2016-JUN-23
FSL version 7.5.829

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

20216 - (S2-037) Apache Struts REST Plugin Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-4438

Description

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

Observation

Apache Struts is a popular Java web application framework.

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

20225 - (APSB16-20) Vulnerabilities In Adobe Brackets

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

Risk Level: High

CVE: CVE-2016-4164, CVE-2016-4165

Description

Multiple vulnerabilities are present in some versions of Adobe Brackets.

Observation

Adobe Brackets is an open source code editor oriented for web designers and front-end developers.

Multiple vulnerabilities are present in some versions of Adobe Brackets. The flaws are due to multiple logic issues. Successful exploitation could allow an attacker to inject arbitrary code or to have unspecified impact in the affected system. Exploitation doesn't require authentication.

The update provided by Adobe bulletin APSB16-20 resolves the issues. The target system is missing this update.

20226 - (APSB16-20) Vulnerabilities In Adobe Brackets

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4164, CVE-2016-4165

Description

Multiple vulnerabilities are present in some versions of Adobe Brackets.

Observation

Adobe Brackets is an open source code editor oriented for web designers and front-end developers.

Multiple vulnerabilities are present in some versions of Adobe Brackets. The flaws are due to multiple logic issues. Successful exploitation could allow an attacker to inject arbitrary code or to have unspecified impact in the affected system. Exploitation doesn't require authentication.

The update provided by Adobe bulletin APSB16-20 resolves the issues. The target system is missing this update.

141211 - Red Hat Enterprise Linux RHSA-2016-1238 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2016-1238

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-June/msg00009.html

RHEL5S
x86_64
flash-plugin-11.2.202.626-1.el5_11

i386
flash-plugin-11.2.202.626-1.el5_11

RHEL6D
x86_64
flash-plugin-11.2.202.626-1.el6_8

i386
flash-plugin-11.2.202.626-1.el6_8

RHEL6S
x86_64
flash-plugin-11.2.202.626-1.el6_8

i386
flash-plugin-11.2.202.626-1.el6_8

RHEL6WS
x86_64
flash-plugin-11.2.202.626-1.el6_8

i386
flash-plugin-11.2.202.626-1.el6_8

RHEL5D
x86_64
flash-plugin-11.2.202.626-1.el5_11

i386
flash-plugin-11.2.202.626-1.el5_11

141213 - Red Hat Enterprise Linux RHSA-2016-1237 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8895, CVE-2015-8896, CVE-2015-8897, CVE-2015-8898, CVE-2016-5118, CVE-2016-5239, CVE-2016-5240

Description

The scan detected that the host is missing the following update:
RHSA-2016-1237

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-June/msg00008.html

RHEL7S
ppc64
ImageMagick-debuginfo-6.7.8.9-15.el7_2
ImageMagick-6.7.8.9-15.el7_2
ImageMagick-c++-6.7.8.9-15.el7_2
ImageMagick-c++-devel-6.7.8.9-15.el7_2
ImageMagick-perl-6.7.8.9-15.el7_2
ImageMagick-devel-6.7.8.9-15.el7_2
ImageMagick-doc-6.7.8.9-15.el7_2

RHEL6S
i386
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-debuginfo-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

x86_64
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-debuginfo-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

RHEL6WS
x86_64
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-debuginfo-6.7.2.7-5.el6_8
ImageMagick-6.7.2.7-5.el6_8

i386
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-debuginfo-6.7.2.7-5.el6_8
ImageMagick-6.7.2.7-5.el6_8

RHEL7D
x86_64
ImageMagick-debuginfo-6.7.8.9-15.el7_2
ImageMagick-6.7.8.9-15.el7_2
ImageMagick-c++-6.7.8.9-15.el7_2
ImageMagick-c++-devel-6.7.8.9-15.el7_2
ImageMagick-perl-6.7.8.9-15.el7_2
ImageMagick-devel-6.7.8.9-15.el7_2
ImageMagick-doc-6.7.8.9-15.el7_2

RHEL6D
x86_64
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-debuginfo-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

i386
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-debuginfo-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8

RHEL7WS
x86_64
ImageMagick-debuginfo-6.7.8.9-15.el7_2
ImageMagick-6.7.8.9-15.el7_2
ImageMagick-c++-6.7.8.9-15.el7_2
ImageMagick-c++-devel-6.7.8.9-15.el7_2
ImageMagick-perl-6.7.8.9-15.el7_2
ImageMagick-devel-6.7.8.9-15.el7_2
ImageMagick-doc-6.7.8.9-15.el7_2

144687 - SuSE SLES 11 SP4 SUSE-SU-2016:1604-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1604-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002123.html

SuSE SLES 11 SP4
i586
libxml2-python-2.7.6-0.44.4
libxml2-doc-2.7.6-0.44.1
libxml2-2.7.6-0.44.1

x86_64
libxml2-32bit-2.7.6-0.44.1
libxml2-python-2.7.6-0.44.4
libxml2-doc-2.7.6-0.44.1
libxml2-2.7.6-0.44.1

144690 - SuSE Linux 13.2 openSUSE-SU-2016:1594-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1762, 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-2016-3627, CVE-2016-3705, CVE-2016-4483

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1594-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00064.html

SuSE Linux 13.2
i586
python-libxml2-debugsource-2.9.4-7.17.1
libxml2-2-debuginfo-2.9.4-7.17.1
libxml2-2-2.9.4-7.17.1
libxml2-devel-2.9.4-7.17.1
python-libxml2-debuginfo-2.9.4-7.17.1
libxml2-tools-2.9.4-7.17.1
python-libxml2-2.9.4-7.17.1
libxml2-tools-debuginfo-2.9.4-7.17.1
libxml2-debugsource-2.9.4-7.17.1

noarch
libxml2-doc-2.9.4-7.17.1

x86_64
python-libxml2-debugsource-2.9.4-7.17.1
libxml2-2-debuginfo-2.9.4-7.17.1
libxml2-2-debuginfo-32bit-2.9.4-7.17.1
libxml2-2-2.9.4-7.17.1
libxml2-devel-2.9.4-7.17.1
libxml2-2-32bit-2.9.4-7.17.1
python-libxml2-debuginfo-2.9.4-7.17.1
libxml2-tools-2.9.4-7.17.1
python-libxml2-2.9.4-7.17.1
libxml2-devel-32bit-2.9.4-7.17.1
libxml2-tools-debuginfo-2.9.4-7.17.1
libxml2-debugsource-2.9.4-7.17.1

144701 - SuSE SLES 11 SP4 SUSE-SU-2016:1610-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5118

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1610-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002124.html

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.40.1

x86_64
libMagickCore1-6.4.3.6-7.40.1
libMagickCore1-32bit-6.4.3.6-7.40.1

144704 - SuSE SLED 12, 12 SP1 SUSE-SU-2016:1613-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1613-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002125.html

SuSE SLED 12
x86_64
flash-player-gnome-11.2.202.626-133.1
flash-player-11.2.202.626-133.1

SuSE SLED 12 SP1
x86_64
flash-player-gnome-11.2.202.626-133.1
flash-player-11.2.202.626-133.1

160111 - CentOS 6, 7 CESA-2016-1237 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8895, CVE-2015-8896, CVE-2015-8897, CVE-2015-8898, CVE-2016-5118, CVE-2016-5239, CVE-2016-5240

Description

The scan detected that the host is missing the following update:
CESA-2016-1237

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-June/021910.html
http://lists.centos.org/pipermail/centos-announce/2016-June/021909.html

CentOS 7
x86_64
ImageMagick-6.7.8.9-15.el7_2
ImageMagick-c++-6.7.8.9-15.el7_2
ImageMagick-c++-devel-6.7.8.9-15.el7_2
ImageMagick-perl-6.7.8.9-15.el7_2
ImageMagick-devel-6.7.8.9-15.el7_2
ImageMagick-doc-6.7.8.9-15.el7_2

i686
ImageMagick-c++-6.7.8.9-15.el7_2
ImageMagick-6.7.8.9-15.el7_2
ImageMagick-c++-devel-6.7.8.9-15.el7_2
ImageMagick-devel-6.7.8.9-15.el7_2

CentOS 6
x86_64
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

i686
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

163108 - Oracle Enterprise Linux ELSA-2016-1237 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8895, CVE-2015-8896, CVE-2015-8897, CVE-2015-8898, CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-5118, CVE-2016-5239, CVE-2016-5240

Description

The scan detected that the host is missing the following update:
ELSA-2016-1237

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-June/006121.html
http://oss.oracle.com/pipermail/el-errata/2016-June/006120.html

OEL7
x86_64
ImageMagick-6.7.8.9-15.el7_2
ImageMagick-c++-6.7.8.9-15.el7_2
ImageMagick-c++-devel-6.7.8.9-15.el7_2
ImageMagick-perl-6.7.8.9-15.el7_2
ImageMagick-devel-6.7.8.9-15.el7_2
ImageMagick-doc-6.7.8.9-15.el7_2

OEL6
x86_64
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

i386
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

163109 - Oracle Enterprise Linux ELSA-2016-3576 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2109

Description

The scan detected that the host is missing the following update:
ELSA-2016-3576

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-June/006124.html

OEL5
i386
openssl-devel-0.9.8e-40.0.2.el5_11
openssl-0.9.8e-40.0.2.el5_11
openssl-perl-0.9.8e-40.0.2.el5_11

x86_64

openssl-devel-0.9.8e-40.0.2.el5_11
openssl-0.9.8e-40.0.2.el5_11
openssl-perl-0.9.8e-40.0.2.el5_11

174973 - Scientific Linux Security ERRATA Important: spice-server on SL6.x x86_64 (1606-4989)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: spice-server on SL6.x x86_64 (1606-4989)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=4989

SL6
x86_64
spice-server-debuginfo-0.12.4-13.el6.1
spice-server-0.12.4-13.el6.1
spice-server-devel-0.12.4-13.el6.1

174976 - Scientific Linux Security ERRATA Important: ImageMagick on SL6.x, SL7.x i386/x86_64 (1606-6155)

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

Risk Level: High

CVE: CVE-2015-8895, CVE-2015-8896, CVE-2015-8897, CVE-2015-8898, CVE-2016-5118, CVE-2016-5239, CVE-2016-5240

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: ImageMagick on SL6.x, SL7.x i386/x86_64 (1606-6155)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=6155

SL7
x86_64
ImageMagick-debuginfo-6.7.8.9-15.el7_2
ImageMagick-6.7.8.9-15.el7_2
ImageMagick-c++-6.7.8.9-15.el7_2
ImageMagick-c++-devel-6.7.8.9-15.el7_2
ImageMagick-perl-6.7.8.9-15.el7_2
ImageMagick-devel-6.7.8.9-15.el7_2
ImageMagick-doc-6.7.8.9-15.el7_2

SL6
x86_64
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8

ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-debuginfo-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

i386
ImageMagick-6.7.2.7-5.el6_8
ImageMagick-devel-6.7.2.7-5.el6_8
ImageMagick-perl-6.7.2.7-5.el6_8
ImageMagick-doc-6.7.2.7-5.el6_8
ImageMagick-c++-6.7.2.7-5.el6_8
ImageMagick-debuginfo-6.7.2.7-5.el6_8
ImageMagick-c++-devel-6.7.2.7-5.el6_8

178185 - Gentoo Linux GLSA-201606-07 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1503, CVE-2016-1504

Description

The scan detected that the host is missing the following update:
GLSA-201606-07

Observation

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

https://security.gentoo.org/glsa/201606-07

Affected packages:
net-misc/dhcpcd < 6.10.0

178187 - Gentoo Linux GLSA-201606-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6501, CVE-2014-9705, CVE-2014-9709, CVE-2015-0231, CVE-2015-0273, CVE-2015-1351, CVE-2015-1352, CVE-2015-2301, CVE-2015-2348, CVE-2015-2783, CVE-2015-2787, CVE-2015-3329, CVE-2015-3330, CVE-2015-4021, CVE-2015-4022, CVE-2015-4025, CVE-2015-4026, CVE-2015-4147, CVE-2015-4148, CVE-2015-4642, CVE-2015-4643, CVE-2015-4644, CVE-2015-6831, CVE-2015-6832, CVE-2015-6833, CVE-2015-6834, CVE-2015-6835, CVE-2015-6836, CVE-2015-6837, CVE-2015-6838, CVE-2015-7803, CVE-2015-7804

Description

The scan detected that the host is missing the following update:
GLSA-201606-10

Observation

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

https://security.gentoo.org/glsa/201606-10

Affected packages:
dev-lang/php < 5.6.19

178188 - Gentoo Linux GLSA-201606-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1019, CVE-2016-4117, CVE-2016-4120, CVE-2016-4121, CVE-2016-4160, CVE-2016-4161, CVE-2016-4162, CVE-2016-4163, CVE-2016-4171

Description

The scan detected that the host is missing the following update:
GLSA-201606-08

Observation

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

https://security.gentoo.org/glsa/201606-08

Affected packages:
www-plugins/adobe-flash < 11.2.202.626

178189 - Gentoo Linux GLSA-201606-05 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
GLSA-201606-05

Observation

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

https://security.gentoo.org/glsa/201606-05

Affected packages:
app-emulation/spice < 0.12.7-r1

181978 - FreeBSD flash Multiple Vulnerabilities (07888b49-35c4-11e6-8e82-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-1006, CVE-2016-1011, CVE-2016-1012, CVE-2016-1013, CVE-2016-1014, CVE-2016-1015, CVE-2016-1016, CVE-2016-1017, CVE-2016-1018, CVE-2016-1019, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1030, CVE-2016-1031, CVE-2016-1032, CVE-2016-1033

Description

The scan detected that the host is missing the following update:
flash -- multiple vulnerabilities (07888b49-35c4-11e6-8e82-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/07888b49-35c4-11e6-8e82-002590263bf5.html

Affected packages:
linux-c6-flashplugin < 11.2r202.616
linux-c6_64-flashplugin < 11.2r202.616
linux-f10-flashplugin < 11.2r202.616

181979 - FreeBSD flash Multiple Vulnerabilities (0c6b008d-35c4-11e6-8e82-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD 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, CVE-2016-4160, CVE-2016-4161, CVE-2016-4162, CVE-2016-4163

Description

The scan detected that the host is missing the following update:
flash -- multiple vulnerabilities (0c6b008d-35c4-11e6-8e82-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/0c6b008d-35c4-11e6-8e82-002590263bf5.html

Affected packages:
linux-c6-flashplugin < 11.2r202.621
linux-c6_64-flashplugin < 11.2r202.621
linux-f10-flashplugin < 11.2r202.621

181982 - FreeBSD flash Multiple Vulnerabilities (0e3dfdde-35c4-11e6-8e82-002590263bf5)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
flash -- multiple vulnerabilities (0e3dfdde-35c4-11e6-8e82-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/0e3dfdde-35c4-11e6-8e82-002590263bf5.html

Affected packages:

linux-c6-flashplugin < 11.2r202.626
linux-c6_64-flashplugin < 11.2r202.626
linux-f10-flashplugin < 11.2r202.626

185323 - Ubuntu Linux 14.04, 15.10, 16.04 USN-3014-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
USN-3014-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-June/003471.html

Ubuntu 16.04

libspice-server1_0.12.6-4ubuntu0.1

Ubuntu 15.10

libspice-server1_0.12.5-1.1ubuntu2.1

Ubuntu 14.04

libspice-server1_0.12.4-0nocelt2ubuntu1.3

20128 - (VideoLAN-SA-1601) VideoLAN VLC Media Player IMA File Handling Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2016-5108

Description

A buffer overflow vulnerability is present in some versions of VideoLAN VLC Media Player.

Observation

VideoLAN VLC Media Player is a popular open source media player.

A buffer overflow vulnerability is present in some versions of VideoLAN VLC Media Player. The flaw is due to a buffer overflow in DecodeAdpcmImaQT() in 'modules/codec/adpcm.c' when handling specially crafted QuickTime IMA file. Successful exploitation could allow an attacker to cause denial of service or execute arbitrary code.

20129 - (VMSA-2016-0005) VMware vCenter Server JMX RMI Remote Code Execution

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

Risk Level: High

CVE: CVE-2016-3427

Description

A remote code execution vulnerability is present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

A remote code execution vulnerability is present in some versions of VMware vCenter Server. The flaw lies in the RMI server of Oracle JRE JMX. Successful exploitation could allow an attacker to execute remote code affecting confidentiality, integrity and availability. Authentication is not required to exploit this vulnerability.

20130 - (VMSA-2016-0005) VMware vCenter Server JMX RMI Remote Code Execution

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-3427

Description

A remote code execution vulnerability is present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

A remote code execution vulnerability is present in some versions of VMware vCenter Server. The flaw lies in the RMI server of Oracle JRE JMX. Successful exploitation could allow an attacker to execute remote code affecting confidentiality, integrity and availability. Authentication is not required to exploit this vulnerability.

20223 - (VMSA-2016-0005) VMware vSphere Replication JMX RMI Remote Code Execution

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-3427

Description

A remote code execution vulnerability is present in some versions of VMware vSphere Replication.

Observation

VMware vSphere Replication is a replication solution for vSphere virtual machines.

A remote code execution vulnerability is present in some versions of VMware vSphere Replication. The flaw lies in the RMI server of Oracle JRE JMX. Successful exploitation could allow an attacker to execute remote code affecting confidentiality, integrity and availability. Authentication is not required to exploit this vulnerability.

20224 - (ESA-2016-072) EMC NetWorker Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-0916

Description

A vulnerability is present in some versions of EMC NetWorker.

Observation

EMC NetWorker is an enterprise backup and recovery solution.

A vulnerability is present in some versions of EMC NetWorker. The flaw lies in the authentication implementation. Successful exploitation could allow an attacker to execute remote code by leveraging access to a different NetWorker instance.

132243 - Oracle VM OVMSA-2016-0077 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-3378, CVE-2012-0060, CVE-2012-0061, CVE-2012-0815, CVE-2013-6435

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0077

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000492.html

OVM3.2
x86_64
rpm-libs-4.4.2.3-36.0.1.el5_11
popt-1.10.2.3-36.0.1.el5_11
rpm-python-4.4.2.3-36.0.1.el5_11
rpm-4.4.2.3-36.0.1.el5_11

132249 - Oracle VM OVMSA-2016-0070 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5600, CVE-2016-3115

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0070

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000482.html

OVM3.2
x86_64
openssh-server-4.3p2-82.0.2.el5
openssh-clients-4.3p2-82.0.2.el5
openssh-4.3p2-82.0.2.el5

132256 - Oracle VM OVMSA-2016-0055 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-1033, CVE-2012-1667, CVE-2012-3817, CVE-2012-4244, CVE-2012-5166, CVE-2014-8500, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000, CVE-2015-8704, CVE-2016-1285, CVE-2016-1286

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0055

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000477.html

OVM3.2
x86_64
bind-utils-9.3.6-25.P1.el5_11.8
bind-libs-9.3.6-25.P1.el5_11.8

20120 - Cisco Adaptive Security Appliance VPN Memory Block Exhaustion Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1379

Description

A denial of service vulnerability is present in some versions of Cisco Adaptive Security Appliance Software.

Observation

Cisco Adaptive Security Appliance Software is an operating system used in Cisco ASA device.

A denial of service vulnerability is present in some versions of Cisco Adaptive Security Appliance Software. The flaw occurs due to and error in the implementation of ICMP error handling for IPsec packets. Successful exploitation could allow an attacker to consume the available memory causing instability or cause the system to stop forwarding traffic, resulting in a denial of service condition.

20196 - (HPSBGN03609) HPE LoadRunner Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-4359, CVE-2016-4360, CVE-2016-4361

Description

Multiple vulnerabilities are present in some versions of HP LoadRunner.

Observation

HP LoadRunner is a test automation software.

Multiple vulnerabilities are present in some versions of HP LoadRunner. The flaws lie in multiple components. Successful exploitation could allow a remote attacker to cause a denial of service, delete arbitrary files, or execute arbitrary code.

20198 - Apache Cordova iOS Security Bypass And Arbitrary Plugin Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-5207, CVE-2015-5208

Description

Two vulnerabilities are present in some versions of Cordova iOS.

Observation

Apache Cordova is a mobile application development framework.

Two vulnerabilities are present in some versions of Cordova iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to bypass the URL access restrictions provided by the whitelist, or execute arbitrary plugins.

Notes:

The checks only search the Cordova package installed globally.

20199 - Apache Cordova iOS Security Bypass And Arbitrary Plugin Execution Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-5207, CVE-2015-5208

Description

Two vulnerabilities are present in some versions of Cordova iOS.

Observation

Apache Cordova is a mobile application development framework.

Two vulnerabilities are present in some versions of Cordova iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to bypass the URL access restrictions provided by the whitelist, or execute arbitrary plugins.

Notes:

The checks only search the Cordova package installed globally.

20210 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.2

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

Risk Level: High

CVE: CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2824, CVE-2016-2826, CVE-2016-2828, CVE-2016-2831

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, conduct spoofing attacks, escalate privileges or remotely execute arbitrary code.

20211 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2824, CVE-2016-2826, CVE-2016-2828, CVE-2016-2831

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, conduct spoofing attacks, escalate privileges or remotely execute arbitrary code.

20217 - Apache ActiveMQ Fileserver Web Application Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-3088

Description

Multiple vulnerabilities are present in some versions of Apache ActiveMQ.

Observation

Apache ActiveMQ is an open source messaging server.

Multiple vulnerabilities are present in some versions of Apache ActiveMQ. The flaws lie in the Fileserver web application. Successful exploitation could allow an attacker to execute arbitrary code.

88786 - Slackware Linux 14.1 SSA:2016-172-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1283

Description

The scan detected that the host is missing the following update:
SSA:2016-172-02

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.343110

Slackware 14.1
x86_64
pcre-8.39-x86_64-1

132241 - Oracle VM OVMSA-2016-0081 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6375, CVE-2014-3615, CVE-2015-5307, CVE-2015-7504, CVE-2015-7835, CVE-2015-7969, CVE-2015-7971, CVE-2015-8339, CVE-2015-8340, CVE-2015-8550, CVE-2015-8554, CVE-2015-8555, CVE-2016-1570, CVE-2016-1571, CVE-2016-2270, CVE-2016-3158, CVE-2016-3159, CVE-2016-3710, CVE-2016-3712, CVE-2016-3960

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0081

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000495.html

OVM3.2
x86_64
xen-devel-4.1.3-25.el5.223.26
xen-4.1.3-25.el5.223.26
xen-tools-4.1.3-25.el5.223.26

132242 - Oracle VM OVMSA-2016-0066 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1568, CVE-2015-2721, CVE-2015-2730, CVE-2015-7181, CVE-2015-7182, CVE-2016-1950

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0066

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000488.html

OVM3.2
x86_64
nss-3.21.0-6.el5_11

132244 - Oracle VM OVMSA-2016-0076 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-5195, CVE-2012-5526, CVE-2012-6329, CVE-2013-1667

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0076

Observation

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

For more information see:

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000491.html

OVM3.2
x86_64
perl-5.8.8-43.el5_11

132247 - Oracle VM OVMSA-2016-0060 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-7509, CVE-2015-8215, CVE-2015-8543, CVE-2015-8767, CVE-2016-4565

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0060

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000481.html

OVM3.2
x86_64
kernel-uek-firmware-2.6.39-400.279.1.el5uek
kernel-uek-2.6.39-400.279.1.el5uek

132254 - Oracle VM OVMSA-2016-0057 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-0292

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0057

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000480.html

OVM3.2
x86_64
dbus-glib-0.73-11.el5_9

132257 - Oracle VM OVMSA-2016-0058 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-0997, CVE-2011-2748, CVE-2011-2749, CVE-2012-3571

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0058

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000486.html

OVM3.2
x86_64
dhclient-3.0.5-33.el5_9

132258 - Oracle VM OVMSA-2016-0065 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2015-7183

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0065

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000485.html

OVM3.2
x86_64
nspr-4.11.0-1.el5_11

141210 - Red Hat Enterprise Linux RHSA-2016-1262 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1704

Description

The scan detected that the host is missing the following update:
RHSA-2016-1262

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-June/msg00010.html

RHEL6D
x86_64
chromium-browser-51.0.2704.103-1.el6
chromium-browser-debuginfo-51.0.2704.103-1.el6

i386
chromium-browser-51.0.2704.103-1.el6
chromium-browser-debuginfo-51.0.2704.103-1.el6

RHEL6S
x86_64
chromium-browser-51.0.2704.103-1.el6
chromium-browser-debuginfo-51.0.2704.103-1.el6

i386
chromium-browser-51.0.2704.103-1.el6
chromium-browser-debuginfo-51.0.2704.103-1.el6

RHEL6WS
x86_64
chromium-browser-51.0.2704.103-1.el6
chromium-browser-debuginfo-51.0.2704.103-1.el6

i386
chromium-browser-51.0.2704.103-1.el6
chromium-browser-debuginfo-51.0.2704.103-1.el6

141212 - Red Hat Enterprise Linux RHSA-2016-1267 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4444, CVE-2016-4445, CVE-2016-4446, CVE-2016-4989

Description

The scan detected that the host is missing the following update:
RHSA-2016-1267

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-June/msg00011.html

RHEL6D
i386
setroubleshoot-doc-3.0.47-12.el6_8
setroubleshoot-server-3.0.47-12.el6_8
setroubleshoot-3.0.47-12.el6_8
setroubleshoot-debuginfo-3.0.47-12.el6_8

noarch
setroubleshoot-plugins-3.0.40-3.1.el6_8

x86_64
setroubleshoot-doc-3.0.47-12.el6_8
setroubleshoot-server-3.0.47-12.el6_8
setroubleshoot-3.0.47-12.el6_8
setroubleshoot-debuginfo-3.0.47-12.el6_8

RHEL6S
i386
setroubleshoot-doc-3.0.47-12.el6_8
setroubleshoot-server-3.0.47-12.el6_8

setroubleshoot-3.0.47-12.el6_8
setroubleshoot-debuginfo-3.0.47-12.el6_8

noarch
setroubleshoot-plugins-3.0.40-3.1.el6_8

x86_64
setroubleshoot-doc-3.0.47-12.el6_8
setroubleshoot-server-3.0.47-12.el6_8
setroubleshoot-3.0.47-12.el6_8
setroubleshoot-debuginfo-3.0.47-12.el6_8

RHEL6WS
i386
setroubleshoot-server-3.0.47-12.el6_8
setroubleshoot-3.0.47-12.el6_8
setroubleshoot-debuginfo-3.0.47-12.el6_8

noarch
setroubleshoot-plugins-3.0.40-3.1.el6_8

x86_64
setroubleshoot-server-3.0.47-12.el6_8
setroubleshoot-3.0.47-12.el6_8
setroubleshoot-debuginfo-3.0.47-12.el6_8

144683 - SuSE SLES 11 SP4 SUSE-SU-2016:1584-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1584-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002116.html

SuSE SLES 11 SP4
i586
ntp-doc-4.2.8p8-14.1
ntp-4.2.8p8-14.1

x86_64
ntp-doc-4.2.8p8-14.1
ntp-4.2.8p8-14.1

144685 - SuSE Linux 13.2 openSUSE-SU-2016:1583-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1583-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00058.html

SuSE Linux 13.2
x86_64
ntp-4.2.8p8-25.18.1
ntp-debuginfo-4.2.8p8-25.18.1
ntp-doc-4.2.8p8-25.18.1
ntp-debugsource-4.2.8p8-25.18.1

i586
ntp-4.2.8p8-25.18.1
ntp-debuginfo-4.2.8p8-25.18.1
ntp-doc-4.2.8p8-25.18.1
ntp-debugsource-4.2.8p8-25.18.1

144686 - SuSE SLES 11 SP4 SUSE-SU-2016:1640-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1640-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002133.html

SuSE SLES 11 SP4
i586
ctdb-1.0.114.6-0.14.1

x86_64
ctdb-1.0.114.6-0.14.1

144688 - SuSE Linux 13.2 openSUSE-SU-2016:1637-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1637-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00081.html

SuSE Linux 13.2
x86_64
ctdb-devel-2.5.3-5.3.1
ctdb-pcp-pmda-debuginfo-2.5.3-5.3.1
ctdb-debuginfo-2.5.3-5.3.1
ctdb-2.5.3-5.3.1
ctdb-pcp-pmda-2.5.3-5.3.1
ctdb-debugsource-2.5.3-5.3.1

i586
ctdb-devel-2.5.3-5.3.1
ctdb-pcp-pmda-debuginfo-2.5.3-5.3.1
ctdb-debuginfo-2.5.3-5.3.1
ctdb-2.5.3-5.3.1
ctdb-pcp-pmda-2.5.3-5.3.1
ctdb-debugsource-2.5.3-5.3.1

144689 - SuSE Linux 13.2 openSUSE-SU-2016:1635-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5301

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1635-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00079.html

SuSE Linux 13.2
x86_64
python-libtorrent-rasterbar-debuginfo-0.16.17-2.5.1
python-libtorrent-rasterbar-0.16.17-2.5.1
libtorrent-rasterbar-debugsource-0.16.17-2.5.1
libtorrent-rasterbar-devel-0.16.17-2.5.1
libtorrent-rasterbar7-0.16.17-2.5.1
libtorrent-rasterbar7-debuginfo-0.16.17-2.5.1
libtorrent-rasterbar-doc-0.16.17-2.5.1

i586
python-libtorrent-rasterbar-debuginfo-0.16.17-2.5.1
python-libtorrent-rasterbar-0.16.17-2.5.1
libtorrent-rasterbar-debugsource-0.16.17-2.5.1
libtorrent-rasterbar-devel-0.16.17-2.5.1
libtorrent-rasterbar7-0.16.17-2.5.1
libtorrent-rasterbar7-debuginfo-0.16.17-2.5.1
libtorrent-rasterbar-doc-0.16.17-2.5.1

144693 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1596-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1596-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002119.html

SuSE SLED 12
x86_64
kernel-default-devel-3.12.55-52.45.1
kernel-xen-3.12.55-52.45.1
kernel-xen-debugsource-3.12.55-52.45.1
kernel-default-extra-3.12.55-52.45.1
kernel-xen-devel-3.12.55-52.45.1
kernel-default-debuginfo-3.12.55-52.45.1
kernel-xen-debuginfo-3.12.55-52.45.1
kernel-default-3.12.55-52.45.1
kernel-syms-3.12.55-52.45.1
kernel-default-extra-debuginfo-3.12.55-52.45.1
kernel-default-debugsource-3.12.55-52.45.1

noarch
kernel-devel-3.12.55-52.45.1
kernel-macros-3.12.55-52.45.1
kernel-source-3.12.55-52.45.1

SuSE SLES 12
noarch
kernel-devel-3.12.55-52.45.1
kernel-macros-3.12.55-52.45.1
kernel-source-3.12.55-52.45.1

x86_64
kernel-xen-3.12.55-52.45.1
kernel-xen-base-debuginfo-3.12.55-52.45.1
kernel-syms-3.12.55-52.45.1
kernel-xen-base-3.12.55-52.45.1
kernel-default-debuginfo-3.12.55-52.45.1
kernel-default-debugsource-3.12.55-52.45.1
kernel-xen-debuginfo-3.12.55-52.45.1
kernel-default-3.12.55-52.45.1
kernel-xen-debugsource-3.12.55-52.45.1
kernel-xen-devel-3.12.55-52.45.1
kernel-default-base-debuginfo-3.12.55-52.45.1
kernel-default-base-3.12.55-52.45.1
kernel-default-devel-3.12.55-52.45.1

144695 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1620-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0505, CVE-2016-0546, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0606, CVE-2016-0608, CVE-2016-0609, CVE-2016-0616, 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-2016-0651, CVE-2016-0655, CVE-2016-0666, CVE-2016-0668, CVE-2016-2047

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1620-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002129.html

SuSE SLES 12 SP1
x86_64
mariadb-tools-debuginfo-10.0.25-6.1
libmysqlclient18-debuginfo-10.0.25-6.1
libmysqlclient18-10.0.25-6.1
mariadb-errormessages-10.0.25-6.1
libmysqlclient18-debuginfo-32bit-10.0.25-6.1
mariadb-debugsource-10.0.25-6.1
libmysqlclient18-32bit-10.0.25-6.1
mariadb-client-debuginfo-10.0.25-6.1
mariadb-10.0.25-6.1
mariadb-client-10.0.25-6.1
mariadb-debuginfo-10.0.25-6.1
mariadb-tools-10.0.25-6.1

SuSE SLED 12 SP1
x86_64
mariadb-client-debuginfo-10.0.25-6.1
libmysqlclient18-debuginfo-10.0.25-6.1
libmysqlclient18-10.0.25-6.1
mariadb-errormessages-10.0.25-6.1
libmysqlclient18-debuginfo-32bit-10.0.25-6.1
libmysqlclient18-32bit-10.0.25-6.1
libmysqlclient_r18-32bit-10.0.25-6.1
libmysqlclient_r18-10.0.25-6.1
mariadb-10.0.25-6.1
mariadb-debugsource-10.0.25-6.1
mariadb-debuginfo-10.0.25-6.1
mariadb-client-10.0.25-6.1

144697 - SuSE Linux 13.2 openSUSE-SU-2016:1612-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5350, CVE-2016-5351, CVE-2016-5353, CVE-2016-5354, CVE-2016-5355, CVE-2016-5356, CVE-2016-5357, CVE-2016-5358

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1612-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00068.html

SuSE Linux 13.2
x86_64
wireshark-ui-gtk-debuginfo-1.12.12-38.1
wireshark-ui-qt-debuginfo-1.12.12-38.1
wireshark-ui-gtk-1.12.12-38.1
wireshark-debuginfo-1.12.12-38.1
wireshark-ui-qt-1.12.12-38.1
wireshark-debugsource-1.12.12-38.1
wireshark-devel-1.12.12-38.1
wireshark-1.12.12-38.1

i586
wireshark-ui-gtk-debuginfo-1.12.12-38.1
wireshark-ui-qt-debuginfo-1.12.12-38.1
wireshark-ui-gtk-1.12.12-38.1
wireshark-debuginfo-1.12.12-38.1
wireshark-ui-qt-1.12.12-38.1
wireshark-debugsource-1.12.12-38.1
wireshark-devel-1.12.12-38.1
wireshark-1.12.12-38.1

144698 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1619-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0505, CVE-2016-0546, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0606, CVE-2016-0608, CVE-2016-0609, CVE-2016-0616, 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-2016-0651, CVE-2016-0655, CVE-2016-0666, CVE-2016-0668, CVE-2016-2047

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1619-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002128.html

SuSE SLED 12
x86_64
mariadb-client-debuginfo-10.0.25-20.6.1
libmysqlclient_r18-10.0.25-20.6.1
libmysqlclient18-10.0.25-20.6.1
mariadb-debugsource-10.0.25-20.6.1
libmysqlclient18-32bit-10.0.25-20.6.1
mariadb-10.0.25-20.6.1
mariadb-debuginfo-10.0.25-20.6.1
libmysqlclient18-debuginfo-10.0.25-20.6.1
mariadb-errormessages-10.0.25-20.6.1

libmysqlclient_r18-32bit-10.0.25-20.6.1
mariadb-client-10.0.25-20.6.1
libmysqlclient18-debuginfo-32bit-10.0.25-20.6.1

SuSE SLES 12
x86_64
mariadb-client-debuginfo-10.0.25-20.6.1
libmysqlclient18-debuginfo-32bit-10.0.25-20.6.1
libmysqlclient18-10.0.25-20.6.1
mariadb-debugsource-10.0.25-20.6.1
libmysqlclient18-32bit-10.0.25-20.6.1
mariadb-tools-10.0.25-20.6.1
mariadb-10.0.25-20.6.1
mariadb-debuginfo-10.0.25-20.6.1
libmysqlclient18-debuginfo-10.0.25-20.6.1
mariadb-errormessages-10.0.25-20.6.1
mariadb-client-10.0.25-20.6.1
mariadb-tools-debuginfo-10.0.25-20.6.1

144700 - SuSE SLED 12, 12 SP1 SUSE-SU-2016:1633-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7456, CVE-2015-8876, CVE-2015-8877, CVE-2015-8879, CVE-2016-5093, CVE-2016-5094, CVE-2016-5095, CVE-2016-5096

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1633-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002130.html

SuSE SLED 12
x86_64
libc-client2007e_suse-2007e_suse-19.1
imap-debuginfo-2007e_suse-19.1
libc-client2007e_suse-debuginfo-2007e_suse-19.1
imap-debugsource-2007e_suse-19.1

SuSE SLED 12 SP1
x86_64
libc-client2007e_suse-2007e_suse-19.1
imap-debuginfo-2007e_suse-19.1
libc-client2007e_suse-debuginfo-2007e_suse-19.1
imap-debugsource-2007e_suse-19.1

144703 - SuSE Linux 13.2 openSUSE-SU-2016:1626-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1704

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1626-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00073.html

SuSE Linux 13.2
x86_64
chromium-ffmpegsumo-debuginfo-51.0.2704.103-108.1
chromium-51.0.2704.103-108.1
chromium-ffmpegsumo-51.0.2704.103-108.1
chromium-debuginfo-51.0.2704.103-108.1
chromium-debugsource-51.0.2704.103-108.1
chromedriver-debuginfo-51.0.2704.103-108.1
chromedriver-51.0.2704.103-108.1
chromium-desktop-kde-51.0.2704.103-108.1
chromium-desktop-gnome-51.0.2704.103-108.1

i586
chromium-ffmpegsumo-debuginfo-51.0.2704.103-108.1
chromium-51.0.2704.103-108.1
chromium-ffmpegsumo-51.0.2704.103-108.1
chromium-debuginfo-51.0.2704.103-108.1
chromium-debugsource-51.0.2704.103-108.1
chromedriver-debuginfo-51.0.2704.103-108.1
chromedriver-51.0.2704.103-108.1
chromium-desktop-kde-51.0.2704.103-108.1
chromium-desktop-gnome-51.0.2704.103-108.1

160112 - CentOS 6 CESA-2016-1267 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4444, CVE-2016-4445, CVE-2016-4446, CVE-2016-4989

Description

The scan detected that the host is missing the following update:
CESA-2016-1267

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-June/021914.html
http://lists.centos.org/pipermail/centos-announce/2016-June/021913.html

CentOS 6
i686
setroubleshoot-doc-3.0.47-12.el6_8
setroubleshoot-3.0.47-12.el6_8
setroubleshoot-server-3.0.47-12.el6_8

noarch
setroubleshoot-plugins-3.0.40-3.1.el6_8

x86_64
setroubleshoot-doc-3.0.47-12.el6_8
setroubleshoot-3.0.47-12.el6_8
setroubleshoot-server-3.0.47-12.el6_8

163107 - Oracle Enterprise Linux ELSA-2016-1267 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4444, CVE-2016-4445, CVE-2016-4446, CVE-2016-4989

Description

The scan detected that the host is missing the following update:
ELSA-2016-1267

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-June/006126.html

OEL6
x86_64
setroubleshoot-doc-3.0.47-12.0.1.el6_8
setroubleshoot-plugins-3.0.40-3.1.0.1.el6_8
setroubleshoot-3.0.47-12.0.1.el6_8
setroubleshoot-server-3.0.47-12.0.1.el6_8

i386
setroubleshoot-doc-3.0.47-12.0.1.el6_8
setroubleshoot-plugins-3.0.40-3.1.0.1.el6_8
setroubleshoot-3.0.47-12.0.1.el6_8
setroubleshoot-server-3.0.47-12.0.1.el6_8

178190 - Gentoo Linux GLSA-201606-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-3587, CVE-2016-0742, CVE-2016-0746, CVE-2016-0747, CVE-2016-4450

Description

The scan detected that the host is missing the following update:
GLSA-201606-06

Observation

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

https://security.gentoo.org/glsa/201606-06

Affected packages:
www-servers/nginx < 1.10.1

185324 - Ubuntu Linux 12.04 USN-3013-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6702, CVE-2015-1283, CVE-2016-0718, CVE-2016-4472, CVE-2016-5300

Description

The scan detected that the host is missing the following update:
USN-3013-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-June/003470.html

Ubuntu 12.04

libxmlrpc-core-c3_1.16.33-3.1ubuntu5.2

185325 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-3010-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
USN-3010-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-June/003466.html

Ubuntu 12.04

libexpat1_2.0.1-7.2ubuntu1.4
lib64expat1_2.0.1-7.2ubuntu1.4

Ubuntu 16.04

libexpat1_2.1.0-7ubuntu0.16.04.2
lib64expat1_2.1.0-7ubuntu0.16.04.2

Ubuntu 15.10

lib64expat1_2.1.0-7ubuntu0.15.10.2
libexpat1_2.1.0-7ubuntu0.15.10.2

Ubuntu 14.04

libexpat1_2.1.0-4ubuntu1.3
lib64expat1_2.1.0-4ubuntu1.3

20197 - Splunk Enterprise Multiple Vulnerabilities (SP-CAAAPN9)

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Splunk Enterprise.

Observation

Splunk Enterprise is a platform for the real-time operational intelligence.

Multiple vulnerabilities are present in some versions of Splunk Enterprise. The flaws lie in Splunk Web. Successful exploitation could allow an attacker to execute arbitrary script code.

20205 - Trihedral VTScada Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-4510, CVE-2016-4523, CVE-2016-4532

Description

Multiple vulnerabilities are present in some versions of Trihedral VTScada.

Observation

Trihedral VTScada is an industrial control and monitoring software.

Multiple vulnerabilities are present in some versions of Trihedral VTScada. The flaws lie in WAP interface and they are related with out-of-bounds read, directory traversal and authentication bypass. Successful exploitation could allow a remote attacker to download or view arbitrary files, or to cause the server to crash.

20215 - (APSB16-22) Vulnerability In Adobe ColdFusion

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

Risk Level: Medium

CVE: CVE-2016-4159

Description

A vulnerability is present in some versions of Adobe ColdFusion.

Observation

Adobe ColdFusion is a web application development platform.

A vulnerability is present in some versions of Adobe ColdFusion. The flaw is due to improper validation of input data. Successful exploitation could allow an attacker to conduct cross-site scripting attacks.

The update provided by Adobe bulletin APSB16-22 resolves these issues. The target system appears to be missing this update.

130521 - Debian Linux 8.0 DSA-3603-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3062

Description

The scan detected that the host is missing the following update:
DSA-3603-1

Observation

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

http://www.debian.org/security/2016/dsa-3603

Debian 8.0
all
libavfilter5_6:11.7-1~deb8u1
libavdevice55_6:11.7-1~deb8u1
libswscale-dev_6:11.7-1~deb8u1
libavcodec-dev_6:11.7-1~deb8u1
libavformat56_6:11.7-1~deb8u1
libavformat-dev_6:11.7-1~deb8u1
libav-doc_6:11.7-1~deb8u1
libavdevice-dev_6:11.7-1~deb8u1
libavutil-dev_6:11.7-1~deb8u1
libavresample-dev_6:11.7-1~deb8u1
libavutil54_6:11.7-1~deb8u1
libavfilter-dev_6:11.7-1~deb8u1
libavcodec56_6:11.7-1~deb8u1
libswscale3_6:11.7-1~deb8u1
libav-dbg_6:11.7-1~deb8u1
libav-tools_6:11.7-1~deb8u1
libavcodec-extra_6:11.7-1~deb8u1
libavresample2_6:11.7-1~deb8u1
libavcodec-extra-56_6:11.7-1~deb8u1

132252 - Oracle VM OVMSA-2016-0079 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1775, CVE-2013-1776, CVE-2013-2776, CVE-2013-2777, CVE-2014-0106

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0079

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000493.html

OVM3.2
x86_64
sudo-1.7.2p1-29.el5_10

132255 - Oracle VM OVMSA-2016-0056 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2011-2192, CVE-2013-1944, CVE-2013-2174

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0056

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000478.html

OVM3.2
x86_64
curl-7.15.5-17.el5_9

144692 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1593-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2335

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1593-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002118.html

SuSE SLED 12 SP1
x86_64
p7zip-debuginfo-9.20.1-6.1
p7zip-debugsource-9.20.1-6.1
p7zip-9.20.1-6.1

SuSE SLED 12
x86_64
p7zip-debuginfo-9.20.1-6.1
p7zip-debugsource-9.20.1-6.1
p7zip-9.20.1-6.1

SuSE SLES 12 SP1
x86_64
p7zip-debuginfo-9.20.1-6.1
p7zip-debugsource-9.20.1-6.1
p7zip-9.20.1-6.1

SuSE SLES 12
x86_64
p7zip-debuginfo-9.20.1-6.1
p7zip-debugsource-9.20.1-6.1
p7zip-9.20.1-6.1

144702 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1588-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1541

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1588-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002117.html

SuSE SLED 12 SP1
x86_64
libarchive-debugsource-3.1.2-12.1
libarchive13-debuginfo-3.1.2-12.1
libarchive13-3.1.2-12.1

SuSE SLED 12
x86_64
libarchive-debugsource-3.1.2-12.1
libarchive13-debuginfo-3.1.2-12.1
libarchive13-3.1.2-12.1

SuSE SLES 12 SP1
x86_64
libarchive-debugsource-3.1.2-12.1
libarchive13-debuginfo-3.1.2-12.1
libarchive13-3.1.2-12.1

SuSE SLES 12
x86_64
libarchive-debugsource-3.1.2-12.1
libarchive13-debuginfo-3.1.2-12.1
libarchive13-3.1.2-12.1

160113 - CentOS 5, 6, 7 CESA-2016-1217 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-June/021906.html
http://lists.centos.org/pipermail/centos-announce/2016-June/021908.html

http://lists.centos.org/pipermail/centos-announce/2016-June/021907.html

CentOS 6
x86_64
firefox-45.2.0-1.el6.centos

i686
firefox-45.2.0-1.el6.centos

CentOS 7
x86_64
firefox-45.2.0-1.el7.centos

i686
firefox-45.2.0-1.el7.centos

CentOS 5
x86_64
firefox-45.2.0-1.el5.centos

i386
firefox-45.2.0-1.el5.centos

170692 - Amazon Linux AMI ALAS-2016-713 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4554, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
ALAS-2016-713

Observation

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

https://alas.aws.amazon.com/ALAS-2016-713.html

Amazon Linux AMI
x86_64
squid-debuginfo-3.1.23-16.21.amzn1
squid-3.1.23-16.21.amzn1

i686
squid-debuginfo-3.1.23-16.21.amzn1
squid-3.1.23-16.21.amzn1

174971 - Scientific Linux Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1606-3658)

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

Risk Level: Medium

CVE: CVE-2010-5313, CVE-2013-4312, CVE-2014-7842, CVE-2014-8134, CVE-2015-5156, CVE-2015-7509, CVE-2015-8215, CVE-2015-8324, CVE-2015-8543

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1606-3658)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=3658

SL6
i386
kernel-devel-2.6.32-642.el6
python-perf-2.6.32-642.el6
perf-2.6.32-642.el6
kernel-debuginfo-2.6.32-642.el6
kernel-debuginfo-common-i686-2.6.32-642.el6
kernel-headers-2.6.32-642.el6
kernel-debug-devel-2.6.32-642.el6
perf-debuginfo-2.6.32-642.el6
kernel-debug-2.6.32-642.el6
kernel-2.6.32-642.el6
python-perf-debuginfo-2.6.32-642.el6
kernel-debug-debuginfo-2.6.32-642.el6

noarch
kernel-abi-whitelists-2.6.32-642.el6
kernel-firmware-2.6.32-642.el6
kernel-doc-2.6.32-642.el6

x86_64
perf-debuginfo-2.6.32-642.el6
python-perf-2.6.32-642.el6
kernel-debug-2.6.32-642.el6
kernel-2.6.32-642.el6
kernel-debuginfo-common-x86_64-2.6.32-642.el6
python-perf-debuginfo-2.6.32-642.el6
perf-2.6.32-642.el6
kernel-debug-devel-2.6.32-642.el6
kernel-debuginfo-common-i686-2.6.32-642.el6
kernel-headers-2.6.32-642.el6
kernel-debug-debuginfo-2.6.32-642.el6
kernel-devel-2.6.32-642.el6
kernel-debuginfo-2.6.32-642.el6

174972 - Scientific Linux Security ERRATA Moderate: squid on SL6.x i386/x86_64 (1606-4582)

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4554, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: squid on SL6.x i386/x86_64 (1606-4582)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=4582

SL6
x86_64
squid-3.1.23-16.el6_8.4
squid-debuginfo-3.1.23-16.el6_8.4

i386
squid-3.1.23-16.el6_8.4
squid-debuginfo-3.1.23-16.el6_8.4

174975 - Scientific Linux Security ERRATA Moderate: squid34 on SL6.x i386/x86_64 (1606-4138)

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

Risk Level: Medium

CVE: CVE-2009-0801, CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: squid34 on SL6.x i386/x86_64 (1606-4138)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=4138

SL6
x86_64
squid34-debuginfo-3.4.14-9.el6_8.3
squid34-3.4.14-9.el6_8.3

i386
squid34-debuginfo-3.4.14-9.el6_8.3
squid34-3.4.14-9.el6_8.3

174977 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1606-5730)

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1606-5730)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=5730

SL5
x86_64
firefox-debuginfo-45.2.0-1.el5_11

firefox-45.2.0-1.el5_11

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

SL7
x86_64
firefox-debuginfo-45.2.0-1.el7_2
firefox-45.2.0-1.el7_2

SL6
x86_64
firefox-45.2.0-1.el6_8
firefox-debuginfo-45.2.0-1.el6_8

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

178186 - Gentoo Linux GLSA-201606-09 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9676, CVE-2016-1897, CVE-2016-1898, CVE-2016-2213, CVE-2016-2326, CVE-2016-2327, CVE-2016-2328, CVE-2016-2329, CVE-2016-2330

Description

The scan detected that the host is missing the following update:
GLSA-201606-09

Observation

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

https://security.gentoo.org/glsa/201606-09

Affected packages:
media-video/ffmpeg < 2.8.6

20214 - IBM WebSphere MQ GSKit Information Disclosure Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2015-7420, CVE-2015-7421

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a messaging middleware.

Multiple vulnerabilities are present in some versions of IBM WebSphere MQ. The flaws lie in GSKit. Successful exploitation could allow an attacker to obtain sensitive information.

20221 - (HPSBGN03623) HPE Universal CMDB Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-4367

Description

A vulnerability is present in some versions of HP UCMDB.

Observation

HP UCMDB is a product for enterprise system general management.

A vulnerability is present in some versions of HP UCMDB. The flaw lies in the Universal Discovery component. Successful exploitation could allow an attacker to retrieve sensitive data.

20222 - (HPSBGN03623) HPE Universal CMDB Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-4367

Description

A vulnerability is present in some versions of HP UCMDB.

Observation

HP UCMDB is a product for enterprise system general management.

A vulnerability is present in some versions of HP UCMDB. The flaw lies in the Universal Discovery component. Successful exploitation could allow an attacker to retrieve sensitive data.

37532 - IBM AIX IV85298 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

Description

The scan detected that the host is missing the following update:
IV85298

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV85298

5300-12
bos.net.tcp.server < 5.3.12.7

37533 - IBM AIX IV84984 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

Description

The scan detected that the host is missing the following update:
IV84984

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV84984

6100-09
bos.net.tcp.server < 6.1.9.102

37534 - IBM AIX IV85296 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

Description

The scan detected that the host is missing the following update:
IV85296

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV85296

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

37535 - IBM AIX IV84947 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

Description

The scan detected that the host is missing the following update:
IV84947

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV84947

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

37536 - IBM AIX IV85297 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

Description

The scan detected that the host is missing the following update:
IV85297

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV85297

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

130522 - Debian Linux 8.0 DSA-3605-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7995, CVE-2016-1683, CVE-2016-1684

Description

The scan detected that the host is missing the following update:
DSA-3605-1

Observation

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

http://www.debian.org/security/2016/dsa-3605

Debian 8.0
all
libxslt1-dbg_1.1.28-2+deb8u1
python-libxslt1_1.1.28-2+deb8u1
xsltproc_1.1.28-2+deb8u1
libxslt1.1_1.1.28-2+deb8u1
python-libxslt1-dbg_1.1.28-2+deb8u1
libxslt1-dev_1.1.28-2+deb8u1

132245 - Oracle VM OVMSA-2016-0063 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0063

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000484.html

OVM3.2
x86_64
libxml2-2.6.26-2.1.25.0.1.el5_11
libxml2-python-2.6.26-2.1.25.0.1.el5_11

132248 - Oracle VM OVMSA-2016-0071 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2015-3195, CVE-2015-3197, CVE-2016-0797

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0071

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000490.html

OVM3.2
x86_64
openssl-0.9.8e-39.0.1.el5_11

132250 - Oracle VM OVMSA-2016-0069 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2011-1024, CVE-2013-4449, CVE-2015-6908

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0069

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000489.html

OVM3.2
x86_64
openldap-clients-2.3.43-29.el5_11
openldap-2.3.43-29.el5_11

144684 - SuSE SLES 11 SP4 SUSE-SU-2016:1645-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7041, CVE-2015-3238

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1645-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002134.html

SuSE SLES 11 SP4
i586
pam-doc-1.1.5-0.17.2
pam-1.1.5-0.17.2

x86_64
pam-32bit-1.1.5-0.17.2
pam-1.1.5-0.17.2
pam-doc-1.1.5-0.17.2

144699 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1639-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5104

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1639-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002132.html

SuSE SLES 12
x86_64
usbmuxd-debugsource-1.0.8-12.1
usbmuxd-1.0.8-12.1
usbmuxd-debuginfo-1.0.8-12.1
libimobiledevice4-1.1.5-6.1
libimobiledevice4-debuginfo-1.1.5-6.1
libusbmuxd2-debuginfo-1.0.8-12.1
libimobiledevice-debugsource-1.1.5-6.1
libusbmuxd2-1.0.8-12.1

SuSE SLES 12 SP1
x86_64
usbmuxd-debugsource-1.0.8-12.1
usbmuxd-1.0.8-12.1
usbmuxd-debuginfo-1.0.8-12.1
libimobiledevice4-1.1.5-6.1
libimobiledevice4-debuginfo-1.1.5-6.1

libusbmuxd2-debuginfo-1.0.8-12.1
libimobiledevice-debugsource-1.1.5-6.1
libusbmuxd2-1.0.8-12.1

SuSE SLED 12
x86_64
libimobiledevice-tools-1.1.5-6.1
libimobiledevice-tools-debuginfo-1.1.5-6.1
usbmuxd-debugsource-1.0.8-12.1
usbmuxd-1.0.8-12.1
usbmuxd-debuginfo-1.0.8-12.1
libimobiledevice4-1.1.5-6.1
libimobiledevice4-debuginfo-1.1.5-6.1
libusbmuxd2-debuginfo-1.0.8-12.1
libimobiledevice-debugsource-1.1.5-6.1
libusbmuxd2-1.0.8-12.1

SuSE SLED 12 SP1
x86_64
libimobiledevice-tools-1.1.5-6.1
libimobiledevice-tools-debuginfo-1.1.5-6.1
usbmuxd-debugsource-1.0.8-12.1
usbmuxd-1.0.8-12.1
usbmuxd-debuginfo-1.0.8-12.1
libimobiledevice4-1.1.5-6.1
libimobiledevice4-debuginfo-1.1.5-6.1
libusbmuxd2-debuginfo-1.0.8-12.1
libimobiledevice-debugsource-1.1.5-6.1
libusbmuxd2-1.0.8-12.1

170691 - Amazon Linux AMI ALAS-2016-715 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4450

Description

The scan detected that the host is missing the following update:
ALAS-2016-715

Observation

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

https://alas.aws.amazon.com/ALAS-2016-715.html

Amazon Linux AMI
x86_64
nginx-debuginfo-1.8.1-3.27.amzn1
nginx-1.8.1-3.27.amzn1

i686
nginx-debuginfo-1.8.1-3.27.amzn1
nginx-1.8.1-3.27.amzn1

174974 - Scientific Linux Security ERRATA Moderate: ntp on SL6.x, SL7.x i386/x86_64 (1606-5337)

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

Risk Level: Medium

CVE: CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ntp on SL6.x, SL7.x i386/x86_64 (1606-5337)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=5337

SL7
x86_64
ntpdate-4.2.6p5-22.el7_2.2
ntp-4.2.6p5-22.el7_2.2
ntp-debuginfo-4.2.6p5-22.el7_2.2
sntp-4.2.6p5-22.el7_2.2

noarch
ntp-doc-4.2.6p5-22.el7_2.2
ntp-perl-4.2.6p5-22.el7_2.2

SL6
i386
ntpdate-4.2.6p5-10.el6.1
ntp-perl-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1
ntp-debuginfo-4.2.6p5-10.el6.1

noarch
ntp-doc-4.2.6p5-10.el6.1

x86_64
ntpdate-4.2.6p5-10.el6.1
ntp-perl-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1
ntp-debuginfo-4.2.6p5-10.el6.1

181980 - FreeBSD libxslt Denial Of Service (1a2aa04f-3718-11e6-b3c8-14dae9d210b8)

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

Risk Level: Medium

CVE: CVE-2016-1683, CVE-2016-1684

Description

The scan detected that the host is missing the following update:
libxslt -- Denial of Service (1a2aa04f-3718-11e6-b3c8-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/1a2aa04f-3718-11e6-b3c8-14dae9d210b8.html

Affected packages:
libxslt < 1.1.29

144691 - SuSE SLES 11 SP4 SUSE-SU-2016:1600-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1600-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002120.html

SuSE SLES 11 SP4
i586
libtasn1-1.5-1.34.1
libtasn1-3-1.5-1.34.1

x86_64
libtasn1-3-1.5-1.34.1
libtasn1-1.5-1.34.1
libtasn1-3-32bit-1.5-1.34.1

144694 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1601-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1601-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002121.html

SuSE SLED 12 SP1
x86_64
libtasn1-6-3.7-11.1
libtasn1-debuginfo-3.7-11.1
libtasn1-6-32bit-3.7-11.1
libtasn1-debugsource-3.7-11.1
libtasn1-6-debuginfo-32bit-3.7-11.1
libtasn1-6-debuginfo-3.7-11.1
libtasn1-3.7-11.1

SuSE SLED 12

x86_64
libtasn1-6-3.7-11.1
libtasn1-debuginfo-3.7-11.1
libtasn1-6-32bit-3.7-11.1
libtasn1-debugsource-3.7-11.1
libtasn1-6-debuginfo-32bit-3.7-11.1
libtasn1-6-debuginfo-3.7-11.1
libtasn1-3.7-11.1

SuSE SLES 12 SP1
x86_64
libtasn1-6-3.7-11.1
libtasn1-debuginfo-3.7-11.1
libtasn1-6-32bit-3.7-11.1
libtasn1-debugsource-3.7-11.1
libtasn1-6-debuginfo-32bit-3.7-11.1
libtasn1-6-debuginfo-3.7-11.1
libtasn1-3.7-11.1

SuSE SLES 12
x86_64
libtasn1-6-3.7-11.1
libtasn1-debuginfo-3.7-11.1
libtasn1-6-32bit-3.7-11.1
libtasn1-debugsource-3.7-11.1
libtasn1-6-debuginfo-32bit-3.7-11.1
libtasn1-6-debuginfo-3.7-11.1
libtasn1-3.7-11.1

144696 - SuSE SLES 11 SP4 SUSE-SU-2016:1618-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4000

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1618-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002127.html

SuSE SLES 11 SP4
i586
libmysqlclient15-5.0.96-0.8.10.3
libmysqlclient_r15-5.0.96-0.8.10.3

x86_64
libmysqlclient_r15-5.0.96-0.8.10.3
libmysqlclient15-5.0.96-0.8.10.3
libmysqlclient15-32bit-5.0.96-0.8.10.3

20200 - IBM WebSphere MQ Local runmqsc Display Commands Information Disclosure Vulnerability

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0259

Description

An information disclosure vulnerability is present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a messaging solution.

An information disclosure vulnerability is present in some versions of IBM WebSphere MQ. The flaw occurs within local runmqsc process. Successful exploitation could allow an attacker to obtain sensitive data.

20218 - IBM WebSphere MQ Local runmqsc Improper Access Control Vulnerability

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

Risk Level: Low

CVE: CVE-2015-7473

Description

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

Observation

IBM WebSphere MQ is a messaging solution.

A security bypass vulnerability is present in some versions of IBM WebSphere MQ. The flaw is due to how runmqsc controls the access to certain commands. Successful exploitation could allow an attacker to bypass security restrictions.

88785 - Slackware Linux 14.1 SSA:2016-172-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2016-172-01

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.339629

Slackware 14.1
x86_64
libarchive-3.1.2-x86_64-2

130520 - Debian Linux 8.0 DSA-3604-1 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-3604-1

Observation

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

http://www.debian.org/security/2016/dsa-3604

Debian 8.0
all
drupal7_7.32-1+deb8u7

170690 - Amazon Linux AMI ALAS-2016-714 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3099

Description

The scan detected that the host is missing the following update:
ALAS-2016-714

Observation

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

https://alas.aws.amazon.com/ALAS-2016-714.html

Amazon Linux AMI
x86_64
mod24_nss-debuginfo-1.0.12-4.22.amzn1
mod24_nss-1.0.12-4.22.amzn1

i686
mod24_nss-debuginfo-1.0.12-4.22.amzn1
mod24_nss-1.0.12-4.22.amzn1

181976 - FreeBSD Python Integer Overflow In Zipimport Module (1d0f6852-33d8-11e6-a671-60a44ce6887b)

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

Risk Level: Low

CVE: CVE-2016-5636

Description

The scan detected that the host is missing the following update:
Python -- Integer overflow in zipimport module (1d0f6852-33d8-11e6-a671-60a44ce6887b)

Observation

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

http://www.vuxml.org/freebsd/1d0f6852-33d8-11e6-a671-60a44ce6887b.html

Affected packages:
python35 < 3.5.1_3
python34 < 3.4.4_3
python33 < 3.3.6_5
python27 < 2.7.11_3

181977 - FreeBSD wget HTTP To FTP Redirection File Name Confusion Vulnerability (6df56c60-3738-11e6-a671-60a44ce6887b)

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

Risk Level: Low

CVE: CVE-2016-4971

Description

The scan detected that the host is missing the following update:
wget -- HTTP to FTP redirection file name confusion vulnerability (6df56c60-3738-11e6-a671-60a44ce6887b)

Observation

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

http://www.vuxml.org/freebsd/6df56c60-3738-11e6-a671-60a44ce6887b.html

Affected packages:
wget < 1.18

181981 - FreeBSD chromium Multiple Vulnerabilities (d59ebed4-34be-11e6-be25-3065ec8fd3ec)

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

Risk Level: Low

CVE: CVE-2016-1704

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (d59ebed4-34be-11e6-be25-3065ec8fd3ec)

Observation

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

http://www.vuxml.org/freebsd/d59ebed4-34be-11e6-be25-3065ec8fd3ec.html

Affected packages:
chromium < 51.0.2704.103
chromium-npapi < 51.0.2704.103
chromium-pulse < 51.0.2704.103

181983 - FreeBSD drupal Multiple Vulnerabilities (7932548e-3427-11e6-8e82-002590263bf5)

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:
drupal -- multiple vulnerabilities (7932548e-3427-11e6-8e82-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/7932548e-3427-11e6-8e82-002590263bf5.html

Affected packages:
drupal7 < 7.44
drupal8 < 8.1.3

185326 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-3012-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4971

Description

The scan detected that the host is missing the following update:
USN-3012-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-June/003469.html

Ubuntu 12.04

wget_1.13.4-2ubuntu1.4

Ubuntu 16.04

wget_1.17.1-1ubuntu1.1

Ubuntu 15.10

wget_1.16.1-1ubuntu1.1

Ubuntu 14.04

wget_1.15-1ubuntu1.14.04.2

185327 - Ubuntu Linux 16.04 USN-3011-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5360

Description

The scan detected that the host is missing the following update:
USN-3011-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-June/003468.html

Ubuntu 16.04

haproxy_1.6.3-1ubuntu0.1

185328 - Ubuntu Linux 15.10, 16.04 USN-3009-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8899

Description

The scan detected that the host is missing the following update:
USN-3009-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-June/003467.html

Ubuntu 15.10

dnsmasq_2.75-1ubuntu0.15.10.1
dnsmasq-base_2.75-1ubuntu0.15.10.1
dnsmasq-utils_2.75-1ubuntu0.15.10.1

Ubuntu 16.04

dnsmasq-utils_2.75-1ubuntu0.16.04.1
dnsmasq_2.75-1ubuntu0.16.04.1
dnsmasq-base_2.75-1ubuntu0.16.04.1

132246 - Oracle VM OVMSA-2016-0062 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4242

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0062

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000483.html

OVM3.2

x86_64
libgcrypt-1.4.4-7.el5_10

132251 - Oracle VM OVMSA-2016-0068 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0068

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000487.html

OVM3.2
x86_64
OpenIPMI-tools-2.0.16-16.el5

132253 - Oracle VM OVMSA-2016-0078 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0078

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-June/000494.html

OVM3.2
x86_64
sos-1.7-9.73.0.1.el5

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.

9835 - ProSysInfo TFTP Server TFTPDWIN Long File Name Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> Instrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2006-4948

Update Details

Recommendation is updated

14181 - Oracle Business Transaction Management SOAP Web Service Directory Traversal Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14250 - QNX FTPD Denial of Service

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14324 - RealNetworks RealPlayer 3GP File Handling Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

18873 - (SOL17079) F5 BIG-IP Java SE Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-2590, CVE-2015-4732

Update Details

Recommendation is updated

645 - Netscape Enterprise Server 3.6 SP2 Authentication Overflow

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

Risk Level: High

CVE: CVE-1999-0853

Update Details

Recommendation is updated

772 - Netscape FastTrack Authentication Buffer Overflow

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

Risk Level: High

CVE: CVE-1999-0853

Update Details

Recommendation is updated

18079 - Cisco AnyConnect Secure Mobility Client Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-0662, CVE-2015-0663, CVE-2015-0664, CVE-2015-0665

Update Details

Recommendation is updated Documentation is updated FASLScript is updated

18080 - Cisco AnyConnect Secure Mobility Client Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-0662, CVE-2015-0663, CVE-2015-0664, CVE-2015-0665

Update Details

Recommendation is updated Documentation is updated FASLScript is updated

18874 - (SOL17113) F5 BIG-IP OpenSSH Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-5600

Update Details

FASLScript is updated

4270 - Network Tools for PHP-Nuke hostinput Vulnerability

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

Risk Level: High

CVE: CVE-2001-0899

Update Details

Recommendation is updated

4835 - Oracle Portal HTTP Response Splitting

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

Risk Level: High

CVE: CVE-2006-6697, CVE-2006-6699, CVE-2006-6703

Update Details

Recommendation is updated

9865 - Network Associates WebShield SMTP Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> Instrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2000-0447

Update Details

Recommendation is updated

19708 - Netgear Management System NMS300 Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-1524, CVE-2016-1525

Update Details

Documentation is updated

11538 - Novell Netware SSH Remote Buffer Overflow

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12359 - Oracle Java Runtime Environment Insecure File Loading

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12904 - NexusPHP thanks php SQL Injection Denial Of Service

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

Risk Level: Medium

CVE: CVE-2011-4026

Update Details

Recommendation is updated

170685 - Amazon Linux AMI ALAS-2016-707 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7456, CVE-2016-4343, CVE-2016-5093, CVE-2016-5094, CVE-2016-5095, CVE-2016-5096

Update Details

CVE is updated

643 - Netscape Enterprise Server 3.6 SP2 Accept Buffer Overflow

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

Risk Level: Medium

CVE: CVE-1999-0751

Update Details

Recommendation is updated

12163 - Quest NetVault SmartDisk libnvbasics.dll Integer Overflow Denial Of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12172 - Quest NetVault SmartDisk libnvbasics.dll Denial Of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12896 - Oracle Hyperion Financial Management TList6 ActiveX Control Remote Code Execution

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12935 - Oracle Hyperion Strategic Finance Client TTF16 ActiveX SetDevNames Remote Code Execution

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14464 - Oracle Java SE OpenJDK Hash Table Denial of Service II

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

Risk Level: Medium

CVE: CVE-2012-5373

Update Details

Recommendation is updated

17565 - Symantec Web Gateway Command Injection Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2014-7285

Update Details

FASLScript is updated

18107 - Panasonic Configurator DL Remote Denial of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

18510 - Novell ZENworks Mobile Management Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

19559 - (SOL12824341) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-3195

Update Details

Documentation is updated FASLScript is updated

20180 - (MS16-074) Microsoft Windows ATMFD.DLL Privilege Escalation (3164036)

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

Risk Level: Medium

CVE: CVE-2016-3220

Update Details

CVE is updated

170684 - Amazon Linux AMI ALAS-2016-706 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7456, CVE-2016-5093, CVE-2016-5094, CVE-2016-5095, CVE-2016-5096

Update Details

CVE is updated

19453 - (SOL17516) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7852

Update Details

Documentation is updated FASLScript is updated

895 - PHP info.php Information Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

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

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

Risk Level: Low

CVE: CVE-2016-2178

Update Details

FASLScript 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

51003 - Oracle Solaris Account Not Disabled

Category: SSH Module -> NonIntrusive -> Solaris Security Policy/Options

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70046 - macosx.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70048 - adobe.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70050 - vmware.fasl3.inc

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

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.