2016-JUN-09
FSL version 7.5.826

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

130508 - Debian Linux 8.0 DSA-3593-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8806, 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-2016-2073, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4449, CVE-2016-4483

Description

The scan detected that the host is missing the following update:
DSA-3593-1

Observation

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

http://www.debian.org/security/2016/dsa-3593

Debian 8.0
all
libxml2_2.9.1+dfsg1-5+deb8u2

144659 - SuSE SLES 12 SP1 SUSE-SU-2016:1475-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1475-1

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/002090.html

SuSE SLES 12 SP1
x86_64
java-1_8_0-ibm-plugin-1.8.0_sr3.0-10.1
java-1_8_0-ibm-1.8.0_sr3.0-10.1
java-1_8_0-ibm-alsa-1.8.0_sr3.0-10.1

170687 - Amazon Linux AMI ALAS-2016-705 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8863

Description

The scan detected that the host is missing the following update:
ALAS-2016-705

Observation

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

https://alas.aws.amazon.com/ALAS-2016-705.html

Amazon Linux AMI
x86_64
jq-devel-1.5-1.2.amzn1
jq-1.5-1.2.amzn1
jq-debuginfo-1.5-1.2.amzn1
jq-libs-1.5-1.2.amzn1

i686
jq-libs-1.5-1.2.amzn1
jq-1.5-1.2.amzn1
jq-devel-1.5-1.2.amzn1
jq-debuginfo-1.5-1.2.amzn1

185303 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2990-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718, CVE-2016-5118

Description

The scan detected that the host is missing the following update:
USN-2990-1

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/003447.html

Ubuntu 12.04

imagemagick-common_6.6.9.7-5ubuntu3.4
libmagickcore4_6.6.9.7-5ubuntu3.4
imagemagick_6.6.9.7-5ubuntu3.4

Ubuntu 16.04

imagemagick-common_6.8.9.9-7ubuntu5.1
libmagickcore-6.q16-2_6.8.9.9-7ubuntu5.1

imagemagick-6.q16_6.8.9.9-7ubuntu5.1
imagemagick_6.8.9.9-7ubuntu5.1

Ubuntu 15.10

libmagickcore-6.q16-2_6.8.9.9-5ubuntu2.1
imagemagick-6.q16_6.8.9.9-5ubuntu2.1
imagemagick-common_6.8.9.9-5ubuntu2.1
imagemagick_6.8.9.9-5ubuntu2.1

Ubuntu 14.04

libmagickcore5_6.7.7.10-6ubuntu3.1
imagemagick-common_6.7.7.10-6ubuntu3.1
imagemagick_6.7.7.10-6ubuntu3.1

185305 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2994-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8806, 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-2016-2073, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4449, CVE-2016-4483

Description

The scan detected that the host is missing the following update:
USN-2994-1

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/003450.html

Ubuntu 12.04

libxml2_2.7.8.dfsg-5.1ubuntu4.15

Ubuntu 16.04

libxml2_2.9.3+dfsg1-1ubuntu0.1

Ubuntu 15.10

libxml2_2.9.2+zdfsg1-4ubuntu0.4

Ubuntu 14.04

libxml2_2.9.1+dfsg1-3ubuntu4.8

130511 - Debian Linux 8.0 DSA-3590-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1667, CVE-2016-1668, CVE-2016-1669, CVE-2016-1670, CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1676, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-

1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695

Description

The scan detected that the host is missing the following update:
DSA-3590-1

Observation

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

http://www.debian.org/security/2016/dsa-3590

Debian 8.0
all
chromedriver_51.0.2704.63-1~deb8u1
chromium-l10n_51.0.2704.63-1~deb8u1
chromium_51.0.2704.63-1~deb8u1
chromium-inspector_51.0.2704.63-1~deb8u1
chromium-dbg_51.0.2704.63-1~deb8u1

20121 - (HPSBMU03590) HPE Systems Insight Manager Multiple Vulnerabilities Prior to 7.5.1

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

Risk Level: High

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-6565, CVE-2016-0705, CVE-2016-0799, CVE-2016-2017, CVE-2016-2018, CVE-2016-2019, CVE-2016-2020, CVE-2016-2021, CVE-2016-2022, CVE-2016-2030, CVE-2016-2842, CVE-2016-4366

Description

Multiple vulnerabilities are present in some versions of HP Systems Insight Manager.

Observation

HP Systems Insight Manager is a hardware management solution.

Multiple vulnerabilities are present in some versions of HP Systems Insight Manager. The flaws lie in the OpenSSL component. Successful exploitation could allow a remote attacker to disclose potentially sensitive information, bypass certain security restrictions or cause a denial of service.

20127 - Lenovo Fingerprint Manager and Lenovo Touch Fingerprint Software Privilege Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2016-2393

Description

A vulnerability is present in some versions of Lenovo Fingerprint Manager and Lenovo Touch Fingerprint Software.

Observation

Lenovo Fingerprint Manager and Lenovo Touch Fingerprint Software are drivers that enable the Validity Fingerprint Sensor in supported Lenovo products.

A vulnerability is present in some versions of Lenovo Fingerprint Manager and Lenovo Touch Fingerprint Software. The flaw is due to incorrect access control lists on services and files within the application. Successful exploitation could allow a local attacker to gain escalated privileges.

185306 - Ubuntu Linux 14.04 USN-2989-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
USN-2989-1

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/003446.html

Ubuntu 14.04

linux-image-3.13.0-87-generic_3.13.0-87.133
linux-image-3.13.0-87-generic-lpae_3.13.0-87.133
linux-image-3.13.0-87-powerpc64-smp_3.13.0-87.133
linux-image-3.13.0-87-lowlatency_3.13.0-87.133
linux-image-3.13.0-87-powerpc-smp_3.13.0-87.133
linux-image-3.13.0-87-powerpc64-emb_3.13.0-87.133
linux-image-3.13.0-87-powerpc-e500_3.13.0-87.133
linux-image-3.13.0-87-powerpc-e500mc_3.13.0-87.133

141205 - Red Hat Enterprise Linux RHSA-2016-1205 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise 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:
RHSA-2016-1205

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/msg00003.html

RHEL7D
x86_64
spice-server-0.12.4-15.el7_2.1
spice-server-devel-0.12.4-15.el7_2.1
spice-debuginfo-0.12.4-15.el7_2.1

RHEL7S
x86_64
spice-server-0.12.4-15.el7_2.1
spice-server-devel-0.12.4-15.el7_2.1
spice-debuginfo-0.12.4-15.el7_2.1

RHEL7WS
x86_64
spice-server-0.12.4-15.el7_2.1
spice-server-devel-0.12.4-15.el7_2.1
spice-debuginfo-0.12.4-15.el7_2.1

141208 - Red Hat Enterprise Linux RHSA-2016-1204 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise 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:
RHSA-2016-1204

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/msg00002.html

RHEL6D
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

RHEL6S
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

RHEL6WS
x86_64
spice-server-0.12.4-13.el6.1
spice-server-debuginfo-0.12.4-13.el6.1

144645 - SuSE SLES 11 SP4 SUSE-SU-2016:1509-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4574, CVE-2016-4579

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1509-1

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/002098.html

SuSE SLES 11 SP4
i586
libksba-1.0.4-1.25.1

x86_64
libksba-1.0.4-1.25.1

144646 - SuSE SLES 11 SP4 SUSE-SU-2016:1465-1 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-2016:1465-1

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/002088.html

SuSE SLES 11 SP4
i586
NetworkManager-openvpn-kde4-0.9.svn1043876-1.3.15
NetworkManager-kde4-libs-0.9.svn1043876-1.3.15
NetworkManager-pptp-kde4-0.9.svn1043876-1.3.15
NetworkManager-kde4-lang-0.9.svn1043876-1.3.15
NetworkManager-kde4-0.9.svn1043876-1.3.15
plasmoid-networkmanagement-0.9.svn1043876-1.3.15

x86_64
NetworkManager-openvpn-kde4-0.9.svn1043876-1.3.15
NetworkManager-kde4-libs-0.9.svn1043876-1.3.15
NetworkManager-pptp-kde4-0.9.svn1043876-1.3.15
NetworkManager-kde4-lang-0.9.svn1043876-1.3.15
NetworkManager-kde4-0.9.svn1043876-1.3.15
plasmoid-networkmanagement-0.9.svn1043876-1.3.15

144648 - SuSE Linux 13.2 openSUSE-SU-2016:1516-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5116

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1516-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00019.html

SuSE Linux 13.2
x86_64
libgd3-32bit-2.1.0-7.8.1
libgd3-2.1.0-7.8.1
libgd3-debuginfo-32bit-2.1.0-7.8.1
gd-devel-2.1.0-7.8.1
gd-debuginfo-2.1.0-7.8.1
gd-2.1.0-7.8.1
libgd3-debuginfo-2.1.0-7.8.1
gd-debugsource-2.1.0-7.8.1

i586
libgd3-2.1.0-7.8.1
gd-devel-2.1.0-7.8.1
gd-debuginfo-2.1.0-7.8.1
gd-2.1.0-7.8.1
libgd3-debuginfo-2.1.0-7.8.1
gd-debugsource-2.1.0-7.8.1

144649 - SuSE SLES 11 SP4 SUSE-SU-2016:1514-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1602

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1514-1

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/002102.html

SuSE SLES 11 SP4
noarch
supportutils-1.20-121.1

144651 - SuSE SLES 11 SP4 SUSE-SU-2016:1512-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1283, CVE-2016-0718

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1512-1

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/002101.html

SuSE SLES 11 SP4

i586
expat-2.0.1-88.38.1
libexpat1-2.0.1-88.38.1

x86_64
libexpat1-32bit-2.0.1-88.38.1
expat-2.0.1-88.38.1
libexpat1-2.0.1-88.38.1

144652 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1510-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4574, CVE-2016-4579

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1510-1

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/002099.html

SuSE SLED 12 SP1
x86_64
libksba8-1.3.0-23.1
libksba-debugsource-1.3.0-23.1
libksba8-debuginfo-1.3.0-23.1

SuSE SLED 12
x86_64
libksba8-1.3.0-23.1
libksba-debugsource-1.3.0-23.1
libksba8-debuginfo-1.3.0-23.1

SuSE SLES 12 SP1
x86_64
libksba8-1.3.0-23.1
libksba-debugsource-1.3.0-23.1
libksba8-debuginfo-1.3.0-23.1

SuSE SLES 12
x86_64
libksba8-1.3.0-23.1
libksba-debugsource-1.3.0-23.1
libksba8-debuginfo-1.3.0-23.1

144653 - SuSE SLES 11 SP4 SUSE-SU-2016:1459-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3566, CVE-2015-8076, CVE-2015-8077, CVE-2015-8078

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1459-1

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/002087.html

SuSE SLES 11 SP4
i586
perl-Cyrus-SIEVE-managesieve-2.3.11-60.65.67.1
perl-Cyrus-IMAP-2.3.11-60.65.67.1
cyrus-imapd-2.3.11-60.65.67.1

x86_64
perl-Cyrus-SIEVE-managesieve-2.3.11-60.65.67.1
perl-Cyrus-IMAP-2.3.11-60.65.67.1
cyrus-imapd-2.3.11-60.65.67.1

144654 - SuSE Linux 13.2 openSUSE-SU-2016:1464-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2335

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1464-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00004.html

SuSE Linux 13.2
x86_64
p7zip-9.20.1-12.6.1
p7zip-debuginfo-9.20.1-12.6.1
p7zip-debugsource-9.20.1-12.6.1

i586
p7zip-9.20.1-12.6.1
p7zip-debuginfo-9.20.1-12.6.1
p7zip-debugsource-9.20.1-12.6.1

144658 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1507-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1602

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1507-1

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/002096.html

SuSE SLED 12 SP1
noarch
supportutils-3.0-82.1

SuSE SLED 12
noarch
supportutils-3.0-82.1

SuSE SLES 12 SP1
noarch
supportutils-3.0-82.1

SuSE SLES 12
noarch
supportutils-3.0-82.1

144660 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1508-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1283, CVE-2016-0718

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1508-1

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/002097.html

SuSE SLED 12 SP1
x86_64
expat-debugsource-2.1.0-17.1
libexpat1-32bit-2.1.0-17.1
libexpat1-debuginfo-32bit-2.1.0-17.1
libexpat1-2.1.0-17.1
expat-debuginfo-32bit-2.1.0-17.1
expat-debuginfo-2.1.0-17.1
libexpat1-debuginfo-2.1.0-17.1
expat-2.1.0-17.1

SuSE SLED 12
x86_64
expat-debugsource-2.1.0-17.1
libexpat1-32bit-2.1.0-17.1
libexpat1-debuginfo-32bit-2.1.0-17.1
libexpat1-2.1.0-17.1
expat-debuginfo-32bit-2.1.0-17.1
expat-debuginfo-2.1.0-17.1

libexpat1-debuginfo-2.1.0-17.1
expat-2.1.0-17.1

SuSE SLES 12 SP1
x86_64
expat-debugsource-2.1.0-17.1
libexpat1-32bit-2.1.0-17.1
libexpat1-debuginfo-32bit-2.1.0-17.1
libexpat1-2.1.0-17.1
libexpat1-debuginfo-2.1.0-17.1
expat-debuginfo-2.1.0-17.1
expat-debuginfo-32bit-2.1.0-17.1
expat-2.1.0-17.1

SuSE SLES 12
x86_64
expat-debugsource-2.1.0-17.1
libexpat1-32bit-2.1.0-17.1
libexpat1-debuginfo-32bit-2.1.0-17.1
libexpat1-2.1.0-17.1
libexpat1-debuginfo-2.1.0-17.1
expat-debuginfo-2.1.0-17.1
expat-debuginfo-32bit-2.1.0-17.1
expat-2.1.0-17.1

160109 - CentOS 6 CESA-2016-1204 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS 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:
CESA-2016-1204

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/021903.html

CentOS 6
x86_64
spice-server-devel-0.12.4-13.el6.1
spice-server-0.12.4-13.el6.1

160110 - CentOS 7 CESA-2016-1205 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS 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:
CESA-2016-1205

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/021904.html

CentOS 7
x86_64
spice-server-0.12.4-15.el7_2.1
spice-server-devel-0.12.4-15.el7_2.1

163101 - Oracle Enterprise Linux ELSA-2016-1204 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise 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:
ELSA-2016-1204

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/006104.html

OEL6
x86_64
spice-server-devel-0.12.4-13.el6.1
spice-server-0.12.4-13.el6.1

163102 - Oracle Enterprise Linux ELSA-2016-1205 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise 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:
ELSA-2016-1205

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/006103.html

OEL7
x86_64
spice-server-0.12.4-15.el7_2.1
spice-server-devel-0.12.4-15.el7_2.1

170686 - Amazon Linux AMI ALAS-2016-704 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4913

Description

The scan detected that the host is missing the following update:
ALAS-2016-704

Observation

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

https://alas.aws.amazon.com/ALAS-2016-704.html

Amazon Linux AMI
i686
kernel-devel-4.4.11-23.53.amzn1
kernel-headers-4.4.11-23.53.amzn1
kernel-tools-4.4.11-23.53.amzn1
kernel-4.4.11-23.53.amzn1
kernel-tools-devel-4.4.11-23.53.amzn1
perf-debuginfo-4.4.11-23.53.amzn1
perf-4.4.11-23.53.amzn1
kernel-debuginfo-common-i686-4.4.11-23.53.amzn1
kernel-debuginfo-4.4.11-23.53.amzn1
kernel-tools-debuginfo-4.4.11-23.53.amzn1

noarch
kernel-doc-4.4.11-23.53.amzn1

x86_64
kernel-devel-4.4.11-23.53.amzn1
kernel-headers-4.4.11-23.53.amzn1
kernel-tools-4.4.11-23.53.amzn1
kernel-4.4.11-23.53.amzn1
kernel-debuginfo-common-x86_64-4.4.11-23.53.amzn1
kernel-tools-devel-4.4.11-23.53.amzn1
perf-debuginfo-4.4.11-23.53.amzn1
perf-4.4.11-23.53.amzn1
kernel-debuginfo-4.4.11-23.53.amzn1
kernel-tools-debuginfo-4.4.11-23.53.amzn1

174962 - Scientific Linux Security ERRATA Important: spice on SL7.x x86_64 (1606-75)

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 on SL7.x x86_64 (1606-75)

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=75

SL7
x86_64
spice-server-0.12.4-15.el7_2.1
spice-server-devel-0.12.4-15.el7_2.1
spice-debuginfo-0.12.4-15.el7_2.1

178183 - Gentoo Linux GLSA-201606-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5309, CVE-2016-2563

Description

The scan detected that the host is missing the following update:
GLSA-201606-01

Observation

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

https://security.gentoo.org/glsa/201606-01

Affected packages:
net-misc/putty < 0.67

130509 - Debian Linux 8.0 DSA-3594-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1696, CVE-2016-1697, CVE-2016-1698, CVE-2016-1699, CVE-2016-1700, CVE-2016-1701, CVE-2016-1702, CVE-2016-1703

Description

The scan detected that the host is missing the following update:
DSA-3594-1

Observation

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

http://www.debian.org/security/2016/dsa-3594

Debian 8.0
all
chromium-inspector_51.0.2704.79-1~deb8u1
chromedriver_51.0.2704.79-1~deb8u1
chromium-dbg_51.0.2704.79-1~deb8u1
chromium-l10n_51.0.2704.79-1~deb8u1
chromium_51.0.2704.79-1~deb8u1

141206 - Red Hat Enterprise Linux RHSA-2016-1190 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1676, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695

Description

The scan detected that the host is missing the following update:
RHSA-2016-1190

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/msg00000.html

RHEL6D
x86_64
chromium-browser-51.0.2704.63-1.el6
chromium-browser-debuginfo-51.0.2704.63-1.el6

i386
chromium-browser-51.0.2704.63-1.el6
chromium-browser-debuginfo-51.0.2704.63-1.el6

RHEL6S
x86_64
chromium-browser-51.0.2704.63-1.el6
chromium-browser-debuginfo-51.0.2704.63-1.el6

i386
chromium-browser-51.0.2704.63-1.el6
chromium-browser-debuginfo-51.0.2704.63-1.el6

RHEL6WS
x86_64
chromium-browser-51.0.2704.63-1.el6
chromium-browser-debuginfo-51.0.2704.63-1.el6

i386
chromium-browser-51.0.2704.63-1.el6
chromium-browser-debuginfo-51.0.2704.63-1.el6

141207 - Red Hat Enterprise Linux RHSA-2016-1201 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1696, CVE-2016-1697, CVE-2016-1698, CVE-2016-1699, CVE-2016-1700, CVE-2016-1701, CVE-2016-1702, CVE-2016-1703

Description

The scan detected that the host is missing the following update:
RHSA-2016-1201

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/msg00001.html

RHEL6D
x86_64
chromium-browser-debuginfo-51.0.2704.79-1.el6
chromium-browser-51.0.2704.79-1.el6

i386
chromium-browser-debuginfo-51.0.2704.79-1.el6
chromium-browser-51.0.2704.79-1.el6

RHEL6S
x86_64
chromium-browser-debuginfo-51.0.2704.79-1.el6
chromium-browser-51.0.2704.79-1.el6

i386
chromium-browser-debuginfo-51.0.2704.79-1.el6
chromium-browser-51.0.2704.79-1.el6

RHEL6WS
x86_64
chromium-browser-debuginfo-51.0.2704.79-1.el6
chromium-browser-51.0.2704.79-1.el6

i386
chromium-browser-debuginfo-51.0.2704.79-1.el6
chromium-browser-51.0.2704.79-1.el6

144647 - SuSE Linux 13.2 openSUSE-SU-2016:1496-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1676, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695, CVE-2016-1696, CVE-2016-1697, CVE-2016-1698, CVE-2016-1699, CVE-2016-1700, CVE-2016-1701, CVE-2016-1702, CVE-2016-1703

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1496-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00014.html

SuSE Linux 13.2
x86_64
chromium-ffmpegsumo-debuginfo-51.0.2704.79-105.2
chromium-51.0.2704.79-105.2
chromium-debugsource-51.0.2704.79-105.2
chromedriver-51.0.2704.79-105.2
chromium-desktop-kde-51.0.2704.79-105.2
chromedriver-debuginfo-51.0.2704.79-105.2

chromium-debuginfo-51.0.2704.79-105.2
chromium-ffmpegsumo-51.0.2704.79-105.2
chromium-desktop-gnome-51.0.2704.79-105.2

i586
chromium-ffmpegsumo-debuginfo-51.0.2704.79-105.2
chromium-51.0.2704.79-105.2
chromium-debugsource-51.0.2704.79-105.2
chromedriver-51.0.2704.79-105.2
chromium-desktop-kde-51.0.2704.79-105.2
chromedriver-debuginfo-51.0.2704.79-105.2
chromium-debuginfo-51.0.2704.79-105.2
chromium-ffmpegsumo-51.0.2704.79-105.2
chromium-desktop-gnome-51.0.2704.79-105.2

144657 - SuSE Linux 13.2 openSUSE-SU-2016:1463-1 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:
openSUSE-SU-2016:1463-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00003.html

SuSE Linux 13.2
x86_64
libarchive13-debuginfo-32bit-3.1.2-7.8.1
bsdtar-3.1.2-7.8.1
libarchive-debugsource-3.1.2-7.8.1
libarchive13-debuginfo-3.1.2-7.8.1
libarchive13-3.1.2-7.8.1
libarchive13-32bit-3.1.2-7.8.1
libarchive-devel-3.1.2-7.8.1
bsdtar-debuginfo-3.1.2-7.8.1

i586
bsdtar-3.1.2-7.8.1
libarchive-debugsource-3.1.2-7.8.1
libarchive13-debuginfo-3.1.2-7.8.1
libarchive13-3.1.2-7.8.1
libarchive-devel-3.1.2-7.8.1
bsdtar-debuginfo-3.1.2-7.8.1

170683 - Amazon Linux AMI ALAS-2016-711 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3659

Description

The scan detected that the host is missing the following update:
ALAS-2016-711

Observation

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

https://alas.aws.amazon.com/ALAS-2016-711.html

Amazon Linux AMI
noarch
cacti-0.8.8h-1.13.amzn1

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-2016-5096

Description

The scan detected that the host is missing the following update:
ALAS-2016-707

Observation

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

https://alas.aws.amazon.com/ALAS-2016-707.html

Amazon Linux AMI
x86_64
php55-5.5.36-1.115.amzn1
php55-dba-5.5.36-1.115.amzn1
php55-xmlrpc-5.5.36-1.115.amzn1
php55-intl-5.5.36-1.115.amzn1
php55-tidy-5.5.36-1.115.amzn1
php55-gmp-5.5.36-1.115.amzn1
php55-common-5.5.36-1.115.amzn1
php55-pdo-5.5.36-1.115.amzn1
php55-soap-5.5.36-1.115.amzn1
php55-enchant-5.5.36-1.115.amzn1
php55-xml-5.5.36-1.115.amzn1
php55-ldap-5.5.36-1.115.amzn1
php55-snmp-5.5.36-1.115.amzn1
php55-debuginfo-5.5.36-1.115.amzn1
php55-gd-5.5.36-1.115.amzn1
php55-fpm-5.5.36-1.115.amzn1
php55-mcrypt-5.5.36-1.115.amzn1
php55-mssql-5.5.36-1.115.amzn1
php55-imap-5.5.36-1.115.amzn1
php55-opcache-5.5.36-1.115.amzn1
php55-cli-5.5.36-1.115.amzn1
php55-recode-5.5.36-1.115.amzn1
php55-process-5.5.36-1.115.amzn1
php55-pspell-5.5.36-1.115.amzn1
php55-pgsql-5.5.36-1.115.amzn1
php55-odbc-5.5.36-1.115.amzn1

php55-embedded-5.5.36-1.115.amzn1
php55-bcmath-5.5.36-1.115.amzn1
php55-mbstring-5.5.36-1.115.amzn1
php55-devel-5.5.36-1.115.amzn1
php55-mysqlnd-5.5.36-1.115.amzn1

i686
php55-5.5.36-1.115.amzn1
php55-dba-5.5.36-1.115.amzn1
php55-xmlrpc-5.5.36-1.115.amzn1
php55-intl-5.5.36-1.115.amzn1
php55-tidy-5.5.36-1.115.amzn1
php55-gmp-5.5.36-1.115.amzn1
php55-common-5.5.36-1.115.amzn1
php55-soap-5.5.36-1.115.amzn1
php55-enchant-5.5.36-1.115.amzn1
php55-xml-5.5.36-1.115.amzn1
php55-ldap-5.5.36-1.115.amzn1
php55-snmp-5.5.36-1.115.amzn1
php55-debuginfo-5.5.36-1.115.amzn1
php55-gd-5.5.36-1.115.amzn1
php55-fpm-5.5.36-1.115.amzn1
php55-mcrypt-5.5.36-1.115.amzn1
php55-mssql-5.5.36-1.115.amzn1
php55-recode-5.5.36-1.115.amzn1
php55-imap-5.5.36-1.115.amzn1
php55-opcache-5.5.36-1.115.amzn1
php55-cli-5.5.36-1.115.amzn1
php55-pdo-5.5.36-1.115.amzn1
php55-process-5.5.36-1.115.amzn1
php55-pspell-5.5.36-1.115.amzn1
php55-pgsql-5.5.36-1.115.amzn1
php55-odbc-5.5.36-1.115.amzn1
php55-embedded-5.5.36-1.115.amzn1
php55-bcmath-5.5.36-1.115.amzn1
php55-mbstring-5.5.36-1.115.amzn1
php55-devel-5.5.36-1.115.amzn1
php55-mysqlnd-5.5.36-1.115.amzn1

174963 - Scientific Linux Security ERRATA Moderate: squid on SL7.x x86_64 (1606-412)

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: squid on SL7.x x86_64 (1606-412)

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=412

SL7
x86_64

squid-3.3.8-26.el7_2.3
squid-sysvinit-3.3.8-26.el7_2.3
squid-debuginfo-3.3.8-26.el7_2.3

181962 - FreeBSD chromium Multiple Vulnerabilities (c039a761-2c29-11e6-8912-3065ec8fd3ec)

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

Risk Level: Medium

CVE: CVE-2016-1695, CVE-2016-1696, CVE-2016-1697, CVE-2016-1698, CVE-2016-1699, CVE-2016-1700, CVE-2016-1701, CVE-2016-1702, CVE-2016-1703

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (c039a761-2c29-11e6-8912-3065ec8fd3ec)

Observation

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

http://www.vuxml.org/freebsd/c039a761-2c29-11e6-8912-3065ec8fd3ec.html

Affected packages:
chromium < 51.0.2704.79
chromium-npapi < 51.0.2704.79
chromium-pulse < 51.0.2704.79

185307 - Ubuntu Linux 14.04, 15.10, 16.04 USN-2992-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1673, CVE-2016-1675, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1688, CVE-2016-1689, CVE-2016-1691, CVE-2016-1692, CVE-2016-1695, CVE-2016-1697, CVE-2016-1699, CVE-2016-1702, CVE-2016-1703

Description

The scan detected that the host is missing the following update:
USN-2992-1

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/003449.html

Ubuntu 16.04

liboxideqtcore0_1.15.7-0ubuntu0.16.04.1

Ubuntu 15.10

liboxideqtcore0_1.15.7-0ubuntu0.15.10.1

Ubuntu 14.04

liboxideqtcore0_1.15.7-0ubuntu0.14.04.1

144650 - SuSE SLES 11 SP4 SUSE-SU-2016:1483-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4049

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1483-1

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/002093.html

SuSE SLES 11 SP4
i586
quagga-0.99.15-0.24.2

x86_64
quagga-0.99.15-0.24.2

144655 - SuSE SLES 12, 12 SP1 SUSE-SU-2016:1482-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4049

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1482-1

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/002092.html

SuSE SLES 12 SP1
x86_64
quagga-0.99.22.1-12.1
quagga-debuginfo-0.99.22.1-12.1
quagga-debugsource-0.99.22.1-12.1

SuSE SLES 12
x86_64
quagga-0.99.22.1-12.1
quagga-debuginfo-0.99.22.1-12.1
quagga-debugsource-0.99.22.1-12.1

170681 - Amazon Linux AMI ALAS-2016-712 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4574, CVE-2016-4579

Description

The scan detected that the host is missing the following update:
ALAS-2016-712

Observation

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

https://alas.aws.amazon.com/ALAS-2016-712.html

Amazon Linux AMI
x86_64
libksba-devel-1.3.4-1.8.amzn1
libksba-1.3.4-1.8.amzn1
libksba-debuginfo-1.3.4-1.8.amzn1

i686
libksba-devel-1.3.4-1.8.amzn1
libksba-1.3.4-1.8.amzn1
libksba-debuginfo-1.3.4-1.8.amzn1

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-2016-5096

Description

The scan detected that the host is missing the following update:
ALAS-2016-706

Observation

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

https://alas.aws.amazon.com/ALAS-2016-706.html

Amazon Linux AMI
x86_64
php56-5.6.22-1.125.amzn1
php56-pdo-5.6.22-1.125.amzn1
php56-xml-5.6.22-1.125.amzn1
php56-debuginfo-5.6.22-1.125.amzn1
php56-mysqlnd-5.6.22-1.125.amzn1
php56-pgsql-5.6.22-1.125.amzn1
php56-recode-5.6.22-1.125.amzn1
php56-fpm-5.6.22-1.125.amzn1
php56-intl-5.6.22-1.125.amzn1
php56-imap-5.6.22-1.125.amzn1
php56-xmlrpc-5.6.22-1.125.amzn1
php56-mbstring-5.6.22-1.125.amzn1
php56-snmp-5.6.22-1.125.amzn1
php56-cli-5.6.22-1.125.amzn1
php56-mcrypt-5.6.22-1.125.amzn1
php56-odbc-5.6.22-1.125.amzn1

php56-common-5.6.22-1.125.amzn1
php56-tidy-5.6.22-1.125.amzn1
php56-embedded-5.6.22-1.125.amzn1
php56-bcmath-5.6.22-1.125.amzn1
php56-opcache-5.6.22-1.125.amzn1
php56-dba-5.6.22-1.125.amzn1
php56-enchant-5.6.22-1.125.amzn1
php56-gmp-5.6.22-1.125.amzn1
php56-gd-5.6.22-1.125.amzn1
php56-ldap-5.6.22-1.125.amzn1
php56-soap-5.6.22-1.125.amzn1
php56-dbg-5.6.22-1.125.amzn1
php56-devel-5.6.22-1.125.amzn1
php56-pspell-5.6.22-1.125.amzn1
php56-process-5.6.22-1.125.amzn1
php56-mssql-5.6.22-1.125.amzn1

i686
php56-5.6.22-1.125.amzn1
php56-pdo-5.6.22-1.125.amzn1
php56-xml-5.6.22-1.125.amzn1
php56-embedded-5.6.22-1.125.amzn1
php56-debuginfo-5.6.22-1.125.amzn1
php56-mysqlnd-5.6.22-1.125.amzn1
php56-pgsql-5.6.22-1.125.amzn1
php56-recode-5.6.22-1.125.amzn1
php56-fpm-5.6.22-1.125.amzn1
php56-imap-5.6.22-1.125.amzn1
php56-xmlrpc-5.6.22-1.125.amzn1
php56-intl-5.6.22-1.125.amzn1
php56-snmp-5.6.22-1.125.amzn1
php56-cli-5.6.22-1.125.amzn1
php56-mcrypt-5.6.22-1.125.amzn1
php56-common-5.6.22-1.125.amzn1
php56-tidy-5.6.22-1.125.amzn1
php56-odbc-5.6.22-1.125.amzn1
php56-bcmath-5.6.22-1.125.amzn1
php56-opcache-5.6.22-1.125.amzn1
php56-dba-5.6.22-1.125.amzn1
php56-enchant-5.6.22-1.125.amzn1
php56-gmp-5.6.22-1.125.amzn1
php56-gd-5.6.22-1.125.amzn1
php56-ldap-5.6.22-1.125.amzn1
php56-soap-5.6.22-1.125.amzn1
php56-dbg-5.6.22-1.125.amzn1
php56-mbstring-5.6.22-1.125.amzn1
php56-devel-5.6.22-1.125.amzn1
php56-pspell-5.6.22-1.125.amzn1
php56-process-5.6.22-1.125.amzn1
php56-mssql-5.6.22-1.125.amzn1

170688 - Amazon Linux AMI ALAS-2016-708 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1548, CVE-2016-1550, CVE-2016-2516, CVE-2016-2518

Description

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

ALAS-2016-708

Observation

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

https://alas.aws.amazon.com/ALAS-2016-708.html

Amazon Linux AMI
i686
ntp-4.2.6p5-40.30.amzn1
ntp-debuginfo-4.2.6p5-40.30.amzn1
ntpdate-4.2.6p5-40.30.amzn1

noarch
ntp-perl-4.2.6p5-40.30.amzn1
ntp-doc-4.2.6p5-40.30.amzn1

x86_64
ntp-4.2.6p5-40.30.amzn1
ntp-debuginfo-4.2.6p5-40.30.amzn1
ntpdate-4.2.6p5-40.30.amzn1

178181 - Gentoo Linux GLSA-201606-04 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3591, CVE-2015-0837

Description

The scan detected that the host is missing the following update:
GLSA-201606-04

Observation

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

https://security.gentoo.org/glsa/201606-04

Affected packages:
app-crypt/gnupg < 2.0.26-r3
dev-libs/libgcrypt < 1.6.3-r4

178182 - Gentoo Linux GLSA-201606-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2785, CVE-2016-2786

Description

The scan detected that the host is missing the following update:
GLSA-201606-02

Observation

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

For more information see:

https://security.gentoo.org/glsa/201606-02

Affected packages:
app-admin/puppet-agent < 1.4.2
app-admin/puppetserver < 2.3.2

178184 - Gentoo Linux GLSA-201606-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6629, CVE-2013-6630

Description

The scan detected that the host is missing the following update:
GLSA-201606-03

Observation

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

https://security.gentoo.org/glsa/201606-03

Affected packages:
media-libs/libjpeg-turbo < 1.4.2

181965 - FreeBSD openafs Multiple Vulnerabilities (bcbd3fe0-2b46-11e6-ae88-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-2860, CVE-2016-4536

Description

The scan detected that the host is missing the following update:
openafs -- multiple vulnerabilities (bcbd3fe0-2b46-11e6-ae88-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/bcbd3fe0-2b46-11e6-ae88-002590263bf5.html

Affected packages:
openafs < 1.6.17

130510 - Debian Linux 8.0 DSA-3595-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0640, CVE-2016-0641, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0655, CVE-2016-0666, CVE-2016-0668

Description

The scan detected that the host is missing the following update:
DSA-3595-1

Observation

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

http://www.debian.org/security/2016/dsa-3595

Debian 8.0
all
mariadb-server-core-10.0_10.0.25-0+deb8u1
mariadb-oqgraph-engine-10.0_10.0.25-0+deb8u1
mariadb-server-10.0_10.0.25-0+deb8u1
mariadb-client-10.0_10.0.25-0+deb8u1
mariadb-connect-engine-10.0_10.0.25-0+deb8u1
mariadb-client_10.0.25-0+deb8u1
mariadb-server_10.0.25-0+deb8u1
mariadb-common_10.0.25-0+deb8u1
mariadb-test_10.0.25-0+deb8u1
mariadb-test-10.0_10.0.25-0+deb8u1
libmariadbd-dev_10.0.25-0+deb8u1
mariadb-client-core-10.0_10.0.25-0+deb8u1

144644 - SuSE Linux 13.2 openSUSE-SU-2016:1462-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0678

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1462-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00002.html

SuSE Linux 13.2
i586
python-virtualbox-debuginfo-5.0.20-46.1
virtualbox-guest-kmp-desktop-5.0.20_k3.16.7_35-46.1
virtualbox-guest-kmp-pae-5.0.20_k3.16.7_35-46.1
virtualbox-guest-tools-5.0.20-46.1
virtualbox-5.0.20-46.1
virtualbox-host-kmp-default-5.0.20_k3.16.7_35-46.1
virtualbox-websrv-debuginfo-5.0.20-46.1
virtualbox-guest-kmp-desktop-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-host-kmp-pae-5.0.20_k3.16.7_35-46.1
virtualbox-websrv-5.0.20-46.1
virtualbox-guest-tools-debuginfo-5.0.20-46.1
virtualbox-guest-kmp-default-5.0.20_k3.16.7_35-46.1
python-virtualbox-5.0.20-46.1
virtualbox-guest-kmp-default-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-guest-x11-5.0.20-46.1

virtualbox-host-kmp-desktop-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-host-kmp-default-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-debugsource-5.0.20-46.1
virtualbox-guest-x11-debuginfo-5.0.20-46.1
virtualbox-host-kmp-pae-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-qt-5.0.20-46.1
virtualbox-host-kmp-desktop-5.0.20_k3.16.7_35-46.1
virtualbox-qt-debuginfo-5.0.20-46.1
virtualbox-debuginfo-5.0.20-46.1
virtualbox-devel-5.0.20-46.1
virtualbox-guest-kmp-pae-debuginfo-5.0.20_k3.16.7_35-46.1

noarch
virtualbox-host-source-5.0.20-46.1
virtualbox-guest-desktop-icons-5.0.20-46.1

x86_64
python-virtualbox-debuginfo-5.0.20-46.1
virtualbox-guest-kmp-desktop-5.0.20_k3.16.7_35-46.1
virtualbox-guest-tools-5.0.20-46.1
virtualbox-5.0.20-46.1
virtualbox-host-kmp-default-5.0.20_k3.16.7_35-46.1
virtualbox-websrv-debuginfo-5.0.20-46.1
virtualbox-guest-kmp-desktop-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-websrv-5.0.20-46.1
virtualbox-guest-tools-debuginfo-5.0.20-46.1
virtualbox-guest-kmp-default-5.0.20_k3.16.7_35-46.1
python-virtualbox-5.0.20-46.1
virtualbox-guest-kmp-default-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-guest-x11-5.0.20-46.1
virtualbox-host-kmp-desktop-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-host-kmp-default-debuginfo-5.0.20_k3.16.7_35-46.1
virtualbox-debugsource-5.0.20-46.1
virtualbox-guest-x11-debuginfo-5.0.20-46.1
virtualbox-qt-5.0.20-46.1
virtualbox-host-kmp-desktop-5.0.20_k3.16.7_35-46.1
virtualbox-qt-debuginfo-5.0.20-46.1
virtualbox-debuginfo-5.0.20-46.1
virtualbox-devel-5.0.20-46.1

170682 - Amazon Linux AMI ALAS-2016-710 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2167, CVE-2016-2168

Description

The scan detected that the host is missing the following update:
ALAS-2016-710

Observation

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

https://alas.aws.amazon.com/ALAS-2016-710.html

Amazon Linux AMI
x86_64

mod_dav_svn-debuginfo-1.9.4-2.52.amzn1
mod_dav_svn-1.9.4-2.52.amzn1

i686
mod_dav_svn-1.9.4-2.52.amzn1
mod_dav_svn-debuginfo-1.9.4-2.52.amzn1

170689 - Amazon Linux AMI ALAS-2016-709 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2167, CVE-2016-2168

Description

The scan detected that the host is missing the following update:
ALAS-2016-709

Observation

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

https://alas.aws.amazon.com/ALAS-2016-709.html

Amazon Linux AMI
x86_64
subversion-debuginfo-1.9.4-2.54.amzn1
subversion-python27-1.9.4-2.54.amzn1
subversion-ruby-1.9.4-2.54.amzn1
subversion-tools-1.9.4-2.54.amzn1
subversion-perl-1.9.4-2.54.amzn1
subversion-1.9.4-2.54.amzn1
subversion-python26-1.9.4-2.54.amzn1
subversion-libs-1.9.4-2.54.amzn1
subversion-devel-1.9.4-2.54.amzn1
mod24_dav_svn-1.9.4-2.54.amzn1
subversion-javahl-1.9.4-2.54.amzn1

i686
subversion-tools-1.9.4-2.54.amzn1
subversion-debuginfo-1.9.4-2.54.amzn1
subversion-python27-1.9.4-2.54.amzn1
subversion-ruby-1.9.4-2.54.amzn1
subversion-devel-1.9.4-2.54.amzn1
subversion-perl-1.9.4-2.54.amzn1
subversion-1.9.4-2.54.amzn1
subversion-python26-1.9.4-2.54.amzn1
subversion-libs-1.9.4-2.54.amzn1
mod24_dav_svn-1.9.4-2.54.amzn1
subversion-javahl-1.9.4-2.54.amzn1

181966 - FreeBSD ikiwiki XSS Vulnerability (0297b260-2b3b-11e6-ae88-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-4561

Description

The scan detected that the host is missing the following update:
ikiwiki -- XSS vulnerability (0297b260-2b3b-11e6-ae88-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/0297b260-2b3b-11e6-ae88-002590263bf5.html

Affected packages:
ikiwiki < 3.20160509

181967 - FreeBSD openafs Local DoS Vulnerability (2e8fe57e-2b46-11e6-ae88-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-8312

Description

The scan detected that the host is missing the following update:
openafs -- local DoS vulnerability (2e8fe57e-2b46-11e6-ae88-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/2e8fe57e-2b46-11e6-ae88-002590263bf5.html

Affected packages:
openafs < 1.6.16

88783 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2016-155-01 Update Is Not Installed

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

Risk Level: Low

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:
SSA:2016-155-01

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.543072

Slackware 14.0
x86_64
ntp-4.2.8p8-x86_64-1

Slackware 13.0
x86_64
ntp-4.2.8p8-x86_64-1

Slackware 13.1
x86_64
ntp-4.2.8p8-x86_64-1

Slackware 14.1
x86_64
ntp-4.2.8p8-x86_64-1

Slackware 13.37
x86_64
ntp-4.2.8p8-x86_64-1

130512 - Debian Linux 8.0 DSA-3591-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5118

Description

The scan detected that the host is missing the following update:
DSA-3591-1

Observation

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

http://www.debian.org/security/2016/dsa-3591

Debian 8.0
all
imagemagick_8:6.8.9.9-5+deb8u3

130513 - Debian Linux 8.0 DSA-3596-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
DSA-3596-1

Observation

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

http://www.debian.org/security/2016/dsa-3596

Debian 8.0
all
libspice-server-dev_0.12.5-1+deb8u3
spice-client_0.12.5-1+deb8u3
libspice-server1-dbg_0.12.5-1+deb8u3
libspice-server1_0.12.5-1+deb8u3

130514 - Debian Linux 8.0 DSA-3597-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
DSA-3597-1

Observation

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

http://www.debian.org/security/2016/dsa-3597

Debian 8.0
all
expat_2.1.0-6+deb8u3

130515 - Debian Linux 8.0 DSA-3592-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4450

Description

The scan detected that the host is missing the following update:
DSA-3592-1

Observation

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

http://www.debian.org/security/2016/dsa-3592

Debian 8.0
all
nginx_1.6.2-5+deb8u2

181961 - FreeBSD h2o Use After Free On Premature Connection Close (65bb1858-27de-11e6-b714-74d02b9a84d5)

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:
h2o -- use after free on premature connection close (65bb1858-27de-11e6-b714-74d02b9a84d5)

Observation

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

http://www.vuxml.org/freebsd/65bb1858-27de-11e6-b714-74d02b9a84d5.html

Affected packages:
h2o < 1.7.3

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

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

Risk Level: Low

CVE: CVE-2016-2834

Description

The scan detected that the host is missing the following update:
NSS -- multiple vulnerabilities (32166082-53fa-41fa-b081-207e7a989a0a)

Observation

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

http://www.vuxml.org/freebsd/32166082-53fa-41fa-b081-207e7a989a0a.html

Affected packages:
3.22 <= nss < 3.23
3.22 <= linux-c6-nss < 3.23
linux-seamonkey < 2.44

181964 - FreeBSD gnutls File Overwrite By Setuid Programs (9c196cfd-2ccc-11e6-94b0-0011d823eebd)

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:
gnutls -- file overwrite by setuid programs (9c196cfd-2ccc-11e6-94b0-0011d823eebd)

Observation

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

http://www.vuxml.org/freebsd/9c196cfd-2ccc-11e6-94b0-0011d823eebd.html

Affected packages:
3.4.12 <= gnutls < 3.4.13

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

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

Risk Level: Low

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

Description

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

mozilla -- multiple vulnerabilities (8065d37b-8e7c-4707-a608-1b0a2b8509c3)

Observation

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

http://www.vuxml.org/freebsd/8065d37b-8e7c-4707-a608-1b0a2b8509c3.html

Affected packages:
firefox < 47.0,1
seamonkey < 2.44
linux-seamonkey < 2.44
firefox-esr < 45.2.0,1
linux-firefox < 45.2.0,2
libxul < 45.2.0
thunderbird < 45.2.0
linux-thunderbird < 45.2.0

185304 - Ubuntu Linux 14.04, 15.10, 16.04 USN-2991-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4450

Description

The scan detected that the host is missing the following update:
USN-2991-1

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/003448.html

Ubuntu 16.04

nginx-full_1.10.0-0ubuntu0.16.04.2
nginx-light_1.10.0-0ubuntu0.16.04.2
nginx-core_1.10.0-0ubuntu0.16.04.2
nginx-extras_1.10.0-0ubuntu0.16.04.2

Ubuntu 15.10

nginx-extras_1.9.3-1ubuntu1.2
nginx-core_1.9.3-1ubuntu1.2
nginx-full_1.9.3-1ubuntu1.2
nginx-light_1.9.3-1ubuntu1.2

Ubuntu 14.04

nginx-core_1.4.6-1ubuntu3.5
nginx-extras_1.4.6-1ubuntu3.5
nginx-light_1.4.6-1ubuntu3.5
nginx-full_1.4.6-1ubuntu3.5

20124 - (HPSBGN03602) HPE RESTful Interface Tool Local Information Disclosure Vulnerability

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

Risk Level: Low

CVE: CVE-2016-2023

Description

An information disclosure vulnerability is present in some versions of HPE RESTful Interface Tool.

Observation

HPE RESTful Interface Tool is a tool used to access RESTful API of HPE Integrated Lights-Out (iLO).

An information disclosure vulnerability is present in some versions of HPE RESTful Interface Tool. The flaw occurs due to unknown issue. Successful exploitation could allow an attacker to obtain sensitive information.

20125 - (HPSBGN03602) HPE RESTful Interface Tool Local Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2016-2023

Description

An information disclosure vulnerability is present in some versions of HPE RESTful Interface Tool.

Observation

HPE RESTful Interface Tool is a tool used to access RESTful API of HPE Integrated Lights-Out (iLO).

An information disclosure vulnerability is present in some versions of HPE RESTful Interface Tool. The flaw occurs due to unknown issue. Successful exploitation could allow an attacker to obtain sensitive information.

144656 - SuSE Linux 13.2 openSUSE-SU-2016:1461-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8872, CVE-2016-4804

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1461-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00001.html

SuSE Linux 13.2
x86_64
dosfstools-debugsource-3.0.26-3.8.1
dosfstools-debuginfo-3.0.26-3.8.1
dosfstools-3.0.26-3.8.1

i586
dosfstools-debugsource-3.0.26-3.8.1
dosfstools-debuginfo-3.0.26-3.8.1

dosfstools-3.0.26-3.8.1

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

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

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

Risk Level: High

CVE: CVE-2016-1096, CVE-2016-1097, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1101, CVE-2016-1102, CVE-2016-1103, CVE-2016-1104, CVE-2016-1105, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, CVE-2016-4109, CVE-2016-4110, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4116, CVE-2016-4117, CVE-2016-4120, CVE-2016-4121, CVE-2016-4160, CVE-2016-4161, CVE-2016-4162, CVE-2016-4163

Update Details

CVE 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

FASLScript is updated

181952 - FreeBSD expat Denial Of Service Vulnerability On Malformed Input (57b3aba7-1e25-11e6-8dd3-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-0718

Update Details

FASLScript is updated

20116 - Google Chrome Multiple Vulnerabilities Prior To 51.0.2704.63

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

Risk Level: Medium

CVE: CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1676, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695

Update Details

Risk is updated

20117 - Google Chrome Multiple Vulnerabilities Prior To 51.0.2704.63

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1676, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695

Update Details

Risk is updated

20122 - Google Chrome Multiple Vulnerabilities Prior To 51.0.2704.79

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

Risk Level: Medium

CVE: CVE-2016-1696, CVE-2016-1697, CVE-2016-1698, CVE-2016-1699, CVE-2016-1700, CVE-2016-1701, CVE-2016-1702, CVE-2016-1703

Update Details

Risk is updated

20123 - Google Chrome Multiple Vulnerabilities Prior To 51.0.2704.79

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-1696, CVE-2016-1697, CVE-2016-1698, CVE-2016-1699, CVE-2016-1700, CVE-2016-1701, CVE-2016-1702, CVE-2016-1703

Update Details

Risk is updated

33145 - Oracle Solaris 150401-37 Update Is Not Installed

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

Risk Level: Medium

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

Update Details

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

181955 - FreeBSD chromium Multiple Vulnerabilities (1a6bbb95-24b8-11e6-bd31-3065ec8fd3ec)

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

Risk Level: Medium

CVE: CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695

Update Details

Risk is updated

130507 - Debian Linux 8.0 DSA-3588-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1902, CVE-2016-4423

Update Details

Risk is updated

20022 - (MS16-065) Microsoft .NET Framework Encryption TLS/SSL Information Disclosure (3156757)

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

Risk Level: Medium

CVE: CVE-2016-0149

Update Details

Risk is updated

20023 - (MS16-065) Security Update for .NET Framework (3156757)

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

Risk Level: Medium

CVE: CVE-2016-0149

Update Details

Risk is updated

33162 - Oracle Solaris 150400-37 Update Is Not Installed

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

Risk Level: Medium

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

Update Details

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

33168 - Oracle Solaris 149638-05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-5864

Update Details

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

33319 - Oracle Solaris 151913-05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33323 - Oracle Solaris 151912-05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33329 - Oracle Solaris 151915-05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33330 - Oracle Solaris 151914-05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

181954 - FreeBSD nginx A Specially Crafted Request Might Result In Worker Process Crash (36cf7670-2774-11e6-af29-f0def16c5c1b)

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

Risk Level: Low

CVE: CVE-2016-4450

Update Details

FASLScript is updated

144633 - SuSE Linux 13.2 openSUSE-SU-2016:1417-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3697

Update Details

Risk is updated

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

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

Risk Level: Low

CVE: CVE-2016-3697

Update Details

Risk is updated

185297 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2986-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8872, CVE-2016-4804

Update Details

Risk 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.