2016-MAY-26
FSL version 7.5.824

MCAFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

20088 - Solarwinds Storage Resource Monitor Multiple SQL Injection Vulnerabilities Prior to 6.2.3

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

Risk Level: High

CVE: CVE-2016-4350

Description

Multiple SQL Injection vulnerabilities are present in some versions of Solarwinds Storage Resource Monitor.

Observation

Solarwinds Storage Resource Monitor is a storage manager software.

Multiple SQL Injection vulnerabilities are present in some versions of Solarwinds Storage Resource Monitor. The flaws lie in several components. Successful exploitation could allow a malicious user to compromise the integrity, confidentiality and availability of the system. Exploitation of this vulnerability doesn't require authentication.

20090 - (HPSBGN03580) HP Data Protector Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-2808, CVE-2016-2004, CVE-2016-2005, CVE-2016-2006, CVE-2016-2007, CVE-2016-2008

Description

Multiple vulnerabilities are present in some versions of HP Data Protector.

Observation

HP Data Protector automates high performance backups and recovery.

Multiple vulnerabilities are present in some versions of HP Data Protector. These flaws occur due to indeterminate issues. Successful exploitation could allow an attacker to execute arbitrary code or disclose sensitive information.

20091 - (HPSBGN03580) HP Data Protector Multiple Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2015-2808, CVE-2016-2004, CVE-2016-2005, CVE-2016-2006, CVE-2016-2007, CVE-2016-2008

Description

Multiple vulnerabilities are present in some versions of HP Data Protector.

Observation

HP Data Protector automates high performance backups and recovery.

Multiple vulnerabilities are present in some versions of HP Data Protector. These flaws occur due to indeterminate issues. Successful exploitation could allow an attacker to execute arbitrary code or disclose sensitive information.

20102 - (HT206567) Apple OS X Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-8865, CVE-2016-1791, CVE-2016-1792, CVE-2016-1793, CVE-2016-1794, CVE-2016-1795, CVE-2016-1796, CVE-2016-1797, CVE-2016-1798, CVE-2016-1799, CVE-2016-1800, CVE-2016-1801, CVE-2016-1802, CVE-2016-1803, CVE-2016-1804, CVE-2016-1805, CVE-2016-1806, CVE-2016-1807, CVE-2016-1808, CVE-2016-1809, CVE-2016-1810, CVE-2016-1811, CVE-2016-1812, CVE-2016-1813, CVE-2016-1814, CVE-2016-1815, CVE-2016-1816, CVE-2016-1817, CVE-2016-1818, CVE-2016-1819, CVE-2016-1820, CVE-2016-1821, CVE-2016-1822, CVE-2016-1823, CVE-2016-1824, CVE-2016-1825, CVE-2016-1826, CVE-2016-1827, CVE-2016-1828, CVE-2016-1829, CVE-2016-1830, CVE-2016-1831, CVE-2016-1832, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-1841, CVE-2016-1842, CVE-2016-1843, CVE-2016-1844, CVE-2016-1846, CVE-2016-1847, CVE-2016-1848, CVE-2016-1850, CVE-2016-1851, CVE-2016-1853, CVE-2016-1860, CVE-2016-1861, CVE-2016-3141, CVE-2016-3142, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073

Description

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

Observation

Apple Mac OS X is the operating system developed by Apple.

Multiple vulnerabilities are present in some versions of Apple Mac OS X. The flaws are mostly due to several memory corruption issues. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or remotely execute arbitrary code.

20106 - IBM WebSphere Application Server Multiple Java SDK Vulnerabilities (swg21982223)

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

Risk Level: High

CVE: CVE-2016-3426, CVE-2016-3427

Description

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

Observation

IBM WebSphere Application Server is a Java EE application server.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaws lie in the JDC and in the JMX Java components. Successful exploitation could allow an attacker to affect confidentiality, integrity, or availability.

20107 - IBM WebSphere Application Server Liberty Profile Multiple Java SDK Vulnerabilities (swg21982223)

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

Risk Level: High

CVE: CVE-2016-3426, CVE-2016-3427

Description

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

Observation

IBM WebSphere Application Server Liberty Profile is a Java EE application server.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server Liberty Profile. The flaws lie in the JDC and in the JMX Java components. Successful exploitation could allow an attacker to affect confidentiality, integrity, or availability.

144613 - SuSE Linux 13.2 openSUSE-SU-2016:1334-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3125

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1334-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00080.html

SuSE Linux 13.2
i586
proftpd-1.3.5b-6.1
proftpd-sqlite-debuginfo-1.3.5b-6.1
proftpd-debugsource-1.3.5b-6.1
proftpd-mysql-1.3.5b-6.1
proftpd-ldap-1.3.5b-6.1
proftpd-mysql-debuginfo-1.3.5b-6.1
proftpd-pgsql-debuginfo-1.3.5b-6.1
proftpd-ldap-debuginfo-1.3.5b-6.1
proftpd-doc-1.3.5b-6.1
proftpd-pgsql-1.3.5b-6.1
proftpd-radius-debuginfo-1.3.5b-6.1
proftpd-devel-1.3.5b-6.1
proftpd-debuginfo-1.3.5b-6.1
proftpd-radius-1.3.5b-6.1
proftpd-sqlite-1.3.5b-6.1

noarch
proftpd-lang-1.3.5b-6.1

x86_64
proftpd-1.3.5b-6.1
proftpd-sqlite-debuginfo-1.3.5b-6.1
proftpd-debugsource-1.3.5b-6.1
proftpd-mysql-1.3.5b-6.1
proftpd-ldap-1.3.5b-6.1
proftpd-mysql-debuginfo-1.3.5b-6.1
proftpd-pgsql-debuginfo-1.3.5b-6.1
proftpd-ldap-debuginfo-1.3.5b-6.1
proftpd-doc-1.3.5b-6.1
proftpd-pgsql-1.3.5b-6.1

proftpd-radius-debuginfo-1.3.5b-6.1
proftpd-devel-1.3.5b-6.1
proftpd-debuginfo-1.3.5b-6.1
proftpd-radius-1.3.5b-6.1
proftpd-sqlite-1.3.5b-6.1

144621 - SuSE SLES 10 SP4 SUSE-SU-2016:1352-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1352-1

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-May/002072.html

SuSE SLES 10 SP4
i586
MozillaFirefox-translations-38.8.0esr-0.5.1
MozillaFirefox-38.8.0esr-0.5.1

144624 - SuSE Linux 13.2 openSUSE-SU-2016:1326-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3717, CVE-2016-3718

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1326-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00072.html

SuSE Linux 13.2
x86_64
libGraphicsMagick++-devel-1.3.20-3.1
perl-GraphicsMagick-1.3.20-3.1
libGraphicsMagick3-config-1.3.20-3.1
libGraphicsMagick-Q16-3-1.3.20-3.1
perl-GraphicsMagick-debuginfo-1.3.20-3.1
GraphicsMagick-debugsource-1.3.20-3.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-3.1
GraphicsMagick-devel-1.3.20-3.1
GraphicsMagick-1.3.20-3.1
libGraphicsMagickWand-Q16-2-1.3.20-3.1
libGraphicsMagick++-Q16-3-1.3.20-3.1

libGraphicsMagick-Q16-3-debuginfo-1.3.20-3.1
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-3.1
GraphicsMagick-debuginfo-1.3.20-3.1

i586
libGraphicsMagick++-devel-1.3.20-3.1
perl-GraphicsMagick-1.3.20-3.1
libGraphicsMagick3-config-1.3.20-3.1
libGraphicsMagick-Q16-3-1.3.20-3.1
perl-GraphicsMagick-debuginfo-1.3.20-3.1
GraphicsMagick-debugsource-1.3.20-3.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-3.1
GraphicsMagick-devel-1.3.20-3.1
GraphicsMagick-1.3.20-3.1
libGraphicsMagickWand-Q16-2-1.3.20-3.1
libGraphicsMagick++-Q16-3-1.3.20-3.1
libGraphicsMagick-Q16-3-debuginfo-1.3.20-3.1
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-3.1
GraphicsMagick-debuginfo-1.3.20-3.1

144625 - SuSE SLES 11 SP4 SUSE-SU-2016:1374-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1374-1

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-May/002077.html

SuSE SLES 11 SP4
i586
MozillaFirefox-translations-38.8.0esr-40.5
libfreebl3-3.20.2-30.1
MozillaFirefox-38.8.0esr-40.5
mozilla-nss-3.20.2-30.1
libsoftokn3-3.20.2-30.1
mozilla-nspr-4.12-26.1
mozilla-nss-tools-3.20.2-30.1

x86_64
MozillaFirefox-translations-38.8.0esr-40.5
libfreebl3-3.20.2-30.1
mozilla-nspr-32bit-4.12-26.1
mozilla-nss-32bit-3.20.2-30.1
MozillaFirefox-38.8.0esr-40.5
mozilla-nss-3.20.2-30.1
libsoftokn3-3.20.2-30.1
libfreebl3-32bit-3.20.2-30.1
mozilla-nspr-4.12-26.1
mozilla-nss-tools-3.20.2-30.1
libsoftokn3-32bit-3.20.2-30.1

144627 - SuSE SLES 10 SP4 SUSE-SU-2016:1388-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0264, CVE-2016-0363, CVE-2016-0376, CVE-2016-0686, CVE-2016-0687, CVE-2016-3422, CVE-2016-3426, CVE-2016-3427, CVE-2016-3443, CVE-2016-3449

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1388-1

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-May/002081.html

SuSE SLES 10 SP4
i586
java-1_6_0-ibm-devel-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-alsa-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-plugin-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-jdbc-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-fonts-1.6.0_sr16.25-0.11.1

x86_64
java-1_6_0-ibm-devel-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-jdbc-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-plugin-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-32bit-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-plugin-32bit-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-alsa-32bit-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-fonts-1.6.0_sr16.25-0.11.1
java-1_6_0-ibm-devel-32bit-1.6.0_sr16.25-0.11.1

144629 - SuSE Linux 13.2 openSUSE-SU-2016:1332-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3194, CVE-2016-0639, CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0655, CVE-2016-0661, CVE-2016-0665, CVE-2016-0666, CVE-2016-0668, CVE-2016-0705, CVE-2016-2047

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1332-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00078.html

SuSE Linux 13.2
x86_64
mysql-community-server-bench-5.6.30-2.20.2
mysql-community-server-5.6.30-2.20.2
libmysql56client_r18-32bit-5.6.30-2.20.2
libmysql56client18-5.6.30-2.20.2
mysql-community-server-errormessages-5.6.30-2.20.2
mysql-community-server-test-5.6.30-2.20.2
libmysql56client18-debuginfo-32bit-5.6.30-2.20.2
mysql-community-server-bench-debuginfo-5.6.30-2.20.2
libmysql56client_r18-5.6.30-2.20.2
libmysql56client18-debuginfo-5.6.30-2.20.2
mysql-community-server-tools-debuginfo-5.6.30-2.20.2
mysql-community-server-debuginfo-5.6.30-2.20.2
mysql-community-server-test-debuginfo-5.6.30-2.20.2
mysql-community-server-client-5.6.30-2.20.2
mysql-community-server-debugsource-5.6.30-2.20.2
libmysql56client18-32bit-5.6.30-2.20.2
mysql-community-server-tools-5.6.30-2.20.2
mysql-community-server-client-debuginfo-5.6.30-2.20.2

i586
mysql-community-server-bench-5.6.30-2.20.2
mysql-community-server-5.6.30-2.20.2
libmysql56client18-5.6.30-2.20.2
mysql-community-server-errormessages-5.6.30-2.20.2
mysql-community-server-test-5.6.30-2.20.2
mysql-community-server-bench-debuginfo-5.6.30-2.20.2
libmysql56client_r18-5.6.30-2.20.2
libmysql56client18-debuginfo-5.6.30-2.20.2
mysql-community-server-tools-debuginfo-5.6.30-2.20.2
mysql-community-server-debuginfo-5.6.30-2.20.2
mysql-community-server-test-debuginfo-5.6.30-2.20.2
mysql-community-server-client-5.6.30-2.20.2
mysql-community-server-debugsource-5.6.30-2.20.2
mysql-community-server-tools-5.6.30-2.20.2
mysql-community-server-client-debuginfo-5.6.30-2.20.2

144631 - SuSE SLES 10 SP4 SUSE-SU-2016:1360-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0702, CVE-2016-2105, CVE-2016-2106, CVE-2016-2108, CVE-2016-2109

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1360-1

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-May/002074.html

SuSE SLES 10 SP4
i586
openssl-0.9.8a-18.96.1
openssl-devel-0.9.8a-18.96.1

openssl-doc-0.9.8a-18.96.1

x86_64
openssl-devel-32bit-0.9.8a-18.96.1
openssl-32bit-0.9.8a-18.96.1
openssl-0.9.8a-18.96.1
openssl-devel-0.9.8a-18.96.1
openssl-doc-0.9.8a-18.96.1

170678 - Amazon Linux AMI ALAS-2016-701 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0639, CVE-2016-0642, CVE-2016-0643, CVE-2016-0647, CVE-2016-0648, CVE-2016-0655, CVE-2016-0666, CVE-2016-0705, CVE-2016-2047

Description

The scan detected that the host is missing the following update:
ALAS-2016-701

Observation

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

https://alas.aws.amazon.com/ALAS-2016-701.html

Amazon Linux AMI
x86_64
mysql56-server-5.6.30-1.15.amzn1
mysql56-libs-5.6.30-1.15.amzn1
mysql56-errmsg-5.6.30-1.15.amzn1
mysql56-embedded-devel-5.6.30-1.15.amzn1
mysql56-embedded-5.6.30-1.15.amzn1
mysql56-common-5.6.30-1.15.amzn1
mysql56-debuginfo-5.6.30-1.15.amzn1
mysql56-test-5.6.30-1.15.amzn1
mysql56-bench-5.6.30-1.15.amzn1
mysql56-devel-5.6.30-1.15.amzn1
mysql56-5.6.30-1.15.amzn1

i686
mysql56-server-5.6.30-1.15.amzn1
mysql56-errmsg-5.6.30-1.15.amzn1
mysql56-embedded-devel-5.6.30-1.15.amzn1
mysql56-devel-5.6.30-1.15.amzn1
mysql56-common-5.6.30-1.15.amzn1
mysql56-debuginfo-5.6.30-1.15.amzn1
mysql56-test-5.6.30-1.15.amzn1
mysql56-libs-5.6.30-1.15.amzn1
mysql56-bench-5.6.30-1.15.amzn1
mysql56-embedded-5.6.30-1.15.amzn1
mysql56-5.6.30-1.15.amzn1

185293 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2973-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1938, CVE-2016-1978, CVE-2016-1979, CVE-2016-2805, CVE-2016-2807

Description

The scan detected that the host is missing the following update:
USN-2973-1

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-May/003436.html

Ubuntu 12.04

thunderbird_38.8.0+build1-0ubuntu0.12.04.1

Ubuntu 16.04

thunderbird_38.8.0+build1-0ubuntu0.16.04.1

Ubuntu 15.10

thunderbird_38.8.0+build1-0ubuntu0.15.10.1

Ubuntu 14.04

thunderbird_38.8.0+build1-0ubuntu0.14.04.1

185294 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2936-3 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
USN-2936-3

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-May/003437.html

Ubuntu 12.04

firefox_46.0.1+build1-0ubuntu0.12.04.2

Ubuntu 16.04

firefox_46.0.1+build1-0ubuntu0.16.04.2

Ubuntu 15.10

firefox_46.0.1+build1-0ubuntu0.15.10.2

Ubuntu 14.04

firefox_46.0.1+build1-0ubuntu0.14.04.3

20092 - (HT206568) Apple iOS Multiple Vulnerabilities Prior To 9.3.2

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2016-1790, CVE-2016-1801, CVE-2016-1802, CVE-2016-1803, CVE-2016-1807, CVE-2016-1808, CVE-2016-1811, CVE-2016-1813, CVE-2016-1814, CVE-2016-1817, CVE-2016-1818, CVE-2016-1819, CVE-2016-1823, CVE-2016-1824, CVE-2016-1827, CVE-2016-1828, CVE-2016-1829, CVE-2016-1830, CVE-2016-1831, CVE-2016-1832, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-1841, CVE-2016-1842, CVE-2016-1847, CVE-2016-1849, CVE-2016-1852, CVE-2016-1854, CVE-2016-1855, CVE-2016-1856, CVE-2016-1857, CVE-2016-1858, CVE-2016-1859

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 attackers to obtain sensitive information, cause a denial of service or execute arbitrary code.

20093 - (CTX212736) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-2107, CVE-2016-2108, CVE-2016-3710, CVE-2016-3712

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information or execute arbitrary code.

20096 - 7-ZIP Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-2334, CVE-2016-2335

Description

Multiple remote code execution vulnerabilities are present in some versions of 7-Zip file archiver.

Observation

7-Zip is an open source file archiver with a high compression ratio.

Multiple remote code execution vulnerabilities are present in some versions of 7-Zip file archiver. The flaws are due to an out-of-

bounds read in the CInArchive::ReadFileItem method when handling UDF files and a heap overflow in the NArchive::NHfs::CHandler::ExtractZlibFile method functionality of 7-Zip. Successful exploitation could allow an attacker to execute arbitrary code on the affected system by convincing the user to open a malicious file.

185296 - Ubuntu Linux 14.04, 15.10, 16.04 USN-2960-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1660, CVE-2016-1661, CVE-2016-1663, CVE-2016-1665, CVE-2016-1666, CVE-2016-1667, CVE-2016-1668, CVE-2016-1669, CVE-2016-1670

Description

The scan detected that the host is missing the following update:
USN-2960-1

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-May/003438.html

Ubuntu 16.04

liboxideqtcore0_1.14.9-0ubuntu0.16.04.1

Ubuntu 15.10

liboxideqtcore0_1.14.9-0ubuntu0.15.10.1

Ubuntu 14.04

liboxideqtcore0_1.14.9-0ubuntu0.14.04.1

20104 - Flexera InstallShield Untrusted Search Path Vulnerability

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

Risk Level: High

CVE: CVE-2016-2542

Description

A vulnerability is present in some versions of Flexera InstallShield.

Observation

Flexera InstallShield is a tool for creating installers or software packages.

A vulnerability is present in some versions of Flexera InstallShield. The flaw is due to insecure DLL loading. Successful exploitation could allow a local attacker to gain elevated privileges.

144619 - SuSE Linux 13.2 openSUSE-SU-2016:1357-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4342, CVE-2016-4343, CVE-2016-4346, CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1357-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00086.html

SuSE Linux 13.2
i586
php5-calendar-5.6.1-61.1
php5-devel-5.6.1-61.1
php5-suhosin-debuginfo-5.6.1-61.1
php5-zip-debuginfo-5.6.1-61.1
php5-gettext-5.6.1-61.1
php5-curl-5.6.1-61.1
php5-snmp-5.6.1-61.1
php5-shmop-5.6.1-61.1
php5-gd-5.6.1-61.1
php5-bcmath-debuginfo-5.6.1-61.1
php5-ftp-5.6.1-61.1
php5-sysvshm-debuginfo-5.6.1-61.1
php5-mbstring-debuginfo-5.6.1-61.1
php5-fastcgi-5.6.1-61.1
php5-calendar-debuginfo-5.6.1-61.1
php5-sysvshm-5.6.1-61.1
php5-readline-debuginfo-5.6.1-61.1
php5-mcrypt-debuginfo-5.6.1-61.1
php5-opcache-5.6.1-61.1
php5-debugsource-5.6.1-61.1
php5-fileinfo-5.6.1-61.1
php5-wddx-5.6.1-61.1
php5-tokenizer-debuginfo-5.6.1-61.1
php5-xmlreader-5.6.1-61.1
php5-mysql-debuginfo-5.6.1-61.1
php5-firebird-5.6.1-61.1
php5-phar-debuginfo-5.6.1-61.1
php5-opcache-debuginfo-5.6.1-61.1
php5-iconv-debuginfo-5.6.1-61.1
php5-pgsql-5.6.1-61.1
php5-openssl-debuginfo-5.6.1-61.1
php5-mysql-5.6.1-61.1
php5-pspell-debuginfo-5.6.1-61.1
php5-debuginfo-5.6.1-61.1
php5-mssql-5.6.1-61.1
php5-xmlrpc-5.6.1-61.1
php5-ftp-debuginfo-5.6.1-61.1
php5-fastcgi-debuginfo-5.6.1-61.1
php5-bz2-5.6.1-61.1
php5-fpm-5.6.1-61.1
php5-firebird-debuginfo-5.6.1-61.1
php5-ctype-5.6.1-61.1
php5-posix-debuginfo-5.6.1-61.1
php5-soap-5.6.1-61.1
php5-sqlite-5.6.1-61.1
php5-posix-5.6.1-61.1

php5-gd-debuginfo-5.6.1-61.1
php5-ctype-debuginfo-5.6.1-61.1
php5-dba-5.6.1-61.1
apache2-mod_php5-debuginfo-5.6.1-61.1
php5-ldap-debuginfo-5.6.1-61.1
php5-5.6.1-61.1
php5-ldap-5.6.1-61.1
php5-gmp-5.6.1-61.1
php5-fpm-debuginfo-5.6.1-61.1
php5-exif-debuginfo-5.6.1-61.1
php5-suhosin-5.6.1-61.1
php5-sysvmsg-5.6.1-61.1
php5-sockets-debuginfo-5.6.1-61.1
php5-dom-debuginfo-5.6.1-61.1
php5-dba-debuginfo-5.6.1-61.1
php5-snmp-debuginfo-5.6.1-61.1
php5-pcntl-debuginfo-5.6.1-61.1
php5-zlib-5.6.1-61.1
php5-openssl-5.6.1-61.1
php5-sysvsem-debuginfo-5.6.1-61.1
php5-iconv-5.6.1-61.1
php5-zip-5.6.1-61.1
php5-json-debuginfo-5.6.1-61.1
php5-xsl-debuginfo-5.6.1-61.1
php5-exif-5.6.1-61.1
php5-wddx-debuginfo-5.6.1-61.1
php5-sqlite-debuginfo-5.6.1-61.1
php5-gettext-debuginfo-5.6.1-61.1
php5-intl-debuginfo-5.6.1-61.1
php5-dom-5.6.1-61.1
php5-tidy-5.6.1-61.1
php5-xmlwriter-5.6.1-61.1
php5-tidy-debuginfo-5.6.1-61.1
php5-sysvsem-5.6.1-61.1
php5-imap-debuginfo-5.6.1-61.1
php5-fileinfo-debuginfo-5.6.1-61.1
php5-pcntl-5.6.1-61.1
php5-json-5.6.1-61.1
php5-shmop-debuginfo-5.6.1-61.1
php5-sysvmsg-debuginfo-5.6.1-61.1
php5-enchant-5.6.1-61.1
php5-sockets-5.6.1-61.1
php5-odbc-5.6.1-61.1
php5-phar-5.6.1-61.1
php5-bz2-debuginfo-5.6.1-61.1
php5-pdo-5.6.1-61.1
php5-enchant-debuginfo-5.6.1-61.1
php5-pgsql-debuginfo-5.6.1-61.1
php5-imap-5.6.1-61.1
php5-xsl-5.6.1-61.1
php5-xmlreader-debuginfo-5.6.1-61.1
php5-xmlrpc-debuginfo-5.6.1-61.1
php5-bcmath-5.6.1-61.1
php5-soap-debuginfo-5.6.1-61.1
php5-intl-5.6.1-61.1
php5-mcrypt-5.6.1-61.1
php5-odbc-debuginfo-5.6.1-61.1
php5-readline-5.6.1-61.1
php5-gmp-debuginfo-5.6.1-61.1
php5-tokenizer-5.6.1-61.1

php5-xmlwriter-debuginfo-5.6.1-61.1
php5-mssql-debuginfo-5.6.1-61.1
apache2-mod_php5-5.6.1-61.1
php5-curl-debuginfo-5.6.1-61.1
php5-pdo-debuginfo-5.6.1-61.1
php5-pspell-5.6.1-61.1
php5-zlib-debuginfo-5.6.1-61.1
php5-mbstring-5.6.1-61.1

noarch
php5-pear-5.6.1-61.1

x86_64
php5-calendar-5.6.1-61.1
php5-devel-5.6.1-61.1
php5-suhosin-debuginfo-5.6.1-61.1
php5-zip-debuginfo-5.6.1-61.1
php5-gettext-5.6.1-61.1
php5-curl-5.6.1-61.1
php5-snmp-5.6.1-61.1
php5-shmop-5.6.1-61.1
php5-gd-5.6.1-61.1
php5-bcmath-debuginfo-5.6.1-61.1
php5-ftp-5.6.1-61.1
php5-sysvshm-debuginfo-5.6.1-61.1
php5-mbstring-debuginfo-5.6.1-61.1
php5-fastcgi-5.6.1-61.1
php5-calendar-debuginfo-5.6.1-61.1
php5-sysvshm-5.6.1-61.1
php5-readline-debuginfo-5.6.1-61.1
php5-mcrypt-debuginfo-5.6.1-61.1
php5-opcache-5.6.1-61.1
php5-debugsource-5.6.1-61.1
php5-fileinfo-5.6.1-61.1
php5-wddx-5.6.1-61.1
php5-tokenizer-debuginfo-5.6.1-61.1
php5-xmlreader-5.6.1-61.1
php5-mysql-debuginfo-5.6.1-61.1
php5-firebird-5.6.1-61.1
php5-phar-debuginfo-5.6.1-61.1
php5-opcache-debuginfo-5.6.1-61.1
php5-iconv-debuginfo-5.6.1-61.1
php5-pgsql-5.6.1-61.1
php5-openssl-debuginfo-5.6.1-61.1
php5-mysql-5.6.1-61.1
php5-pspell-debuginfo-5.6.1-61.1
php5-debuginfo-5.6.1-61.1
php5-mssql-5.6.1-61.1
php5-xmlrpc-5.6.1-61.1
php5-ftp-debuginfo-5.6.1-61.1
php5-fastcgi-debuginfo-5.6.1-61.1
php5-bz2-5.6.1-61.1
php5-fpm-5.6.1-61.1
php5-firebird-debuginfo-5.6.1-61.1
php5-ctype-5.6.1-61.1
php5-posix-debuginfo-5.6.1-61.1
php5-soap-5.6.1-61.1
php5-sqlite-5.6.1-61.1
php5-posix-5.6.1-61.1
php5-gd-debuginfo-5.6.1-61.1

php5-ctype-debuginfo-5.6.1-61.1
php5-dba-5.6.1-61.1
apache2-mod_php5-debuginfo-5.6.1-61.1
php5-ldap-debuginfo-5.6.1-61.1
php5-5.6.1-61.1
php5-ldap-5.6.1-61.1
php5-gmp-5.6.1-61.1
php5-fpm-debuginfo-5.6.1-61.1
php5-exif-debuginfo-5.6.1-61.1
php5-suhosin-5.6.1-61.1
php5-sysvmsg-5.6.1-61.1
php5-sockets-debuginfo-5.6.1-61.1
php5-dom-debuginfo-5.6.1-61.1
php5-dba-debuginfo-5.6.1-61.1
php5-snmp-debuginfo-5.6.1-61.1
php5-pcntl-debuginfo-5.6.1-61.1
php5-zlib-5.6.1-61.1
php5-openssl-5.6.1-61.1
php5-sysvsem-debuginfo-5.6.1-61.1
php5-iconv-5.6.1-61.1
php5-zip-5.6.1-61.1
php5-json-debuginfo-5.6.1-61.1
php5-xsl-debuginfo-5.6.1-61.1
php5-exif-5.6.1-61.1
php5-wddx-debuginfo-5.6.1-61.1
php5-sqlite-debuginfo-5.6.1-61.1
php5-gettext-debuginfo-5.6.1-61.1
php5-intl-debuginfo-5.6.1-61.1
php5-dom-5.6.1-61.1
php5-tidy-5.6.1-61.1
php5-xmlwriter-5.6.1-61.1
php5-tidy-debuginfo-5.6.1-61.1
php5-sysvsem-5.6.1-61.1
php5-imap-debuginfo-5.6.1-61.1
php5-fileinfo-debuginfo-5.6.1-61.1
php5-pcntl-5.6.1-61.1
php5-json-5.6.1-61.1
php5-shmop-debuginfo-5.6.1-61.1
php5-sysvmsg-debuginfo-5.6.1-61.1
php5-enchant-5.6.1-61.1
php5-sockets-5.6.1-61.1
php5-odbc-5.6.1-61.1
php5-phar-5.6.1-61.1
php5-bz2-debuginfo-5.6.1-61.1
php5-pdo-5.6.1-61.1
php5-enchant-debuginfo-5.6.1-61.1
php5-pgsql-debuginfo-5.6.1-61.1
php5-imap-5.6.1-61.1
php5-xsl-5.6.1-61.1
php5-xmlreader-debuginfo-5.6.1-61.1
php5-xmlrpc-debuginfo-5.6.1-61.1
php5-bcmath-5.6.1-61.1
php5-soap-debuginfo-5.6.1-61.1
php5-intl-5.6.1-61.1
php5-mcrypt-5.6.1-61.1
php5-odbc-debuginfo-5.6.1-61.1
php5-readline-5.6.1-61.1
php5-gmp-debuginfo-5.6.1-61.1
php5-tokenizer-5.6.1-61.1
php5-xmlwriter-debuginfo-5.6.1-61.1

php5-mssql-debuginfo-5.6.1-61.1
apache2-mod_php5-5.6.1-61.1
php5-curl-debuginfo-5.6.1-61.1
php5-pdo-debuginfo-5.6.1-61.1
php5-pspell-5.6.1-61.1
php5-zlib-debuginfo-5.6.1-61.1
php5-mbstring-5.6.1-61.1

185295 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2984-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8865, CVE-2016-3078, CVE-2016-3132, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2016-4342, CVE-2016-4343, CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544

Description

The scan detected that the host is missing the following update:
USN-2984-1

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-May/003439.html

Ubuntu 12.04

php5-cgi_5.3.10-1ubuntu3.23
php5-cli_5.3.10-1ubuntu3.23
php5-fpm_5.3.10-1ubuntu3.23
libapache2-mod-php5_5.3.10-1ubuntu3.23

Ubuntu 16.04

libapache2-mod-php7.0_7.0.4-7ubuntu2.1
php7.0-fpm_7.0.4-7ubuntu2.1
php7.0-cgi_7.0.4-7ubuntu2.1
php7.0-cli_7.0.4-7ubuntu2.1

Ubuntu 15.10

php5-fpm_5.6.11+dfsg-1ubuntu3.4
php5-cgi_5.6.11+dfsg-1ubuntu3.4
php5-cli_5.6.11+dfsg-1ubuntu3.4
libapache2-mod-php5_5.6.11+dfsg-1ubuntu3.4

Ubuntu 14.04

libapache2-mod-php5_5.5.9+dfsg-1ubuntu4.17
php5-cli_5.5.9+dfsg-1ubuntu4.17
php5-fpm_5.5.9+dfsg-1ubuntu4.17
php5-cgi_5.5.9+dfsg-1ubuntu4.17

20079 - (HPSBMU03591) HPE Server Migration Pack Remote Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-7547, CVE-2016-0728, CVE-2016-2024

Description

Multiple vulnerabilities are present in some versions of HPE Server Migration Pack.

Observation

HPE Server Migration Pack is used to securely make server upgrades.

Multiple vulnerabilities are present in some versions of HPE Server Migration Pack. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, escalate privileges or remotely execute arbitrary code.

20094 - (HT206565) Apple Safari Multiple Vulnerabilities Prior To 9.1.1

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

Risk Level: High

CVE: CVE-2016-1849, CVE-2016-1854, CVE-2016-1855, CVE-2016-1856, CVE-2016-1857, CVE-2016-1858, CVE-2016-1859

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 multiple components. Successful exploitation could allow an attacker to obtain sensitive information, cause denial of service or execute arbitrary code.

20103 - Autodesk Backburner Manager Stack Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2016-2344

Description

A buffer overflow vulnerability is present in some versions of Autodesk Backburner.

Observation

Autodesk Backburner is a network-rendering management software for Autodesk products.

A buffer overflow vulnerability is present in some versions of Autodesk Backburner. The flaw lies in the Backburner Manager component. Successful exploitation could allow an attacker to execute remote code or cause a denial of service condition.

132239 - Oracle VM OVMSA-2016-0051 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5165, CVE-2015-5279, CVE-2015-7512, CVE-2016-1714, CVE-2016-3710

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0051

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-May/000467.html

OVM3.4
x86_64
qemu-img-0.12.1.2-2.491.el6_8.1

141197 - Red Hat Enterprise Linux RHSA-2016-1100 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5364, CVE-2015-5366

Description

The scan detected that the host is missing the following update:
RHSA-2016-1100

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-1100.html

RHEL6_6S
i386
perf-2.6.32-504.49.1.el6
kernel-2.6.32-504.49.1.el6
kernel-debug-debuginfo-2.6.32-504.49.1.el6
kernel-debug-devel-2.6.32-504.49.1.el6
kernel-debuginfo-2.6.32-504.49.1.el6
kernel-headers-2.6.32-504.49.1.el6
python-perf-debuginfo-2.6.32-504.49.1.el6
perf-debuginfo-2.6.32-504.49.1.el6
kernel-devel-2.6.32-504.49.1.el6
kernel-debuginfo-common-i686-2.6.32-504.49.1.el6
kernel-debug-2.6.32-504.49.1.el6

noarch
kernel-doc-2.6.32-504.49.1.el6
kernel-firmware-2.6.32-504.49.1.el6
kernel-abi-whitelists-2.6.32-504.49.1.el6

x86_64
perf-2.6.32-504.49.1.el6
kernel-2.6.32-504.49.1.el6
kernel-debug-debuginfo-2.6.32-504.49.1.el6
python-perf-debuginfo-2.6.32-504.49.1.el6
kernel-debug-devel-2.6.32-504.49.1.el6
kernel-debuginfo-2.6.32-504.49.1.el6
kernel-headers-2.6.32-504.49.1.el6
perf-debuginfo-2.6.32-504.49.1.el6
kernel-debuginfo-common-x86_64-2.6.32-504.49.1.el6
kernel-devel-2.6.32-504.49.1.el6
kernel-debuginfo-common-i686-2.6.32-504.49.1.el6

kernel-debug-2.6.32-504.49.1.el6

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

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

Risk Level: High

CVE: CVE-2015-8869

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1335-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00081.html

SuSE Linux 13.2
x86_64
ocaml-compiler-libs-devel-4.01.0-6.4.1
ocaml-emacs-4.01.0-6.4.1
ocaml-compiler-libs-4.01.0-6.4.1
ocaml-x11-4.01.0-6.4.1
ocaml-camlp4-4.01.0-6.4.1
ocaml-4.01.0-6.4.1
ocaml-labltk-devel-4.01.0-6.4.1
ocaml-camlp4-devel-debuginfo-4.01.0-6.4.1
ocaml-docs-4.01.0-6.4.1
ocaml-ocamldoc-4.01.0-6.4.1
ocaml-debugsource-4.01.0-6.4.1
ocaml-runtime-debuginfo-4.01.0-6.4.1
ocaml-camlp4-devel-4.01.0-6.4.1
ocaml-ocamldoc-debuginfo-4.01.0-6.4.1
ocaml-debuginfo-4.01.0-6.4.1
ocaml-labltk-4.01.0-6.4.1
ocaml-source-4.01.0-6.4.1
ocaml-labltk-debuginfo-4.01.0-6.4.1
ocaml-runtime-4.01.0-6.4.1

i586
ocaml-compiler-libs-devel-4.01.0-6.4.1
ocaml-emacs-4.01.0-6.4.1
ocaml-compiler-libs-4.01.0-6.4.1
ocaml-x11-4.01.0-6.4.1
ocaml-camlp4-4.01.0-6.4.1
ocaml-4.01.0-6.4.1
ocaml-labltk-devel-4.01.0-6.4.1
ocaml-camlp4-devel-debuginfo-4.01.0-6.4.1
ocaml-docs-4.01.0-6.4.1
ocaml-ocamldoc-4.01.0-6.4.1
ocaml-debugsource-4.01.0-6.4.1
ocaml-runtime-debuginfo-4.01.0-6.4.1
ocaml-camlp4-devel-4.01.0-6.4.1
ocaml-ocamldoc-debuginfo-4.01.0-6.4.1
ocaml-debuginfo-4.01.0-6.4.1
ocaml-labltk-4.01.0-6.4.1
ocaml-source-4.01.0-6.4.1

ocaml-labltk-debuginfo-4.01.0-6.4.1
ocaml-runtime-4.01.0-6.4.1

144614 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1344-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2523, CVE-2016-2530, CVE-2016-2531, CVE-2016-2532

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1344-1

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-May/002068.html

SuSE SLED 12 SP1
x86_64
wireshark-debugsource-1.12.11-25.1
wireshark-debuginfo-1.12.11-25.1
wireshark-1.12.11-25.1

SuSE SLED 12
x86_64
wireshark-debugsource-1.12.11-25.1
wireshark-debuginfo-1.12.11-25.1
wireshark-1.12.11-25.1

SuSE SLES 12 SP1
x86_64
wireshark-debugsource-1.12.11-25.1
wireshark-debuginfo-1.12.11-25.1
wireshark-1.12.11-25.1

SuSE SLES 12
x86_64
wireshark-debugsource-1.12.11-25.1
wireshark-debuginfo-1.12.11-25.1
wireshark-1.12.11-25.1

144616 - SuSE SLES 11 SP4 SUSE-SU-2016:1345-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2523, CVE-2016-2530, CVE-2016-2531, CVE-2016-2532

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1345-1

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-May/002069.html

SuSE SLES 11 SP4
i586
wireshark-1.12.11-0.18.1

x86_64
wireshark-1.12.11-0.18.1

144618 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1386-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1386-1

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-May/002080.html

SuSE SLED 12 SP1
x86_64
openssh-askpass-gnome-6.6p1-42.1
openssh-debuginfo-6.6p1-42.1
openssh-helpers-6.6p1-42.1
openssh-helpers-debuginfo-6.6p1-42.1
openssh-debugsource-6.6p1-42.1
openssh-6.6p1-42.1
openssh-askpass-gnome-debuginfo-6.6p1-42.1

SuSE SLED 12
x86_64
openssh-askpass-gnome-6.6p1-42.1
openssh-debuginfo-6.6p1-42.1
openssh-helpers-6.6p1-42.1
openssh-helpers-debuginfo-6.6p1-42.1
openssh-debugsource-6.6p1-42.1
openssh-6.6p1-42.1
openssh-askpass-gnome-debuginfo-6.6p1-42.1

SuSE SLES 12 SP1
x86_64
openssh-askpass-gnome-6.6p1-42.1
openssh-debuginfo-6.6p1-42.1
openssh-fips-6.6p1-42.1
openssh-helpers-6.6p1-42.1
openssh-helpers-debuginfo-6.6p1-42.1
openssh-debugsource-6.6p1-42.1
openssh-6.6p1-42.1
openssh-askpass-gnome-debuginfo-6.6p1-42.1

SuSE SLES 12

x86_64
openssh-askpass-gnome-6.6p1-42.1
openssh-debuginfo-6.6p1-42.1
openssh-fips-6.6p1-42.1
openssh-helpers-6.6p1-42.1
openssh-helpers-debuginfo-6.6p1-42.1
openssh-debugsource-6.6p1-42.1
openssh-6.6p1-42.1
openssh-askpass-gnome-debuginfo-6.6p1-42.1

144626 - SuSE Linux 13.2 openSUSE-SU-2016:1370-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4574

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1370-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00087.html

SuSE Linux 13.2
x86_64
libksba8-debuginfo-1.3.1-12.1
libksba-debugsource-1.3.1-12.1
libksba-devel-1.3.1-12.1
libksba8-1.3.1-12.1

i586
libksba8-debuginfo-1.3.1-12.1
libksba-debugsource-1.3.1-12.1
libksba-devel-1.3.1-12.1
libksba8-1.3.1-12.1

144630 - SuSE Linux 13.2 openSUSE-SU-2016:1330-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-5326, CVE-2014-9762, CVE-2014-9763, CVE-2014-9764, CVE-2014-9771, CVE-2016-3993, CVE-2016-3994, CVE-2016-4024

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1330-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00076.html

SuSE Linux 13.2
x86_64
imlib2-loaders-debuginfo-1.4.9-17.4.1
imlib2-debuginfo-1.4.9-17.4.1
imlib2-devel-1.4.9-17.4.1
imlib2-1.4.9-17.4.1
imlib2-filters-1.4.9-17.4.1
imlib2-debugsource-1.4.9-17.4.1
libImlib2-1-debuginfo-1.4.9-17.4.1
libImlib2-1-1.4.9-17.4.1
imlib2-loaders-1.4.9-17.4.1
imlib2-filters-debuginfo-1.4.9-17.4.1

i586
imlib2-loaders-debuginfo-1.4.9-17.4.1
imlib2-debuginfo-1.4.9-17.4.1
imlib2-devel-1.4.9-17.4.1
imlib2-1.4.9-17.4.1
imlib2-filters-1.4.9-17.4.1
imlib2-debugsource-1.4.9-17.4.1
libImlib2-1-debuginfo-1.4.9-17.4.1
libImlib2-1-1.4.9-17.4.1
imlib2-loaders-1.4.9-17.4.1
imlib2-filters-debuginfo-1.4.9-17.4.1

163094 - Oracle Enterprise Linux ELSA-2016-3568 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3697

Description

The scan detected that the host is missing the following update:
ELSA-2016-3568

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006087.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006086.html

OEL7
x86_64
docker-engine-1.10.3-1.0.3.el7
docker-engine-selinux-1.10.3-1.0.3.el7

OEL6
x86_64
docker-engine-1.10.3-1.0.3.el6

170680 - Amazon Linux AMI ALAS-2016-703 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8839, CVE-2016-0758, CVE-2016-3961, CVE-2016-4485, CVE-2016-4486, CVE-2016-4557, CVE-2016-4558, CVE-2016-4565, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
ALAS-2016-703

Observation

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

https://alas.aws.amazon.com/ALAS-2016-703.html

Amazon Linux AMI
i686
kernel-4.4.10-22.54.amzn1
kernel-debuginfo-common-i686-4.4.10-22.54.amzn1
kernel-tools-debuginfo-4.4.10-22.54.amzn1
kernel-tools-devel-4.4.10-22.54.amzn1
perf-debuginfo-4.4.10-22.54.amzn1
perf-4.4.10-22.54.amzn1
kernel-debuginfo-4.4.10-22.54.amzn1
kernel-tools-4.4.10-22.54.amzn1
kernel-headers-4.4.10-22.54.amzn1
kernel-devel-4.4.10-22.54.amzn1

noarch
kernel-doc-4.4.10-22.54.amzn1

x86_64
kernel-4.4.10-22.54.amzn1
kernel-tools-4.4.10-22.54.amzn1
kernel-debuginfo-common-x86_64-4.4.10-22.54.amzn1
kernel-tools-debuginfo-4.4.10-22.54.amzn1
kernel-tools-devel-4.4.10-22.54.amzn1
perf-debuginfo-4.4.10-22.54.amzn1
perf-4.4.10-22.54.amzn1
kernel-debuginfo-4.4.10-22.54.amzn1
kernel-headers-4.4.10-22.54.amzn1
kernel-devel-4.4.10-22.54.amzn1

20080 - (HPSBMU03589) HPE Version Control Repository Manager Multiple Denial Of Service Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792

Description

Multiple denial of service vulnerabilities are present in some versions of HPE Version Control Repository Manager.

Observation

HPE Version Control Repository Manager lets customers to manage HP software stored in their repositories.

Multiple denial of service vulnerabilities are present in some versions of HPE Version Control Repository Manager. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to cause a denial of service condition.

132237 - Oracle VM OVMSA-2016-0053 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4312, CVE-2015-8215, CVE-2015-8543, CVE-2016-0758

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0053

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-May/000466.html

OVM3.3
x86_64
kernel-uek-firmware-3.8.13-118.6.2.el6uek
kernel-uek-3.8.13-118.6.2.el6uek

144611 - SuSE Linux 13.2 openSUSE-SU-2016:1336-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3105

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1336-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00082.html

SuSE Linux 13.2
i586
mercurial-3.1.2-10.1
mercurial-debugsource-3.1.2-10.1
mercurial-debuginfo-3.1.2-10.1

noarch
mercurial-lang-3.1.2-10.1

x86_64
mercurial-3.1.2-10.1
mercurial-debugsource-3.1.2-10.1
mercurial-debuginfo-3.1.2-10.1

144620 - SuSE Linux 13.2 openSUSE-SU-2016:1328-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3172, CVE-2016-3659

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1328-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00074.html

SuSE Linux 13.2
noarch
cacti-0.8.8f-4.16.1

163092 - Oracle Enterprise Linux ELSA-2016-3567 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4312, CVE-2015-7509, CVE-2015-8215, CVE-2015-8324, CVE-2015-8543

Description

The scan detected that the host is missing the following update:
ELSA-2016-3567

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006085.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006084.html

OEL5
x86_64
kernel-uek-doc-2.6.32-400.37.17.el5uek
kernel-uek-debug-devel-2.6.32-400.37.17.el5uek
ofa-2.6.32-400.37.17.el5uek-1.5.1-4.0.58
kernel-uek-firmware-2.6.32-400.37.17.el5uek
kernel-uek-devel-2.6.32-400.37.17.el5uek
kernel-uek-2.6.32-400.37.17.el5uek
kernel-uek-debug-2.6.32-400.37.17.el5uek
mlnx_en-2.6.32-400.37.17.el5uekdebug-1.5.7-2
mlnx_en-2.6.32-400.37.17.el5uek-1.5.7-2
ofa-2.6.32-400.37.17.el5uekdebug-1.5.1-4.0.58

i386
kernel-uek-doc-2.6.32-400.37.17.el5uek
kernel-uek-debug-devel-2.6.32-400.37.17.el5uek
ofa-2.6.32-400.37.17.el5uek-1.5.1-4.0.58
kernel-uek-firmware-2.6.32-400.37.17.el5uek
kernel-uek-devel-2.6.32-400.37.17.el5uek
kernel-uek-2.6.32-400.37.17.el5uek
kernel-uek-debug-2.6.32-400.37.17.el5uek
mlnx_en-2.6.32-400.37.17.el5uekdebug-1.5.7-2
mlnx_en-2.6.32-400.37.17.el5uek-1.5.7-2
ofa-2.6.32-400.37.17.el5uekdebug-1.5.1-4.0.58

OEL6

x86_64
kernel-uek-debug-2.6.32-400.37.17.el6uek
kernel-uek-2.6.32-400.37.17.el6uek
kernel-uek-firmware-2.6.32-400.37.17.el6uek
kernel-uek-doc-2.6.32-400.37.17.el6uek
mlnx_en-2.6.32-400.37.17.el6uekdebug-1.5.7-0.1
ofa-2.6.32-400.37.17.el6uekdebug-1.5.1-4.0.58
kernel-uek-debug-devel-2.6.32-400.37.17.el6uek
mlnx_en-2.6.32-400.37.17.el6uek-1.5.7-0.1
kernel-uek-devel-2.6.32-400.37.17.el6uek
ofa-2.6.32-400.37.17.el6uek-1.5.1-4.0.58

i386
kernel-uek-2.6.32-400.37.17.el6uek
kernel-uek-debug-2.6.32-400.37.17.el6uek
kernel-uek-doc-2.6.32-400.37.17.el6uek
mlnx_en-2.6.32-400.37.17.el6uekdebug-1.5.7-0.1
ofa-2.6.32-400.37.17.el6uekdebug-1.5.1-4.0.58
kernel-uek-debug-devel-2.6.32-400.37.17.el6uek
mlnx_en-2.6.32-400.37.17.el6uek-1.5.7-0.1
kernel-uek-devel-2.6.32-400.37.17.el6uek
kernel-uek-firmware-2.6.32-400.37.17.el6uek
ofa-2.6.32-400.37.17.el6uek-1.5.1-4.0.58

163093 - Oracle Enterprise Linux ELSA-2016-3565 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4312, CVE-2015-8215, CVE-2015-8543, CVE-2016-0758

Description

The scan detected that the host is missing the following update:
ELSA-2016-3565

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006080.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006079.html

OEL7
x86_64
kernel-uek-doc-3.8.13-118.6.2.el7uek
kernel-uek-devel-3.8.13-118.6.2.el7uek
dtrace-modules-3.8.13-118.6.2.el7uek-0.4.5-3.el7
kernel-uek-firmware-3.8.13-118.6.2.el7uek
kernel-uek-debug-devel-3.8.13-118.6.2.el7uek
kernel-uek-debug-3.8.13-118.6.2.el7uek
kernel-uek-3.8.13-118.6.2.el7uek

OEL6
x86_64
kernel-uek-firmware-3.8.13-118.6.2.el6uek
dtrace-modules-3.8.13-118.6.2.el6uek-0.4.5-3.el6
kernel-uek-debug-3.8.13-118.6.2.el6uek
kernel-uek-devel-3.8.13-118.6.2.el6uek
kernel-uek-debug-devel-3.8.13-118.6.2.el6uek

kernel-uek-doc-3.8.13-118.6.2.el6uek
kernel-uek-3.8.13-118.6.2.el6uek

163095 - Oracle Enterprise Linux ELSA-2016-3566 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4312, CVE-2015-7509, CVE-2015-8215, CVE-2015-8543

Description

The scan detected that the host is missing the following update:
ELSA-2016-3566

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006081.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006082.html

OEL5
x86_64
kernel-uek-devel-2.6.39-400.278.3.el5uek
kernel-uek-2.6.39-400.278.3.el5uek
kernel-uek-doc-2.6.39-400.278.3.el5uek
kernel-uek-debug-2.6.39-400.278.3.el5uek
kernel-uek-firmware-2.6.39-400.278.3.el5uek
kernel-uek-debug-devel-2.6.39-400.278.3.el5uek

i386
kernel-uek-firmware-2.6.39-400.278.3.el5uek
kernel-uek-2.6.39-400.278.3.el5uek
kernel-uek-doc-2.6.39-400.278.3.el5uek
kernel-uek-debug-2.6.39-400.278.3.el5uek
kernel-uek-devel-2.6.39-400.278.3.el5uek
kernel-uek-debug-devel-2.6.39-400.278.3.el5uek

OEL6
x86_64
kernel-uek-debug-2.6.39-400.278.3.el6uek
kernel-uek-debug-devel-2.6.39-400.278.3.el6uek
kernel-uek-devel-2.6.39-400.278.3.el6uek
kernel-uek-doc-2.6.39-400.278.3.el6uek
kernel-uek-2.6.39-400.278.3.el6uek
kernel-uek-firmware-2.6.39-400.278.3.el6uek

i386
kernel-uek-debug-2.6.39-400.278.3.el6uek
kernel-uek-debug-devel-2.6.39-400.278.3.el6uek
kernel-uek-devel-2.6.39-400.278.3.el6uek
kernel-uek-doc-2.6.39-400.278.3.el6uek
kernel-uek-2.6.39-400.278.3.el6uek
kernel-uek-firmware-2.6.39-400.278.3.el6uek

170679 - Amazon Linux AMI ALAS-2016-702 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ALAS-2016-702

Observation

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

https://alas.aws.amazon.com/ALAS-2016-702.html

Amazon Linux AMI
x86_64
nss-softokn-devel-3.16.2.3-14.2.38.amzn1
nspr-devel-4.11.0-1.37.amzn1
nspr-debuginfo-4.11.0-1.37.amzn1
nss-pkcs11-devel-3.21.0-9.76.amzn1
nss-softokn-3.16.2.3-14.2.38.amzn1
nss-util-devel-3.21.0-2.2.50.amzn1
nss-util-3.21.0-2.2.50.amzn1
nss-softokn-freebl-3.16.2.3-14.2.38.amzn1
nss-softokn-debuginfo-3.16.2.3-14.2.38.amzn1
nss-sysinit-3.21.0-9.76.amzn1
nspr-4.11.0-1.37.amzn1
nss-tools-3.21.0-9.76.amzn1
nss-debuginfo-3.21.0-9.76.amzn1
nss-util-debuginfo-3.21.0-2.2.50.amzn1
nss-3.21.0-9.76.amzn1
nss-devel-3.21.0-9.76.amzn1
nss-softokn-freebl-devel-3.16.2.3-14.2.38.amzn1

i686
nss-util-debuginfo-3.21.0-2.2.50.amzn1
nspr-devel-4.11.0-1.37.amzn1
nss-devel-3.21.0-9.76.amzn1
nspr-debuginfo-4.11.0-1.37.amzn1
nss-pkcs11-devel-3.21.0-9.76.amzn1
nss-softokn-3.16.2.3-14.2.38.amzn1
nss-util-devel-3.21.0-2.2.50.amzn1
nss-softokn-freebl-3.16.2.3-14.2.38.amzn1
nss-softokn-devel-3.16.2.3-14.2.38.amzn1
nss-softokn-debuginfo-3.16.2.3-14.2.38.amzn1
nss-sysinit-3.21.0-9.76.amzn1
nss-util-3.21.0-2.2.50.amzn1
nss-tools-3.21.0-9.76.amzn1
nss-debuginfo-3.21.0-9.76.amzn1
nss-3.21.0-9.76.amzn1
nspr-4.11.0-1.37.amzn1
nss-softokn-freebl-devel-3.16.2.3-14.2.38.amzn1

20087 - (SYM16-007) Symantec Messaging Gateway ACE Library SSL HeartBleed Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-0160

Description

An information disclosure vulnerability is present in some versions of Symantec Messaging Gateway.

Observation

Symantec Messaging Gateway is an email security solution.

An information disclosure vulnerability is present in some versions of Symantec Messaging Gateway. The flaw lies in the ACE Library. Successful exploitation could allow an attacker to obtain sensitive information.

20095 - Apache HTTP Server mod_http2 Denial of Service Vulnerability Prior To 2.4.20

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

Risk Level: Medium

CVE: CVE-2016-1546

Description

A denial of service vulnerability is present in some versions of Apache HTTP Server.

Observation

Apache HTTP Server is an open source web server.

A denial of service vulnerability is present in some versions of Apache HTTP Server. The flaw lies in http2 module. Successful exploitation could allow an attacker to cause denial of service condition.

130500 - Debian Linux 8.0 DSA-3584-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7558, CVE-2016-4347, CVE-2016-4348

Description

The scan detected that the host is missing the following update:
DSA-3584-1

Observation

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

http://www.debian.org/security/2016/dsa-3584

Debian 8.0
all
librsvg2-common_2.40.5-1+deb8u2
librsvg2-doc_2.40.5-1+deb8u2
librsvg2-bin_2.40.5-1+deb8u2
gir1.2-rsvg-2.0_2.40.5-1+deb8u2
librsvg2-dev_2.40.5-1+deb8u2
librsvg2-dbg_2.40.5-1+deb8u2
librsvg2-2_2.40.5-1+deb8u2

130504 - Debian Linux 8.0 DSA-3583-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8466

Description

The scan detected that the host is missing the following update:
DSA-3583-1

Observation

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

http://www.debian.org/security/2016/dsa-3583

Debian 8.0
all
swift-plugin-s3_1.7-5+deb8u1

132238 - Oracle VM OVMSA-2016-0052 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4312, CVE-2015-8767, CVE-2016-0758

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0052

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-May/000465.html

OVM3.4
x86_64
kernel-uek-4.1.12-37.4.1.el6uek
kernel-uek-firmware-4.1.12-37.4.1.el6uek

144623 - SuSE Linux 13.2 openSUSE-SU-2016:1327-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-5333, CVE-2015-5334

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1327-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00073.html

SuSE Linux 13.2
i586
libcrypto34-2.2.7-2.13.1
libressl-2.2.7-2.13.1
libtls4-debuginfo-2.2.7-2.13.1
libressl-devel-2.2.7-2.13.1
libressl-debugsource-2.2.7-2.13.1
libssl33-debuginfo-2.2.7-2.13.1
libressl-debuginfo-2.2.7-2.13.1
libtls4-2.2.7-2.13.1
libcrypto34-debuginfo-2.2.7-2.13.1
libssl33-2.2.7-2.13.1

noarch
libressl-devel-doc-2.2.7-2.13.1

x86_64
libcrypto34-2.2.7-2.13.1
libressl-devel-32bit-2.2.7-2.13.1
libtls4-32bit-2.2.7-2.13.1
libressl-debuginfo-2.2.7-2.13.1
libcrypto34-debuginfo-2.2.7-2.13.1
libssl33-2.2.7-2.13.1
libressl-debugsource-2.2.7-2.13.1
libssl33-32bit-2.2.7-2.13.1
libcrypto34-debuginfo-32bit-2.2.7-2.13.1
libtls4-debuginfo-2.2.7-2.13.1
libcrypto34-32bit-2.2.7-2.13.1
libtls4-debuginfo-32bit-2.2.7-2.13.1
libressl-2.2.7-2.13.1
libtls4-2.2.7-2.13.1
libssl33-debuginfo-2.2.7-2.13.1
libssl33-debuginfo-32bit-2.2.7-2.13.1
libressl-devel-2.2.7-2.13.1

144628 - SuSE Linux 13.2 openSUSE-SU-2016:1333-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4348

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1333-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00079.html

SuSE Linux 13.2
x86_64
gdk-pixbuf-loader-rsvg-debuginfo-2.40.15-10.1
typelib-1_0-Rsvg-2_0-2.40.15-10.1
gdk-pixbuf-loader-rsvg-debuginfo-32bit-2.40.15-10.1
librsvg-devel-2.40.15-10.1
rsvg-view-debuginfo-2.40.15-10.1

librsvg-2-2-32bit-2.40.15-10.1
librsvg-debugsource-2.40.15-10.1
gdk-pixbuf-loader-rsvg-32bit-2.40.15-10.1
librsvg-2-2-debuginfo-32bit-2.40.15-10.1
rsvg-view-2.40.15-10.1
librsvg-2-2-2.40.15-10.1
gdk-pixbuf-loader-rsvg-2.40.15-10.1
librsvg-2-2-debuginfo-2.40.15-10.1

i586
librsvg-devel-2.40.15-10.1
typelib-1_0-Rsvg-2_0-2.40.15-10.1
gdk-pixbuf-loader-rsvg-2.40.15-10.1
librsvg-2-2-2.40.15-10.1
rsvg-view-2.40.15-10.1
rsvg-view-debuginfo-2.40.15-10.1
librsvg-debugsource-2.40.15-10.1
gdk-pixbuf-loader-rsvg-debuginfo-2.40.15-10.1
librsvg-2-2-debuginfo-2.40.15-10.1

174960 - Scientific Linux Security ERRATA Moderate: libndp on SL7.x x86_64 (1605-5718)

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

Risk Level: Medium

CVE: CVE-2016-3698

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libndp on SL7.x x86_64 (1605-5718)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1605&L=scientific-linux-errata&F=&S=&P=5718

SL7
x86_64
libndp-devel-1.2-6.el7_2
libndp-1.2-6.el7_2
libndp-debuginfo-1.2-6.el7_2

181950 - FreeBSD wpa_supplicant Psk Configuration Parameter Update Allowing Arbitrary Data To Be Written (967b852b-1e28-11e6-8dd3-0025902

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

Risk Level: Medium

CVE: CVE-2016-4476, CVE-2016-4477

Description

The scan detected that the host is missing the following update:
wpa_supplicant -- psk configuration parameter update allowing arbitrary data to be written (967b852b-1e28-11e6-8dd3-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/967b852b-1e28-11e6-8dd3-002590263bf5.html

Affected packages:
wpa_supplicant < 2.5_2

185292 - Ubuntu Linux 12.04 USN-2950-4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
USN-2950-4

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-May/003435.html

Ubuntu 12.04

samba_3.6.25-0ubuntu0.12.04.4

130501 - Debian Linux 8.0 DSA-3585-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4006, CVE-2016-4079, CVE-2016-4080, CVE-2016-4081, CVE-2016-4082, CVE-2016-4085

Description

The scan detected that the host is missing the following update:
DSA-3585-1

Observation

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

http://www.debian.org/security/2016/dsa-3585

Debian 8.0
all
wireshark_1.12.1+g01b65bf-4+deb8u6

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

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

Risk Level: Low

CVE: CVE-2016-4478

Description

The scan detected that the host is missing the following update:
DSA-3586-1

Observation

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

http://www.debian.org/security/2016/dsa-3586

Debian 8.0
all
atheme-services_6.0.11-2+deb8u1

130503 - Debian Linux 8.0 DSA-3582-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
DSA-3582-1

Observation

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

http://www.debian.org/security/2016/dsa-3582

Debian 8.0
all
expat_2.1.0-6+deb8u2

144617 - SuSE SLES 11 SP4 SUSE-SU-2016:1366-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1366-1

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-May/002075.html

SuSE SLES 11 SP4
i586
suseRegisterInfo-2.1.12-14.2
rhnlib-2.5.69.8-11.2

x86_64

susuRegisterInfo-2.1.12-14.2
rhnlib-2.5.69.8-11.2

181951 - FreeBSD mediawiki Multiple Vulnerabilities (b50f53ce-2151-11e6-8dd3-002590263bf5)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
mediawiki -- multiple vulnerabilities (b50f53ce-2151-11e6-8dd3-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/b50f53ce-2151-11e6-8dd3-002590263bf5.html

Affected packages:
mediawiki123 < 1.23.14
mediawiki124 <= 1.24.6
mediawiki125 < 1.25.6
mediawiki126 < 1.26.3

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: Low

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
expat -- denial of service vulnerability on malformed input (57b3aba7-1e25-11e6-8dd3-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/57b3aba7-1e25-11e6-8dd3-002590263bf5.html

Affected packages:
expat < 2.1.1

185291 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2983-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
USN-2983-1

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-May/003434.html

Ubuntu 12.04

lib64expat1_2.0.1-7.2ubuntu1.3
libexpat1_2.0.1-7.2ubuntu1.3

Ubuntu 16.04

lib64expat1_2.1.0-7ubuntu0.16.04.1
libexpat1_2.1.0-7ubuntu0.16.04.1

Ubuntu 15.10

lib64expat1_2.1.0-7ubuntu0.15.10.1
libexpat1_2.1.0-7ubuntu0.15.10.1

Ubuntu 14.04

lib64expat1_2.1.0-4ubuntu1.2
libexpat1_2.1.0-4ubuntu1.2

20089 - (SB10158) McAfee VirusScan Enterprise Protections Bypass Vulnerability

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

A security bypass vulnerability is present in some versions of McAfee VirusScan Enterprise.

Observation

McAfee VirusScan Enterprise is McAfee's anti-malware software.

A security bypass vulnerability is present in some versions of McAfee VirusScan Enterprise. The flaw is due to an unspecified defect in the application. Successful exploitation could allow a local attacker to bypass intended access restrictions.

88776 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2016-141-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3739

Description

The scan detected that the host is missing the following update:
SSA:2016-141-01

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.495349

Slackware 14.0
x86_64
curl-7.49.0-x86_64-1

Slackware 13.0
x86_64
curl-7.49.0-x86_64-1

Slackware 13.1
x86_64
curl-7.49.0-x86_64-1

Slackware 14.1
x86_64
curl-7.49.0-x86_64-1

Slackware 13.37
x86_64
curl-7.49.0-x86_64-1

144615 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1346-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-9770, CVE-2015-8842

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1346-1

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-May/002070.html

SuSE SLES 12 SP1
noarch
systemd-bash-completion-210-104.1

x86_64
libudev1-32bit-210-104.1
systemd-sysvinit-210-104.1
systemd-debuginfo-210-104.1
systemd-debugsource-210-104.1
systemd-debuginfo-32bit-210-104.1
libgudev-1_0-0-debuginfo-32bit-210-104.1
libgudev-1_0-0-210-104.1
libgudev-1_0-0-debuginfo-210-104.1
udev-debuginfo-210-104.1
libudev1-210-104.1
libudev1-debuginfo-32bit-210-104.1
libudev1-debuginfo-210-104.1
systemd-32bit-210-104.1
libgudev-1_0-0-32bit-210-104.1
systemd-210-104.1

udev-210-104.1

SuSE SLED 12 SP1
x86_64
systemd-sysvinit-210-104.1
systemd-debuginfo-210-104.1
libudev1-debuginfo-210-104.1
systemd-debugsource-210-104.1
systemd-debuginfo-32bit-210-104.1
libgudev-1_0-0-debuginfo-32bit-210-104.1
udev-210-104.1
libgudev-1_0-0-210-104.1
libgudev-1_0-0-debuginfo-210-104.1
udev-debuginfo-210-104.1
libudev1-210-104.1
libudev1-debuginfo-32bit-210-104.1
libudev1-32bit-210-104.1
systemd-32bit-210-104.1
libgudev-1_0-0-32bit-210-104.1
systemd-210-104.1

noarch
systemd-bash-completion-210-104.1

144622 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1351-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-9770, CVE-2015-8842

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1351-1

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-May/002071.html

SuSE SLED 12
x86_64
systemd-debuginfo-32bit-210-70.48.1
systemd-210-70.48.1
libgudev-1_0-0-debuginfo-210-70.48.1
systemd-32bit-210-70.48.1
systemd-sysvinit-210-70.48.1
systemd-debuginfo-210-70.48.1
libudev1-debuginfo-32bit-210-70.48.1
libudev1-32bit-210-70.48.1
libgudev-1_0-0-32bit-210-70.48.1
udev-210-70.48.1
systemd-debugsource-210-70.48.1
libgudev-1_0-0-debuginfo-32bit-210-70.48.1
udev-debuginfo-210-70.48.1
libgudev-1_0-0-210-70.48.1
libudev1-debuginfo-210-70.48.1
libudev1-210-70.48.1

noarch
systemd-bash-completion-210-70.48.1

SuSE SLES 12
noarch
systemd-bash-completion-210-70.48.1

x86_64
systemd-debuginfo-32bit-210-70.48.1
systemd-210-70.48.1
libgudev-1_0-0-debuginfo-210-70.48.1
systemd-32bit-210-70.48.1
systemd-sysvinit-210-70.48.1
systemd-debuginfo-210-70.48.1
libudev1-debuginfo-32bit-210-70.48.1
libudev1-32bit-210-70.48.1
libgudev-1_0-0-32bit-210-70.48.1
udev-210-70.48.1
systemd-debugsource-210-70.48.1
libgudev-1_0-0-debuginfo-32bit-210-70.48.1
udev-debuginfo-210-70.48.1
libgudev-1_0-0-210-70.48.1
libudev1-debuginfo-210-70.48.1
libudev1-210-70.48.1

70143 - 7-zip.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

7-zip.fasl3.inc

Observation

7-zip.fasl3.inc

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.

20074 - (APSB16-15) Vulnerabilities in Adobe Flash Player

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

Risk Level: High

CVE: CVE-2016-1096, CVE-2016-1097, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1101, CVE-2016-1102, CVE-2016-1103, CVE-2016-1104, CVE-2016-1105, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, CVE-2016-4109, CVE-2016-4110, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4116, CVE-2016-4117, CVE-2016-4120, CVE-2016-4121

Update Details

CVE is updated

20078 - (APSB16-15) Vulnerabilities in Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1096, CVE-2016-1097, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1101, CVE-2016-1102, CVE-2016-1103, CVE-2016-1104, CVE-2016-1105, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, CVE-2016-4109, CVE-2016-4110, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4116, CVE-2016-4117, CVE-2016-4120, CVE-2016-4121

Update Details

CVE is updated

130497 - Debian Linux 8.0 DSA-3579-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2099

Update Details

Risk is updated

141191 - Red Hat Enterprise Linux RHSA-2016-1079 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1096, CVE-2016-1097, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1101, CVE-2016-1102, CVE-2016-1103, CVE-2016-1104, CVE-2016-1105, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, CVE-2016-4109, CVE-2016-4110, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4116, CVE-2016-4117, CVE-2016-4120, CVE-2016-4121

Update Details

CVE is updated

144446 - SuSE Linux 13.2 openSUSE-SU-2016:0709-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2554

Update Details

Risk is updated

170663 - Amazon Linux AMI ALAS-2016-685 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2554

Update Details

Risk is updated

130476 - Debian Linux 8.0 DSA-3560-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8865, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073

Update Details

Risk is updated

190613 - Fedora Linux 24 FEDORA-2016-f4e73663f4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544

Update Details

Risk is updated

11368 - WordPress x7Host's Videox7 UGC Plugin "listid" Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

11468 - WordPress YT-Audio Plugin "v" Parameter Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

11871 - WordPress WP Forum Multiple SQL Injection Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

181914 - FreeBSD moodle Multiple Vulnerabilities (a430e15d-f93f-11e5-92ce-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-2151, CVE-2016-2152, CVE-2016-2153, CVE-2016-2154, CVE-2016-2155, CVE-2016-2156, CVE-2016-2157, CVE-2016-2158, CVE-2016-2159, CVE-2016-2190

Update Details

Risk is updated

190461 - Fedora Linux 24 FEDORA-2016-9b591e1952 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2151, CVE-2016-2152, CVE-2016-2153, CVE-2016-2154, CVE-2016-2155, CVE-2016-2156, CVE-2016-2157, CVE-2016-2158, CVE-2016-2159, CVE-2016-2190

Update Details

Risk is updated

190484 - Fedora Linux 22 FEDORA-2016-b91d895e5a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2151, CVE-2016-2152, CVE-2016-2153, CVE-2016-2154, CVE-2016-2155, CVE-2016-2156, CVE-2016-2157, CVE-2016-2158, CVE-2016-2159, CVE-2016-2190

Update Details

Risk is updated

190489 - Fedora Linux 23 FEDORA-2016-403715aaec Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2151, CVE-2016-2152, CVE-2016-2153, CVE-2016-2154, CVE-2016-2155, CVE-2016-2156, CVE-2016-2157, CVE-2016-2158, CVE-2016-2159, CVE-2016-2190

Update Details

Risk is updated

5540 - Xunlei Web Thunder DPClient.Vod.1 ActiveX Vulnerability

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

Risk Level: Medium

CVE: CVE-2007-5064

Update Details

Recommendation is updated

12068 - WordPress WP-StarsRateBox Plugin Cross Site Scripting And SQL Injection Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

15758 - WordPress WP Ultimate Email Marketer Plugin Multiple Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server
Risk Level: Medium
CVE: CVE-2013-3263, CVE-2013-3264

Update Details
Recommendation is updated

130389 - Debian Linux 7.0, 8.0 DSA-3472-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2221, CVE-2016-2222

Update Details
Risk is updated

130494 - Debian Linux 8.0 DSA-3577-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4425

Update Details
Risk is updated

130498 - Debian Linux 8.0 DSA-3575-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-3674

Update Details
Risk is updated

144606 - SuSE Linux 13.2 openSUSE-SU-2016:1313-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4049

Update Details
Risk is updated

181718 - FreeBSD librsvg2 Denial Of Service Vulnerability (da634091-a84a-11e5-8f5c-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7557

Update Details

Risk is updated

181725 - FreeBSD librsvg2 Denial Of Service Vulnerability (d6c51737-a84b-11e5-8f5c-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-7558

Update Details

Risk is updated

181879 - FreeBSD wordpress Multiple Vulnerabilities (fef03980-e4c6-11e5-b2bd-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-2221, CVE-2016-2222

Update Details

Risk is updated

181917 - FreeBSD go Remote Denial Of Service (f2217cdf-01e4-11e6-b1ce-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-3959

Update Details

Risk is updated

181940 - FreeBSD jansson Local Denial Of Service Vulnerabilities (a6cd01fa-11bd-11e6-bb3c-9cb654ea3e1c)

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

Risk Level: Medium

CVE: CVE-2016-4425

Update Details

Risk is updated

190485 - Fedora Linux 24 FEDORA-2016-175b56bb05 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3674

Update Details

Risk is updated

190527 - Fedora Linux 24 FEDORA-2016-2940ad5550 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2016-3959

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-3959

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-3959

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-3674

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-3674

Update Details
Risk is updated

190627 - Fedora Linux 22 FEDORA-2016-5a9313e4b4 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-8853

Update Details
Risk is updated

130292 - Debian Linux 8.0 DSA-3375-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5714, CVE-2015-5715, CVE-2015-7989

Update Details

Risk is updated

130363 - Debian Linux 7.0, 8.0 DSA-3444-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1564

Update Details

Risk is updated

181598 - FreeBSD wordpress Multiple Vulnerabilities (f4ce64c2-5bd4-11e5-9040-3c970e169bc2)

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

Risk Level: Medium

CVE: CVE-2015-5714, CVE-2015-5715, CVE-2015-7989

Update Details

Risk is updated

181738 - FreeBSD qemu Denial Of Service Vulnerability In USB EHCI Emulation Support (60cb2055-b1b8-11e5-9728-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-8558

Update Details

Risk is updated

181791 - FreeBSD wordpress XSS Vulnerability (fb754341-c3e2-11e5-b5fe-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-1564

Update Details

Risk is updated

181945 - FreeBSD wordpress Multiple Vulnerabilities (3686917b-164d-11e6-94fa-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-4566, CVE-2016-4567

Update Details

Risk is updated

189773 - Fedora Linux 21 FEDORA-2015-15982 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5714, CVE-2015-5715

Update Details

Risk is updated

189774 - Fedora Linux 23 FEDORA-2015-15983 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5714, CVE-2015-5715

Update Details

Risk is updated

189775 - Fedora Linux 22 FEDORA-2015-15981 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5714, CVE-2015-5715

Update Details

Risk is updated

190192 - Fedora Linux 23 FEDORA-2016-e9bba2bb01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7549, CVE-2015-8558, CVE-2015-8666, CVE-2015-8744, CVE-2015-8745

Update Details

Risk is updated

190219 - Fedora Linux 22 FEDORA-2016-890e612f52 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7549, CVE-2015-8558, CVE-2015-8666, CVE-2015-8744, CVE-2015-8745

Update Details

Risk is updated

32831 - Oracle Solaris 145334-35 Update Is Not Installed

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

Risk Level: Low
CVE: CVE-2015-2616

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32838 - Oracle Solaris 145336-21 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32839 - Oracle Solaris 145333-35 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-2015-2616

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32842 - Oracle Solaris 145335-21 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33082 - Oracle Solaris 145645-06 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33083 - Oracle Solaris 145644-06 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

190630 - Fedora Linux 24 FEDORA-2016-4ce97823af Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4482

Update Details

Risk is updated

45000 - ShellLogon.fasl3

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

45001 - ShellInitialize.fasl3

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70064 - ssh-misc-lib.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70087 - hp.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70088 - ibm.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