3194063)

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

Risk Level: High

CVE: CVE-2016-7193

[Update Details](#)

Risk is updated

20641 - (MS16-123) Microsoft Windows Win32k Privilege Escalation V (3192892)

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

Risk Level: High

CVE: CVE-2016-3376

[Update Details](#)

Risk is updated

20759 - (MS16-135) Microsoft Windows Kernel Privilege Escalation IV (3199135)

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

Risk Level: High

CVE: CVE-2016-7255

[Update Details](#)

Risk is updated

593 - Microsoft IIS newdsn.exe Command Execution

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

Risk Level: High

CVE: CVE-1999-0191

[Update Details](#)

Recommendation is updated

12980 - (MS04-011) Microsoft Windows ASN.1 Double Free Heap Corruption via SMB

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2004-0123

[Update Details](#)

FASLScript is updated

13850 - Microsoft IIS FTP Command Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14084 - Microsoft Index Service Ixssso.dll Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

20631 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution IV (3192890)

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

Risk Level: High

CVE: CVE-2016-7190

Update Details

Risk is updated

20632 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution III (3192890)

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

Risk Level: High

CVE: CVE-2016-3390

Update Details

Risk is updated

20633 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution II (3192890)

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

Risk Level: High

CVE: CVE-2016-3389

Update Details

Risk is updated

20642 - (MS16-123) Microsoft Windows Win32k Privilege Escalation IV (3192892)

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

Risk Level: High

CVE: CVE-2016-7211

Update Details

Risk is updated

20643 - (MS16-123) Microsoft Windows Win32k Privilege Escalation III (3192892)

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

Risk Level: High
CVE: CVE-2016-7185

[Update Details](#)

Risk is updated

20644 - (MS16-123) Microsoft Windows Win32k Privilege Escalation II (3192892)

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

Risk Level: High
CVE: CVE-2016-3241

[Update Details](#)

Risk is updated

20663 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution V (3192890)

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

Risk Level: High
CVE: CVE-2016-7194

[Update Details](#)

Risk is updated

20673 - (MS16-118) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution (3192887)

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

Risk Level: High
CVE: CVE-2016-3390

[Update Details](#)

Risk is updated

20676 - (MS16-125) Microsoft Windows Diagnostics Hub Privilege Escalation (3193229)

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

Risk Level: High
CVE: CVE-2016-7188

[Update Details](#)

Risk is updated

20677 - (MS16-125) Security Update for Diagnostic Hub (3193229)

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

Risk Level: High

CVE: CVE-2016-7188

[Update Details](#)

Risk is updated

181952 - FreeBSD expat Denial Of Service Vulnerability On Malformed Input (57b3aba7-1e25-11e6-8dd3-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-0718

[Update Details](#)

FASLScript is updated

9308 - Microsoft IIS HTR Files Password Policy Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2002-0421

[Update Details](#)

Recommendation is updated

13106 - Microsoft Internet Explorer Cache Objects History Enumeration Weakness Information Disclosure

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

Risk Level: Medium

CVE: CVE-2011-4689

[Update Details](#)

Recommendation is updated

16680 - OpenSSL Multiple MITM and DTLS Invalid Fragment Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-0195, CVE-2014-0224

[Update Details](#)

FASLScript is updated

20626 - (MS16-119) Microsoft Edge Browser Privilege Escalation II (3192890)

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

Risk Level: Medium

CVE: CVE-2016-3387

[Update Details](#)

Risk is updated

20671 - (MS16-118) Microsoft Internet Explorer Privilege Escalation I (3192887)

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

Risk Level: Medium

CVE: CVE-2016-3387

Update Details

Risk is updated

33145 - Oracle Solaris 150401-41 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5544, CVE-2016-5553

Update Details

CVE is updated

8380 - Microsoft IIS Sample Application Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

13392 - Microsoft Internet Explorer ASLR/DEP Bypass Denial of Service

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

Risk Level: Medium

CVE: CVE-2012-1545

Update Details

Recommendation is updated

20600 - IBM AIX Pconsole Directory Traversal Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-6038

Update Details

FASLScript is updated

20630 - (MS16-119) Microsoft Edge Browser Information Disclosure I (3192890)

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

Risk Level: Medium

CVE: CVE-2016-3267

[Update Details](#)

Risk is updated

20651 - (MS16-124) Microsoft Windows Kernel Privilege Escalation I (3193227)

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

Risk Level: Medium

CVE: CVE-2016-0070

[Update Details](#)

Risk is updated

20664 - (MS16-118) Microsoft Internet Explorer Information Disclosure I (3192887)

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

Risk Level: Medium

CVE: CVE-2016-3267

[Update Details](#)

Risk is updated

33162 - Oracle Solaris 150400-40 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553

[Update Details](#)

CVE is updated

33351 - Oracle Solaris 152506-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5559

[Update Details](#)

Risk is updated CVE is updated

33352 - Oracle Solaris 152507-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5559

[Update Details](#)

Risk is updated CVE is updated

696 - Microsoft IIS Index Server sqlqhit.asp Path Disclosure

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

Risk Level: Low

CVE: CVE-2001-0986

[Update Details](#)

Recommendation is updated

839 - Microsoft IIS htmimage.exe Path Disclosure

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

Risk Level: Low

CVE: CVE-2000-0122

[Update Details](#)

Recommendation is updated

6936 - Microsoft Internet Explorer AddFavorite Method DoS Vulnerability

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

Risk Level: Low

CVE: CVE-2009-2433

[Update Details](#)

Recommendation is updated

13043 - Microsoft Internet Explorer Cache Objects History Enumeration Weakness

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

Risk Level: Low

CVE: CVE-2002-2435

[Update Details](#)

Recommendation is updated

13846 - Microsoft IIS Tilde Character Short File Name Disclosure (142982)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

20625 - (MS16-119) Microsoft Edge Browser Security Bypass (3192890)

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

Risk Level: Low

CVE: CVE-2016-3392

[Update Details](#)

Risk is updated

20627 - (MS16-119) Microsoft Edge Browser Privilege Escalation I (3192890)

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

Risk Level: Low

CVE: CVE-2016-3388

[Update Details](#)

Risk is updated

20629 - (MS16-119) Microsoft Edge Browser Credential Data Information Disclosure (3192890)

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

Risk Level: Low

CVE: CVE-2016-3391

[Update Details](#)

Risk is updated

20648 - (MS16-124) Microsoft Windows Kernel Privilege Escalation IV (3193227)

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

Risk Level: Low

CVE: CVE-2016-0079

[Update Details](#)

Risk is updated

20649 - (MS16-124) Microsoft Windows Kernel Privilege Escalation III (3193227)

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

Risk Level: Low

CVE: CVE-2016-0075

[Update Details](#)

Risk is updated

20650 - (MS16-124) Microsoft Windows Kernel Privilege Escalation II (3193227)

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

Risk Level: Low

CVE: CVE-2016-0073

[Update Details](#)

Risk is updated

20665 - (MS16-118) Microsoft Internet Explorer Information Disclosure III (3192887)

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

Risk Level: Low

CVE: CVE-2016-3298

[Update Details](#)

Risk is updated

20672 - (MS16-118) Microsoft Internet Explorer Privilege Escalation II (3192887)

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

Risk Level: Low

CVE: CVE-2016-3388

[Update Details](#)

Risk is updated

20674 - (MS16-118) Microsoft Internet Explorer Information Disclosure II (3192887)

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

Risk Level: Low

CVE: CVE-2016-3391

[Update Details](#)

Risk is updated

20689 - (MS16-126) Security Update for Microsoft Internet Messaging API (3196067)

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

Risk Level: Low

CVE: CVE-2016-3298

[Update Details](#)

Risk is updated

20690 - (MS16-126) Internet Explorer Information Disclosure Vulnerability (3196067)

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

Risk Level: Low
CVE: CVE-2016-3298

Update Details

Risk is updated

70086 - oracle.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com/>

Multi-National Phone Support available here:

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

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

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2016 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates