

MCAFFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

145032 - SuSE SLES 11 SP4 SUSE-SU-2016:2976-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-7513, CVE-2015-8956, CVE-2016-0823, CVE-2016-3841, CVE-2016-4998, CVE-2016-5696, CVE-2016-6480, CVE-2016-6828, CVE-2016-7042, CVE-2016-7097, CVE-2016-7117, CVE-2016-7425

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2976-1

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-December/002439.html>

SuSE SLES 11 SP4

i586
kernel-trace-base-3.0.101-88.1
kernel-pae-3.0.101-88.1
kernel-default-devel-3.0.101-88.1
kernel-pae-devel-3.0.101-88.1
kernel-pae-base-3.0.101-88.1
kernel-xen-base-3.0.101-88.1
kernel-trace-devel-3.0.101-88.1
kernel-ec2-devel-3.0.101-88.1
kernel-ec2-3.0.101-88.1
kernel-source-3.0.101-88.1
kernel-trace-3.0.101-88.1
kernel-xen-3.0.101-88.1
kernel-default-3.0.101-88.1
kernel-default-base-3.0.101-88.1
kernel-ec2-base-3.0.101-88.1
kernel-xen-devel-3.0.101-88.1
kernel-syms-3.0.101-88.1

x86_64

kernel-trace-base-3.0.101-88.1
kernel-default-devel-3.0.101-88.1
kernel-xen-base-3.0.101-88.1
kernel-trace-devel-3.0.101-88.1
kernel-ec2-devel-3.0.101-88.1
kernel-ec2-3.0.101-88.1
kernel-source-3.0.101-88.1
kernel-trace-3.0.101-88.1

kernel-xen-3.0.101-88.1
kernel-default-3.0.101-88.1
kernel-default-base-3.0.101-88.1
kernel-ec2-base-3.0.101-88.1
kernel-xen-devel-3.0.101-88.1
kernel-syms-3.0.101-88.1

145038 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2988-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7161, CVE-2016-7170, CVE-2016-7421, CVE-2016-7466, CVE-2016-7908, CVE-2016-7909, CVE-2016-8576, CVE-2016-8577, CVE-2016-8578, CVE-2016-8667, CVE-2016-8669, CVE-2016-8909, CVE-2016-8910, CVE-2016-9101, CVE-2016-9102, CVE-2016-9103, CVE-2016-9104, CVE-2016-9105, CVE-2016-9106

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2988-1

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-December/002440.html>

SuSE SLES 12 SP1

noarch
qemu-sgabios-8-24.6
qemu-seabios-1.8.1-24.6
qemu-ipxe-1.0.0-24.6
qemu-vgabios-1.8.1-24.6

x86_64

qemu-block-curl-2.3.1-24.6
qemu-kvm-2.3.1-24.6
qemu-guest-agent-2.3.1-24.6
qemu-lang-2.3.1-24.6
qemu-tools-debuginfo-2.3.1-24.6
qemu-debugsource-2.3.1-24.6
qemu-block-rbd-debuginfo-2.3.1-24.6
qemu-x86-2.3.1-24.6
qemu-block-rbd-2.3.1-24.6
qemu-guest-agent-debuginfo-2.3.1-24.6
qemu-tools-2.3.1-24.6
qemu-2.3.1-24.6
qemu-block-curl-debuginfo-2.3.1-24.6

SuSE SLED 12 SP1

x86_64
qemu-block-curl-debuginfo-2.3.1-24.6
qemu-debugsource-2.3.1-24.6
qemu-block-curl-2.3.1-24.6
qemu-tools-debuginfo-2.3.1-24.6
qemu-2.3.1-24.6
qemu-x86-2.3.1-24.6
qemu-tools-2.3.1-24.6
qemu-kvm-2.3.1-24.6

noarch
qemu-sgabios-8-24.6
qemu-seabios-1.8.1-24.6
qemu-ipxe-1.0.0-24.6
qemu-vgabios-1.8.1-24.6

178252 - Gentoo Linux GLSA-201612-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2830

Description

The scan detected that the host is missing the following update:
GLSA-201612-08

Observation

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

<https://security.gentoo.org/glsa/201612-08>

Affected packages:

net-fs/cifs-utils < 6.4

178253 - Gentoo Linux GLSA-201612-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8659

Description

The scan detected that the host is missing the following update:
GLSA-201612-06

Observation

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

<https://security.gentoo.org/glsa/201612-06>

Affected packages:

net-libs/nghttp2 < 1.6.0

178255 - Gentoo Linux GLSA-201612-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9496, CVE-2015-7805

Description

The scan detected that the host is missing the following update:
GLSA-201612-03

Observation

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

<https://security.gentoo.org/glsa/201612-03>

Affected packages:

media-libs/libsndfile < 1.0.26

178267 - Gentoo Linux GLSA-201611-21 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718, CVE-2016-5010, CVE-2016-5842, CVE-2016-6491, CVE-2016-7799, CVE-2016-7906

Description

The scan detected that the host is missing the following update:
GLSA-201611-21

Observation

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

<https://security.gentoo.org/glsa/201611-21>

Affected packages:

media-gfx/imagemagick < 6.9.6.2

20933 - (VMSA-2016-0022) VMware vRealize Automation XML External Entity Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7460

Description

An XML External Entity (XXE) vulnerability is present in some versions of VMware vRealize Automation.

Observation

VMware vRealize Automation integrates with VMware vCloud Suite and automates IT tasks.

An XML External Entity (XXE) vulnerability is present in some versions of VMware vRealize Automation. The flaw lies in the Single Sign-On functionality. Successful exploitation could allow an attacker to retrieve sensitive data or cause a denial of service condition.

20953 - Dell iDRAC7 And iDRAC8 Devices Code Injection Vulnerability

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

Risk Level: High

CVE: CVE-2016-5685

Description

A string injection vulnerability is present in some versions of Dell Integrated Dell Remote Access Controller.

Observation

Dell Integrated Dell Remote Access Controller is a popular embedded server management solution.

A string injection vulnerability is present in some versions of Dell Integrated Dell Remote Access Controller. The flaw lies in an unknown component of this product. Successful exploitation could allow an authenticated user to gain bash shell access into the system bypassing security measures.

141376 - Red Hat Enterprise Linux RHSA-2016-2843 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9079

Description

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

RHSA-2016-2843

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2843.html>

RHEL5S

i386

firefox-45.5.1-1.el5_11

firefox-debuginfo-45.5.1-1.el5_11

x86_64

firefox-45.5.1-1.el5_11

firefox-debuginfo-45.5.1-1.el5_11

RHEL7S

x86_64

firefox-45.5.1-1.el7_3

firefox-debuginfo-45.5.1-1.el7_3

RHEL6S

i386

firefox-45.5.1-1.el6_8

firefox-debuginfo-45.5.1-1.el6_8

x86_64

firefox-45.5.1-1.el6_8

firefox-debuginfo-45.5.1-1.el6_8

RHEL6WS

x86_64

firefox-45.5.1-1.el6_8

firefox-debuginfo-45.5.1-1.el6_8

i386

firefox-45.5.1-1.el6_8

firefox-debuginfo-45.5.1-1.el6_8

RHEL5D

x86_64

firefox-45.5.1-1.el5_11

firefox-debuginfo-45.5.1-1.el5_11

i386

firefox-45.5.1-1.el5_11

firefox-debuginfo-45.5.1-1.el5_11

RHEL7D

x86_64

firefox-45.5.1-1.el7_3

firefox-debuginfo-45.5.1-1.el7_3

RHEL6D

x86_64

firefox-45.5.1-1.el6_8

firefox-debuginfo-45.5.1-1.el6_8

i386

firefox-45.5.1-1.el6_8

firefox-debuginfo-45.5.1-1.el6_8

RHEL7WS

x86_64

firefox-45.5.1-1.el7_3

firefox-debuginfo-45.5.1-1.el7_3

145043 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2953-1 Update Is Not Installed

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

Risk Level: High

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

Description

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

SUSE-SU-2016:2953-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2016-November/002431.html>

SuSE SLED 12 SP1

x86_64

java-1_7_0-openjdk-1.7.0.121-36.2

java-1_7_0-openjdk-headless-1.7.0.121-36.2

java-1_7_0-openjdk-headless-debuginfo-1.7.0.121-36.2

java-1_7_0-openjdk-debugsource-1.7.0.121-36.2

java-1_7_0-openjdk-debuginfo-1.7.0.121-36.2

SuSE SLES 12 SP2

x86_64

java-1_7_0-openjdk-demo-1.7.0.121-36.2

java-1_7_0-openjdk-devel-1.7.0.121-36.2

java-1_7_0-openjdk-1.7.0.121-36.2

java-1_7_0-openjdk-devel-debuginfo-1.7.0.121-36.2

java-1_7_0-openjdk-headless-debuginfo-1.7.0.121-36.2

java-1_7_0-openjdk-demo-debuginfo-1.7.0.121-36.2

java-1_7_0-openjdk-debuginfo-1.7.0.121-36.2

java-1_7_0-openjdk-debugsource-1.7.0.121-36.2
java-1_7_0-openjdk-headless-1.7.0.121-36.2

SuSE SLED 12 SP2

x86_64

java-1_7_0-openjdk-1.7.0.121-36.2
java-1_7_0-openjdk-headless-1.7.0.121-36.2
java-1_7_0-openjdk-headless-debuginfo-1.7.0.121-36.2
java-1_7_0-openjdk-debugsource-1.7.0.121-36.2
java-1_7_0-openjdk-debuginfo-1.7.0.121-36.2

SuSE SLES 12 SP1

x86_64

java-1_7_0-openjdk-demo-1.7.0.121-36.2
java-1_7_0-openjdk-devel-1.7.0.121-36.2
java-1_7_0-openjdk-1.7.0.121-36.2
java-1_7_0-openjdk-devel-debuginfo-1.7.0.121-36.2
java-1_7_0-openjdk-headless-debuginfo-1.7.0.121-36.2
java-1_7_0-openjdk-demo-debuginfo-1.7.0.121-36.2
java-1_7_0-openjdk-debuginfo-1.7.0.121-36.2
java-1_7_0-openjdk-debugsource-1.7.0.121-36.2
java-1_7_0-openjdk-headless-1.7.0.121-36.2

145047 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2971-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8964, CVE-2015-2325, CVE-2015-2327, CVE-2015-2328, CVE-2015-3210, CVE-2015-3217, CVE-2015-5073, CVE-2015-8380, CVE-2015-8381, CVE-2015-8382, CVE-2015-8383, CVE-2015-8384, CVE-2015-8385, CVE-2015-8386, CVE-2015-8387, CVE-2015-8388, CVE-2015-8389, CVE-2015-8390, CVE-2015-8391, CVE-2015-8392, CVE-2015-8393, CVE-2015-8394, CVE-2015-8395, CVE-2016-1283, CVE-2016-3191

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2971-1

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-December/002436.html>

SuSE SLED 12 SP2

x86_64

libpcrepp0-8.39-5.1
libpcre1-32bit-8.39-5.1
libpcre1-8.39-5.1
libpcrepp0-debuginfo-8.39-5.1
pcre-debugsource-8.39-5.1
libpcre1-debuginfo-8.39-5.1
libpcre16-0-debuginfo-8.39-5.1
libpcrepp0-32bit-8.39-5.1
libpcre1-debuginfo-32bit-8.39-5.1
libpcre16-0-8.39-5.1
libpcrepp0-debuginfo-32bit-8.39-5.1

SuSE SLES 12 SP2

x86_64

pcre-debugsource-8.39-5.1
libpcre1-debuginfo-32bit-8.39-5.1
libpcre1-8.39-5.1
libpcre16-0-debuginfo-8.39-5.1
libpcre1-32bit-8.39-5.1
libpcre1-debuginfo-8.39-5.1
libpcre16-0-8.39-5.1

SuSE SLES 12 SP1

x86_64
pcre-debugsource-8.39-5.1
libpcre1-debuginfo-32bit-8.39-5.1
libpcre1-8.39-5.1
libpcre16-0-debuginfo-8.39-5.1
libpcre1-32bit-8.39-5.1
libpcre1-debuginfo-8.39-5.1
libpcre16-0-8.39-5.1

SuSE SLED 12 SP1

x86_64
libpcrecpp0-8.39-5.1
libpcre1-32bit-8.39-5.1
libpcre1-8.39-5.1
libpcrecpp0-debuginfo-8.39-5.1
pcre-debugsource-8.39-5.1
libpcre1-debuginfo-8.39-5.1
libpcre16-0-debuginfo-8.39-5.1
libpcrecpp0-32bit-8.39-5.1
libpcre1-debuginfo-32bit-8.39-5.1
libpcre16-0-8.39-5.1
libpcrecpp0-debuginfo-32bit-8.39-5.1

145048 - SuSE Linux 13.1 openSUSE-SU-2016:2990-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2990-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00016.html>

SuSE Linux 13.1

i586
java-1_7_0-openjdk-debugsource-1.7.0.121-24.42.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.121-24.42.1
java-1_7_0-openjdk-accessibility-1.7.0.121-24.42.1
java-1_7_0-openjdk-1.7.0.121-24.42.1
java-1_7_0-openjdk-demo-1.7.0.121-24.42.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.121-24.42.1
java-1_7_0-openjdk-src-1.7.0.121-24.42.1
java-1_7_0-openjdk-debuginfo-1.7.0.121-24.42.1

java-1_7_0-openjdk-headless-1.7.0.121-24.42.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.121-24.42.1
java-1_7_0-openjdk-devel-1.7.0.121-24.42.1

noarch
java-1_7_0-openjdk-javadoc-1.7.0.121-24.42.1

x86_64
java-1_7_0-openjdk-debugsource-1.7.0.121-24.42.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.121-24.42.1
java-1_7_0-openjdk-accessibility-1.7.0.121-24.42.1
java-1_7_0-openjdk-1.7.0.121-24.42.1
java-1_7_0-openjdk-demo-1.7.0.121-24.42.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.121-24.42.1
java-1_7_0-openjdk-src-1.7.0.121-24.42.1
java-1_7_0-openjdk-debuginfo-1.7.0.121-24.42.1
java-1_7_0-openjdk-headless-1.7.0.121-24.42.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.121-24.42.1
java-1_7_0-openjdk-devel-1.7.0.121-24.42.1

160176 - CentOS 5, 6 CESA-2016-2843 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9079

Description

The scan detected that the host is missing the following update:
CESA-2016-2843

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-December/022168.html>
<http://lists.centos.org/pipermail/centos-announce/2016-December/022167.html>

CentOS 5
x86_64
firefox-45.5.1-1.el5.centos

i386
firefox-45.5.1-1.el5.centos

CentOS 6
x86_64
firefox-45.5.1-1.el6.centos

i686
firefox-45.5.1-1.el6.centos

163234 - Oracle Enterprise Linux ELSA-2016-2843 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9079

Description

The scan detected that the host is missing the following update:
ELSA-2016-2843

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006549.html>
<http://oss.oracle.com/pipermail/el-errata/2016-December/006550.html>
<http://oss.oracle.com/pipermail/el-errata/2016-December/006548.html>

OEL6
x86_64
firefox-45.5.1-1.0.1.el6_8

i386
firefox-45.5.1-1.0.1.el6_8

OEL5
x86_64
firefox-45.5.1-1.0.1.el5_11

i386
firefox-45.5.1-1.0.1.el5_11

OEL7
x86_64
firefox-45.5.1-1.0.1.el7_3

178263 - Gentoo Linux GLSA-201612-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8557

Description

The scan detected that the host is missing the following update:
GLSA-201612-05

Observation

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

<https://security.gentoo.org/glsa/201612-05>

Affected packages:
dev-python/pygments < 2.0.2-r1

185512 - Ubuntu Linux 14.04 USN-3146-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7097, CVE-2016-7425, CVE-2016-8658, CVE-2016-9644

Description

The scan detected that the host is missing the following update:
USN-3146-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003650.html>

Ubuntu 14.04

linux-image-4.4.0-51-lowlatency_4.4.0-51.72~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.51.38
linux-image-4.4.0-51-powerpc-smp_4.4.0-51.72~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.51.38
linux-image-4.4.0-51-powerpc64-smp_4.4.0-51.72~14.04.1
linux-image-4.4.0-51-powerpc64-emb_4.4.0-51.72~14.04.1
linux-image-4.4.0-51-powerpc-e500mc_4.4.0-51.72~14.04.1
linux-image-generic-lpae-lts-xenial_4.4.0.51.38
linux-image-lowlatency-lts-xenial_4.4.0.51.38
linux-image-powerpc-smp-lts-xenial_4.4.0.51.38
linux-image-generic-lts-xenial_4.4.0.51.38
linux-image-4.4.0-51-generic-lpae_4.4.0-51.72~14.04.1
linux-image-4.4.0-51-generic_4.4.0-51.72~14.04.1
linux-image-virtual-lts-xenial_4.4.0.51.38
linux-image-powerpc64-emb-lts-xenial_4.4.0.51.38

185517 - Ubuntu Linux 16.04 USN-3146-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7097, CVE-2016-7425, CVE-2016-8658, CVE-2016-9644

Description

The scan detected that the host is missing the following update:
USN-3146-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003649.html>

Ubuntu 16.04

linux-image-generic_4.4.0.51.54
linux-image-powerpc-smp_4.4.0.51.54
linux-image-powerpc64-smp_4.4.0.51.54
linux-image-4.4.0-51-powerpc-e500mc_4.4.0-51.72
linux-image-4.4.0-51-generic_4.4.0-51.72
linux-image-powerpc-e500mc_4.4.0.51.54
linux-image-lowlatency_4.4.0.51.54
linux-image-4.4.0-51-powerpc64-smp_4.4.0-51.72
linux-image-4.4.0-51-powerpc-smp_4.4.0-51.72
linux-image-4.4.0-51-generic-lpae_4.4.0-51.72
linux-image-generic-lpae_4.4.0.51.54
linux-image-powerpc64-emb_4.4.0.51.54

linux-image-4.4.0-51-lowlatency_4.4.0-51.72
linux-image-4.4.0-51-powerpc64-emb_4.4.0-51.72

20941 - (SOL91100352) F5 BIG-IP Mozilla NSS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-1950

Description

A buffer overflow vulnerability is present in Mozilla NSS libraries in some versions of F5 BIG-IP systems.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A buffer overflow vulnerability is present in Mozilla NSS libraries in some versions of F5 BIG-IP systems. The flaw lies in Mozilla Network Security Services (NSS) libraries. Successful exploitation could allow an attacker to execute arbitrary code, retrieve sensitive data or cause a denial of service condition.

20942 - (SOL20145801) F5 BIG-IP Mozilla NSS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-1979

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Mozilla Network Security Services. Successful exploitation could allow an attacker to cause a denial of service condition or possibly have other unspecified impact in the target system.

141375 - Red Hat Enterprise Linux RHSA-2016-2850 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9079

Description

The scan detected that the host is missing the following update:
RHSA-2016-2850

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2850.html>

RHEL6S
i386

thunderbird-45.5.1-1.el6_8
thunderbird-debuginfo-45.5.1-1.el6_8

x86_64
thunderbird-45.5.1-1.el6_8
thunderbird-debuginfo-45.5.1-1.el6_8

RHEL6WS
x86_64
thunderbird-45.5.1-1.el6_8
thunderbird-debuginfo-45.5.1-1.el6_8

i386
thunderbird-45.5.1-1.el6_8
thunderbird-debuginfo-45.5.1-1.el6_8

RHEL5D
x86_64
thunderbird-debuginfo-45.5.1-1.el5_11
thunderbird-45.5.1-1.el5_11

i386
thunderbird-debuginfo-45.5.1-1.el5_11
thunderbird-45.5.1-1.el5_11

RHEL7D
x86_64
thunderbird-debuginfo-45.5.1-1.el7_3
thunderbird-45.5.1-1.el7_3

RHEL6D
x86_64
thunderbird-45.5.1-1.el6_8
thunderbird-debuginfo-45.5.1-1.el6_8

i386
thunderbird-45.5.1-1.el6_8
thunderbird-debuginfo-45.5.1-1.el6_8

RHEL7WS
x86_64
thunderbird-debuginfo-45.5.1-1.el7_3
thunderbird-45.5.1-1.el7_3

145031 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2952-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6823, CVE-2016-8862

Description

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

SUSE-SU-2016:2952-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2016-November/002430.html>

SuSE SLED 12 SP2

x86_64

libMagickCore-6_Q16-1-32bit-6.8.8.1-47.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-47.1

ImageMagick-debugsource-6.8.8.1-47.1

libMagickWand-6_Q16-1-6.8.8.1-47.1

ImageMagick-debuginfo-6.8.8.1-47.1

libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-47.1

libMagick++-6_Q16-3-debuginfo-6.8.8.1-47.1

libMagickWand-6_Q16-1-debuginfo-6.8.8.1-47.1

ImageMagick-6.8.8.1-47.1

libMagickCore-6_Q16-1-6.8.8.1-47.1

libMagick++-6_Q16-3-6.8.8.1-47.1

SuSE SLES 12 SP2

x86_64

libMagickCore-6_Q16-1-6.8.8.1-47.1

ImageMagick-debugsource-6.8.8.1-47.1

ImageMagick-debuginfo-6.8.8.1-47.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-47.1

libMagickWand-6_Q16-1-debuginfo-6.8.8.1-47.1

libMagickWand-6_Q16-1-6.8.8.1-47.1

SuSE SLES 12 SP1

x86_64

libMagickCore-6_Q16-1-6.8.8.1-47.1

ImageMagick-debugsource-6.8.8.1-47.1

ImageMagick-debuginfo-6.8.8.1-47.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-47.1

libMagickWand-6_Q16-1-debuginfo-6.8.8.1-47.1

libMagickWand-6_Q16-1-6.8.8.1-47.1

SuSE SLED 12 SP1

x86_64

libMagickCore-6_Q16-1-32bit-6.8.8.1-47.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-47.1

ImageMagick-debugsource-6.8.8.1-47.1

libMagickWand-6_Q16-1-6.8.8.1-47.1

ImageMagick-debuginfo-6.8.8.1-47.1

libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-47.1

libMagick++-6_Q16-3-debuginfo-6.8.8.1-47.1

libMagickWand-6_Q16-1-debuginfo-6.8.8.1-47.1

ImageMagick-6.8.8.1-47.1

libMagickCore-6_Q16-1-6.8.8.1-47.1

libMagick++-6_Q16-3-6.8.8.1-47.1

145033 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3001-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7942

Description

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

SUSE-SU-2016:3001-1

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-December/002441.html>

SuSE SLED 12 SP1

x86_64

libX11-6-32bit-1.6.2-11.1
libX11-6-debuginfo-1.6.2-11.1
libX11-xcb1-32bit-1.6.2-11.1
libX11-6-debuginfo-32bit-1.6.2-11.1
libX11-xcb1-debuginfo-32bit-1.6.2-11.1
libX11-debugsource-1.6.2-11.1
libX11-6-1.6.2-11.1
libX11-xcb1-debuginfo-1.6.2-11.1
libX11-xcb1-1.6.2-11.1

noarch

libX11-data-1.6.2-11.1

SuSE SLES 12 SP2

noarch

libX11-data-1.6.2-11.1

x86_64

libX11-6-32bit-1.6.2-11.1
libX11-6-debuginfo-1.6.2-11.1
libX11-xcb1-32bit-1.6.2-11.1
libX11-6-debuginfo-32bit-1.6.2-11.1
libX11-xcb1-debuginfo-32bit-1.6.2-11.1
libX11-debugsource-1.6.2-11.1
libX11-6-1.6.2-11.1
libX11-xcb1-debuginfo-1.6.2-11.1
libX11-xcb1-1.6.2-11.1

SuSE SLED 12 SP2

x86_64

libX11-6-32bit-1.6.2-11.1
libX11-6-debuginfo-1.6.2-11.1
libX11-xcb1-32bit-1.6.2-11.1
libX11-6-debuginfo-32bit-1.6.2-11.1
libX11-xcb1-debuginfo-32bit-1.6.2-11.1
libX11-debugsource-1.6.2-11.1
libX11-6-1.6.2-11.1
libX11-xcb1-debuginfo-1.6.2-11.1
libX11-xcb1-1.6.2-11.1

noarch

libX11-data-1.6.2-11.1

SuSE SLES 12 SP1

noarch

libX11-data-1.6.2-11.1

x86_64

libX11-6-32bit-1.6.2-11.1
libX11-6-debuginfo-1.6.2-11.1
libX11-xcb1-32bit-1.6.2-11.1
libX11-6-debuginfo-32bit-1.6.2-11.1

libX11-xcb1-debuginfo-32bit-1.6.2-11.1
libX11-debugsource-1.6.2-11.1
libX11-6-1.6.2-11.1
libX11-xcb1-debuginfo-1.6.2-11.1
libX11-xcb1-1.6.2-11.1

145034 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:2954-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5011

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2954-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-November/002432.html>

SuSE SLED 12 SP2

x86_64
libblkid1-32bit-2.28-42.1
python-libmount-debugsource-2.28-42.4
util-linux-systemd-debuginfo-2.28-42.3
libblkid1-debuginfo-2.28-42.1
libuuid1-2.28-42.1
libfdisk1-debuginfo-2.28-42.1
python-libmount-debuginfo-2.28-42.4
util-linux-2.28-42.1
libmount1-2.28-42.1
util-linux-debuginfo-2.28-42.1
libuuid1-debuginfo-32bit-2.28-42.1
libsmartcols1-2.28-42.1
libmount1-debuginfo-2.28-42.1
libuuid1-debuginfo-2.28-42.1
libblkid1-2.28-42.1
uuidd-2.28-42.3
libsmartcols1-debuginfo-2.28-42.1
libmount1-32bit-2.28-42.1
util-linux-debugsource-2.28-42.1
libfdisk1-2.28-42.1
libmount1-debuginfo-32bit-2.28-42.1
libuuid-devel-2.28-42.1
util-linux-systemd-2.28-42.3
util-linux-systemd-debugsource-2.28-42.3
libblkid1-debuginfo-32bit-2.28-42.1
python-libmount-2.28-42.4
libuuid1-32bit-2.28-42.1
uuidd-debuginfo-2.28-42.3

noarch
util-linux-lang-2.28-42.1

SuSE SLES 12 SP2
noarch

util-linux-lang-2.28-42.1

x86_64

libblkid1-32bit-2.28-42.1

python-libmount-debugsource-2.28-42.4

util-linux-systemd-debuginfo-2.28-42.3

libblkid1-debuginfo-2.28-42.1

libuuid1-2.28-42.1

libfdisk1-debuginfo-2.28-42.1

python-libmount-debuginfo-2.28-42.4

util-linux-2.28-42.1

libmount1-2.28-42.1

util-linux-debuginfo-2.28-42.1

util-linux-systemd-2.28-42.3

libsmartcols1-2.28-42.1

libmount1-debuginfo-2.28-42.1

libuuid1-debuginfo-2.28-42.1

libblkid1-2.28-42.1

uuid-2.28-42.3

libmount1-32bit-2.28-42.1

python-libmount-2.28-42.4

util-linux-debugsource-2.28-42.1

libfdisk1-2.28-42.1

libmount1-debuginfo-32bit-2.28-42.1

libuuid1-debuginfo-32bit-2.28-42.1

util-linux-systemd-debugsource-2.28-42.3

libblkid1-debuginfo-32bit-2.28-42.1

libsmartcols1-debuginfo-2.28-42.1

libuuid1-32bit-2.28-42.1

uuid-debuginfo-2.28-42.3

145036 - SuSE Linux 13.2 openSUSE-SU-2016:2960-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5180

Description

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

openSUSE-SU-2016:2960-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00000.html>

SuSE Linux 13.2

x86_64

libcares2-1.10.0-2.3.1

libcares2-debugsource-1.10.0-2.3.1

libcares2-32bit-1.10.0-2.3.1

libcares2-debuginfo-32bit-1.10.0-2.3.1

libcares2-debuginfo-1.10.0-2.3.1

libcares-devel-1.10.0-2.3.1

i586

libcares2-debugsource-1.10.0-2.3.1

libcares2-debuginfo-1.10.0-2.3.1
libcares-devel-1.10.0-2.3.1
libcares2-1.10.0-2.3.1

145037 - SuSE Linux 13.2 openSUSE-SU-2016:3007-1 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-2016:3007-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00032.html>

SuSE Linux 13.2
noarch
phpMyAdmin-4.4.15.9-42.1

145039 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3014-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5285, CVE-2016-5290, CVE-2016-5291, CVE-2016-5296, CVE-2016-5297, CVE-2016-9064, CVE-2016-9066, CVE-2016-9074

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3014-1

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-December/002443.html>

SuSE SLED 12 SP1
x86_64
libsoftokn3-debuginfo-32bit-3.21.3-50.1
mozilla-nss-32bit-3.21.3-50.1
MozillaFirefox-debuginfo-45.5.0esr-88.1
libsoftokn3-debuginfo-3.21.3-50.1
mozilla-nss-debugsource-3.21.3-50.1
MozillaFirefox-translations-45.5.0esr-88.1
MozillaFirefox-debugsource-45.5.0esr-88.1
mozilla-nss-sysinit-3.21.3-50.1
libsoftokn3-3.21.3-50.1
libfreebl3-32bit-3.21.3-50.1
mozilla-nss-certs-3.21.3-50.1
mozilla-nss-3.21.3-50.1
libfreebl3-3.21.3-50.1

libfreebl3-debuginfo-3.21.3-50.1
mozilla-nss-sysinit-32bit-3.21.3-50.1
mozilla-nss-sysinit-debuginfo-32bit-3.21.3-50.1
mozilla-nss-debuginfo-32bit-3.21.3-50.1
mozilla-nss-debuginfo-3.21.3-50.1
libfreebl3-debuginfo-32bit-3.21.3-50.1
MozillaFirefox-45.5.0esr-88.1
mozilla-nss-certs-debuginfo-3.21.3-50.1
mozilla-nss-certs-32bit-3.21.3-50.1
mozilla-nss-certs-debuginfo-32bit-3.21.3-50.1
mozilla-nss-tools-3.21.3-50.1
mozilla-nss-tools-debuginfo-3.21.3-50.1
mozilla-nss-sysinit-debuginfo-3.21.3-50.1
libsoftokn3-32bit-3.21.3-50.1

SuSE SLES 12 SP2

x86_64

libsoftokn3-debuginfo-32bit-3.21.3-50.1
mozilla-nss-sysinit-debuginfo-32bit-3.21.3-50.1
mozilla-nss-32bit-3.21.3-50.1
MozillaFirefox-debuginfo-45.5.0esr-88.1
libsoftokn3-debuginfo-3.21.3-50.1
mozilla-nss-debugsource-3.21.3-50.1
MozillaFirefox-translations-45.5.0esr-88.1
MozillaFirefox-debugsource-45.5.0esr-88.1
mozilla-nss-sysinit-3.21.3-50.1
libsoftokn3-3.21.3-50.1
libfreebl3-32bit-3.21.3-50.1
mozilla-nss-certs-3.21.3-50.1
mozilla-nss-3.21.3-50.1
libfreebl3-3.21.3-50.1
libfreebl3-debuginfo-3.21.3-50.1
mozilla-nss-sysinit-32bit-3.21.3-50.1
libfreebl3-hmac-3.21.3-50.1
mozilla-nss-debuginfo-32bit-3.21.3-50.1
mozilla-nss-debuginfo-3.21.3-50.1
libfreebl3-debuginfo-32bit-3.21.3-50.1
MozillaFirefox-45.5.0esr-88.1
mozilla-nss-certs-debuginfo-3.21.3-50.1
mozilla-nss-certs-32bit-3.21.3-50.1
mozilla-nss-certs-debuginfo-32bit-3.21.3-50.1
libsoftokn3-hmac-3.21.3-50.1
mozilla-nss-tools-3.21.3-50.1
mozilla-nss-tools-debuginfo-3.21.3-50.1
mozilla-nss-sysinit-debuginfo-3.21.3-50.1
libsoftokn3-hmac-32bit-3.21.3-50.1
libfreebl3-hmac-32bit-3.21.3-50.1
libsoftokn3-32bit-3.21.3-50.1

SuSE SLED 12 SP2

x86_64

libsoftokn3-debuginfo-32bit-3.21.3-50.1
mozilla-nss-32bit-3.21.3-50.1
MozillaFirefox-debuginfo-45.5.0esr-88.1
libsoftokn3-debuginfo-3.21.3-50.1
mozilla-nss-debugsource-3.21.3-50.1
MozillaFirefox-translations-45.5.0esr-88.1
MozillaFirefox-debugsource-45.5.0esr-88.1
mozilla-nss-sysinit-3.21.3-50.1
libsoftokn3-3.21.3-50.1

libfreebl3-32bit-3.21.3-50.1
mozilla-nss-certs-3.21.3-50.1
mozilla-nss-3.21.3-50.1
libfreebl3-3.21.3-50.1
libfreebl3-debuginfo-3.21.3-50.1
mozilla-nss-sysinit-32bit-3.21.3-50.1
mozilla-nss-sysinit-debuginfo-32bit-3.21.3-50.1
mozilla-nss-debuginfo-32bit-3.21.3-50.1
mozilla-nss-debuginfo-3.21.3-50.1
libfreebl3-debuginfo-32bit-3.21.3-50.1
MozillaFirefox-45.5.0esr-88.1
mozilla-nss-certs-debuginfo-3.21.3-50.1
mozilla-nss-certs-32bit-3.21.3-50.1
mozilla-nss-certs-debuginfo-32bit-3.21.3-50.1
mozilla-nss-tools-3.21.3-50.1
mozilla-nss-tools-debuginfo-3.21.3-50.1
mozilla-nss-sysinit-debuginfo-3.21.3-50.1
libsoftokn3-32bit-3.21.3-50.1

SuSE SLES 12 SP1

x86_64

libsoftokn3-debuginfo-32bit-3.21.3-50.1
mozilla-nss-sysinit-debuginfo-32bit-3.21.3-50.1
mozilla-nss-32bit-3.21.3-50.1
MozillaFirefox-debuginfo-45.5.0esr-88.1
libsoftokn3-debuginfo-3.21.3-50.1
mozilla-nss-debugsource-3.21.3-50.1
MozillaFirefox-translations-45.5.0esr-88.1
MozillaFirefox-debugsource-45.5.0esr-88.1
mozilla-nss-sysinit-3.21.3-50.1
libsoftokn3-3.21.3-50.1
libfreebl3-32bit-3.21.3-50.1
mozilla-nss-certs-3.21.3-50.1
mozilla-nss-3.21.3-50.1
libfreebl3-3.21.3-50.1
libfreebl3-debuginfo-3.21.3-50.1
mozilla-nss-sysinit-32bit-3.21.3-50.1
libfreebl3-hmac-3.21.3-50.1
mozilla-nss-debuginfo-32bit-3.21.3-50.1
mozilla-nss-debuginfo-3.21.3-50.1
libfreebl3-debuginfo-32bit-3.21.3-50.1
MozillaFirefox-45.5.0esr-88.1
mozilla-nss-certs-debuginfo-3.21.3-50.1
mozilla-nss-certs-32bit-3.21.3-50.1
mozilla-nss-certs-debuginfo-32bit-3.21.3-50.1
libsoftokn3-hmac-3.21.3-50.1
mozilla-nss-tools-3.21.3-50.1
mozilla-nss-tools-debuginfo-3.21.3-50.1
mozilla-nss-sysinit-debuginfo-3.21.3-50.1
libsoftokn3-hmac-32bit-3.21.3-50.1
libfreebl3-hmac-32bit-3.21.3-50.1
libsoftokn3-32bit-3.21.3-50.1

145040 - SuSE SLES 11 SP4 SUSE-SU-2016:2964-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9907, CVE-2015-8957, CVE-2015-8958, CVE-2015-8959, CVE-2016-5687, CVE-2016-6823, CVE-2016-7101, CVE-2016-7514, CVE-2016-7515, CVE-2016-7516, CVE-2016-7517, CVE-2016-7518, CVE-2016-7519, CVE-2016-7522, CVE-2016-7523,

CVE-2016-7524, CVE-2016-7525, CVE-2016-7526, CVE-2016-7527, CVE-2016-7528, CVE-2016-7529, CVE-2016-7530, CVE-2016-7531, CVE-2016-7533, CVE-2016-7535, CVE-2016-7537, CVE-2016-7799, CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684, CVE-2016-8862

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2964-1

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-December/002434.html>

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.54.1

x86_64
libMagickCore1-6.4.3.6-7.54.1
libMagickCore1-32bit-6.4.3.6-7.54.1

145041 - SuSE Linux 13.1 openSUSE-SU-2016:3011-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5289, CVE-2016-5290, CVE-2016-5291, CVE-2016-5292, CVE-2016-5293, CVE-2016-5294, CVE-2016-5295, CVE-2016-5296, CVE-2016-5297, CVE-2016-5298, CVE-2016-5299, CVE-2016-9061, CVE-2016-9062, CVE-2016-9063, CVE-2016-9064, CVE-2016-9065, CVE-2016-9066, CVE-2016-9067, CVE-2016-9068, CVE-2016-9069, CVE-2016-9070, CVE-2016-9071, CVE-2016-9072, CVE-2016-9073, CVE-2016-9074, CVE-2016-9075, CVE-2016-9076, CVE-2016-9077, CVE-2016-9078, CVE-2016-9079

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3011-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00034.html>

SuSE Linux 13.1
x86_64
mozilla-nss-certs-3.26.2-94.1
libsoftokn3-debuginfo-3.26.2-94.1
MozillaFirefox-debugsource-50.0.2-131.1
MozillaThunderbird-debuginfo-45.5.1-70.92.1
libfreebl3-3.26.2-94.1
mozilla-nss-certs-32bit-3.26.2-94.1
MozillaThunderbird-45.5.1-70.92.1
MozillaThunderbird-translations-common-45.5.1-70.92.1
MozillaFirefox-debuginfo-50.0.2-131.1
mozilla-nss-32bit-3.26.2-94.1
MozillaFirefox-translations-common-50.0.2-131.1
mozilla-nss-sysinit-32bit-3.26.2-94.1
libsoftokn3-32bit-3.26.2-94.1
MozillaThunderbird-devel-45.5.1-70.92.1

MozillaFirefox-translations-other-50.0.2-131.1
libsoftokn3-3.26.2-94.1
mozilla-nss-tools-3.26.2-94.1
mozilla-nss-certs-debuginfo-3.26.2-94.1
mozilla-nss-sysinit-debuginfo-3.26.2-94.1
MozillaFirefox-50.0.2-131.1
libfreebl3-debuginfo-32bit-3.26.2-94.1
MozillaFirefox-branding-upstream-50.0.2-131.1
MozillaFirefox-devel-50.0.2-131.1
mozilla-nss-sysinit-3.26.2-94.1
mozilla-nss-3.26.2-94.1
mozilla-nss-devel-3.26.2-94.1
MozillaThunderbird-debugsource-45.5.1-70.92.1
MozillaFirefox-buildsymbols-50.0.2-131.1
mozilla-nss-tools-debuginfo-3.26.2-94.1
mozilla-nss-debuginfo-3.26.2-94.1
mozilla-nss-certs-debuginfo-32bit-3.26.2-94.1
MozillaThunderbird-buildsymbols-45.5.1-70.92.1
mozilla-nss-sysinit-debuginfo-32bit-3.26.2-94.1
libfreebl3-32bit-3.26.2-94.1
MozillaThunderbird-translations-other-45.5.1-70.92.1
libfreebl3-debuginfo-3.26.2-94.1
libsoftokn3-debuginfo-32bit-3.26.2-94.1
mozilla-nss-debuginfo-32bit-3.26.2-94.1
mozilla-nss-debugsource-3.26.2-94.1

i586

mozilla-nss-certs-3.26.2-94.1
libsoftokn3-debuginfo-3.26.2-94.1
MozillaFirefox-debugsource-50.0.2-131.1
MozillaThunderbird-debuginfo-45.5.1-70.92.1
libfreebl3-3.26.2-94.1
MozillaThunderbird-45.5.1-70.92.1
MozillaThunderbird-translations-common-45.5.1-70.92.1
MozillaFirefox-debuginfo-50.0.2-131.1
MozillaFirefox-translations-common-50.0.2-131.1
MozillaThunderbird-devel-45.5.1-70.92.1
MozillaFirefox-translations-other-50.0.2-131.1
libsoftokn3-3.26.2-94.1
mozilla-nss-tools-3.26.2-94.1
mozilla-nss-certs-debuginfo-3.26.2-94.1
mozilla-nss-sysinit-debuginfo-3.26.2-94.1
MozillaFirefox-50.0.2-131.1
MozillaFirefox-branding-upstream-50.0.2-131.1
MozillaFirefox-devel-50.0.2-131.1
mozilla-nss-sysinit-3.26.2-94.1
mozilla-nss-3.26.2-94.1
mozilla-nss-devel-3.26.2-94.1
MozillaThunderbird-debugsource-45.5.1-70.92.1
MozillaFirefox-buildsymbols-50.0.2-131.1
mozilla-nss-tools-debuginfo-3.26.2-94.1
mozilla-nss-debuginfo-3.26.2-94.1
MozillaThunderbird-buildsymbols-45.5.1-70.92.1
MozillaThunderbird-translations-other-45.5.1-70.92.1
libfreebl3-debuginfo-3.26.2-94.1
mozilla-nss-debugsource-3.26.2-94.1

145042 - SuSE Linux 13.1 openSUSE-SU-2016:3021-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-5634, CVE-2015-8956, CVE-2016-2069, CVE-2016-5696, CVE-2016-6130, CVE-2016-6327, CVE-2016-6480, CVE-2016-6828, CVE-2016-7042, CVE-2016-7097, CVE-2016-7425, CVE-2016-8658

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3021-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00039.html>

SuSE Linux 13.1

i586

iscsitarget-kmp-xen-debuginfo-1.4.20.3_k3.12.67_58-13.36.1

openvswitch-kmp-default-1.11.0_k3.12.67_58-0.43.1

cloop-debuginfo-2.639-11.36.1

virtualbox-qt-4.2.36-2.68.1

vhba-kmp-desktop-debuginfo-20130607_k3.12.67_58-2.36.1

kernel-default-debugsource-3.12.67-58.1

ndiswrapper-1.58-37.1

kernel-default-base-3.12.67-58.1

crash-kmp-xen-7.0.2_k3.12.67_58-2.36.1

crash-doc-7.0.2-2.36.1

pcfclock-kmp-desktop-0.44_k3.12.67_58-258.37.1

cloop-kmp-xen-debuginfo-2.639_k3.12.67_58-11.36.1

iscsitarget-kmp-default-1.4.20.3_k3.12.67_58-13.36.1

iscsitarget-kmp-default-debuginfo-1.4.20.3_k3.12.67_58-13.36.1

hdjmod-kmp-pae-debuginfo-1.28_k3.12.67_58-16.36.1

pcfclock-debuginfo-0.44-258.37.1

openvswitch-controller-debuginfo-1.11.0-0.43.1

kernel-default-devel-3.12.67-58.1

xen-debugsource-4.3.4_10-69.1

crash-7.0.2-2.36.1

cloop-kmp-default-debuginfo-2.639_k3.12.67_58-11.36.1

vhba-kmp-xen-debuginfo-20130607_k3.12.67_58-2.36.1

cloop-kmp-xen-2.639_k3.12.67_58-11.36.1

crash-debugsource-7.0.2-2.36.1

virtualbox-host-kmp-pae-4.2.36_k3.12.67_58-2.68.1

xtables-addons-kmp-xen-debuginfo-2.3_k3.12.67_58-2.35.1

crash-debuginfo-7.0.2-2.36.1

iscsitarget-kmp-desktop-1.4.20.3_k3.12.67_58-13.36.1

xen-libs-debuginfo-4.3.4_10-69.1

ndiswrapper-kmp-default-1.58_k3.12.67_58-37.1

iscsitarget-debuginfo-1.4.20.3-13.36.1

ndiswrapper-debugsource-1.58-37.1

pcfclock-kmp-pae-0.44_k3.12.67_58-258.37.1

openvswitch-pki-1.11.0-0.43.1

pcfclock-0.44-258.37.1

cloop-kmp-desktop-2.639_k3.12.67_58-11.36.1

xtables-addons-debuginfo-2.3-2.35.1

vhba-kmp-desktop-20130607_k3.12.67_58-2.36.1

crash-gcore-debuginfo-7.0.2-2.36.1

openvswitch-kmp-xen-debuginfo-1.11.0_k3.12.67_58-0.43.1

vhba-kmp-pae-20130607_k3.12.67_58-2.36.1

ipset-kmp-pae-6.21.1_k3.12.67_58-2.40.1

crash-kmp-xen-debuginfo-7.0.2_k3.12.67_58-2.36.1

kernel-default-3.12.67-58.1
openvswitch-1.11.0-0.43.1
hdjmod-kmp-xen-debuginfo-1.28_k3.12.67_58-16.36.1
xen-libs-4.3.4_10-69.1
ndiswrapper-kmp-default-debuginfo-1.58_k3.12.67_58-37.1
xen-kmp-pae-debuginfo-4.3.4_10_k3.12.67_58-69.1
virtualbox-devel-4.2.36-2.68.1
ndiswrapper-kmp-pae-debuginfo-1.58_k3.12.67_58-37.1
openvswitch-switch-debuginfo-1.11.0-0.43.1
vhba-kmp-debugsource-20130607-2.36.1
hdjmod-kmp-pae-1.28_k3.12.67_58-16.36.1
virtualbox-host-kmp-desktop-4.2.36_k3.12.67_58-2.68.1
virtualbox-guest-kmp-default-4.2.36_k3.12.67_58-2.68.1
virtualbox-guest-kmp-default-debuginfo-4.2.36_k3.12.67_58-2.68.1
virtualbox-guest-tools-4.2.36-2.68.1
virtualbox-debugsource-4.2.36-2.68.1
virtualbox-guest-x11-4.2.36-2.68.1
virtualbox-host-kmp-default-4.2.36_k3.12.67_58-2.68.1
ipset-6.21.1-2.40.1
kernel-syms-3.12.67-58.1
iscsitarget-kmp-pae-debuginfo-1.4.20.3_k3.12.67_58-13.36.1
openvswitch-controller-1.11.0-0.43.1
xtables-addons-kmp-desktop-2.3_k3.12.67_58-2.35.1
ndiswrapper-debuginfo-1.58-37.1
ipset-debuginfo-6.21.1-2.40.1
python-openvswitch-test-1.11.0-0.43.1
hdjmod-kmp-desktop-debuginfo-1.28_k3.12.67_58-16.36.1
xen-tools-domU-debuginfo-4.3.4_10-69.1
crash-kmp-desktop-debuginfo-7.0.2_k3.12.67_58-2.36.1
pcfclock-kmp-desktop-debuginfo-0.44_k3.12.67_58-258.37.1
vhba-kmp-default-20130607_k3.12.67_58-2.36.1
virtualbox-qt-debuginfo-4.2.36-2.68.1
xtables-addons-kmp-pae-debuginfo-2.3_k3.12.67_58-2.35.1
ipset-kmp-desktop-debuginfo-6.21.1_k3.12.67_58-2.40.1
cloop-2.639-11.36.1
hdjmod-kmp-desktop-1.28_k3.12.67_58-16.36.1
crash-eppic-7.0.2-2.36.1
cloop-kmp-pae-debuginfo-2.639_k3.12.67_58-11.36.1
python-virtualbox-debuginfo-4.2.36-2.68.1
ipset-kmp-desktop-6.21.1_k3.12.67_58-2.40.1
openvswitch-switch-1.11.0-0.43.1
crash-kmp-default-7.0.2_k3.12.67_58-2.36.1
ndiswrapper-kmp-desktop-debuginfo-1.58_k3.12.67_58-37.1
cloop-kmp-pae-2.639_k3.12.67_58-11.36.1
python-openvswitch-1.11.0-0.43.1
crash-kmp-pae-7.0.2_k3.12.67_58-2.36.1
crash-devel-7.0.2-2.36.1
iscsitarget-kmp-pae-1.4.20.3_k3.12.67_58-13.36.1
iscsitarget-kmp-desktop-debuginfo-1.4.20.3_k3.12.67_58-13.36.1
virtualbox-guest-kmp-desktop-4.2.36_k3.12.67_58-2.68.1
xen-tools-domU-4.3.4_10-69.1
ipset-kmp-pae-debuginfo-6.21.1_k3.12.67_58-2.40.1
xen-kmp-desktop-debuginfo-4.3.4_10_k3.12.67_58-69.1
xen-kmp-desktop-4.3.4_10_k3.12.67_58-69.1
openvswitch-kmp-xen-1.11.0_k3.12.67_58-0.43.1
crash-kmp-pae-debuginfo-7.0.2_k3.12.67_58-2.36.1
openvswitch-kmp-pae-1.11.0_k3.12.67_58-0.43.1
python-virtualbox-4.2.36-2.68.1
hdjmod-kmp-default-1.28_k3.12.67_58-16.36.1
openvswitch-test-1.11.0-0.43.1

ipset-devel-6.21.1-2.40.1
pcfclock-debugsource-0.44-258.37.1
kernel-default-debuginfo-3.12.67-58.1
iscsitarget-1.4.20.3-13.36.1
crash-kmp-desktop-7.0.2_k3.12.67_58-2.36.1
cloop-kmp-desktop-debuginfo-2.639_k3.12.67_58-11.36.1
xtables-addons-kmp-xen-2.3_k3.12.67_58-2.35.1
kernel-default-base-debuginfo-3.12.67-58.1
libipset3-6.21.1-2.40.1
hdjmod-kmp-xen-1.28_k3.12.67_58-16.36.1
ipset-kmp-default-debuginfo-6.21.1_k3.12.67_58-2.40.1
ndiswrapper-kmp-desktop-1.58_k3.12.67_58-37.1
ipset-kmp-xen-debuginfo-6.21.1_k3.12.67_58-2.40.1
openvswitch-kmp-default-debuginfo-1.11.0_k3.12.67_58-0.43.1
openvswitch-kmp-desktop-1.11.0_k3.12.67_58-0.43.1
virtualbox-websrv-debuginfo-4.2.36-2.68.1
virtualbox-guest-kmp-pae-4.2.36_k3.12.67_58-2.68.1
virtualbox-host-kmp-default-debuginfo-4.2.36_k3.12.67_58-2.68.1
ipset-kmp-xen-6.21.1_k3.12.67_58-2.40.1
virtualbox-host-kmp-pae-debuginfo-4.2.36_k3.12.67_58-2.68.1
xtables-addons-2.3-2.35.1
virtualbox-host-kmp-desktop-debuginfo-4.2.36_k3.12.67_58-2.68.1
virtualbox-websrv-4.2.36-2.68.1
vhba-kmp-pae-debuginfo-20130607_k3.12.67_58-2.36.1
vhba-kmp-xen-20130607_k3.12.67_58-2.36.1
virtualbox-debuginfo-4.2.36-2.68.1
xtables-addons-kmp-desktop-debuginfo-2.3_k3.12.67_58-2.35.1
openvswitch-kmp-pae-debuginfo-1.11.0_k3.12.67_58-0.43.1
ipset-debugsource-6.21.1-2.40.1
virtualbox-guest-x11-debuginfo-4.2.36-2.68.1
openvswitch-kmp-desktop-debuginfo-1.11.0_k3.12.67_58-0.43.1
iscsitarget-debugsource-1.4.20.3-13.36.1
crash-kmp-default-debuginfo-7.0.2_k3.12.67_58-2.36.1
virtualbox-4.2.36-2.68.1
cloop-debugsource-2.639-11.36.1
cloop-kmp-default-2.639_k3.12.67_58-11.36.1
crash-eppic-debuginfo-7.0.2-2.36.1
xen-devel-4.3.4_10-69.1
xtables-addons-kmp-default-debuginfo-2.3_k3.12.67_58-2.35.1
ndiswrapper-kmp-pae-1.58_k3.12.67_58-37.1
xtables-addons-kmp-pae-2.3_k3.12.67_58-2.35.1
xen-kmp-pae-4.3.4_10_k3.12.67_58-69.1
xen-kmp-default-4.3.4_10_k3.12.67_58-69.1
openvswitch-debuginfo-1.11.0-0.43.1
virtualbox-guest-kmp-pae-debuginfo-4.2.36_k3.12.67_58-2.68.1
virtualbox-guest-tools-debuginfo-4.2.36-2.68.1
hdjmod-kmp-default-debuginfo-1.28_k3.12.67_58-16.36.1
pcfclock-kmp-default-debuginfo-0.44_k3.12.67_58-258.37.1
hdjmod-debugsource-1.28-16.36.1
iscsitarget-kmp-xen-1.4.20.3_k3.12.67_58-13.36.1
libipset3-debuginfo-6.21.1-2.40.1
crash-gcore-7.0.2-2.36.1
vhba-kmp-default-debuginfo-20130607_k3.12.67_58-2.36.1
virtualbox-guest-kmp-desktop-debuginfo-4.2.36_k3.12.67_58-2.68.1
pcfclock-kmp-default-0.44_k3.12.67_58-258.37.1
xtables-addons-debugsource-2.3-2.35.1
openvswitch-debugsource-1.11.0-0.43.1

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

Risk Level: High

CVE: CVE-2016-9079

Description

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

openSUSE-SU-2016:2991-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00017.html>

SuSE Linux 13.2

x86_64

MozillaThunderbird-45.5.1-55.1

MozillaThunderbird-debugsource-45.5.1-55.1

MozillaThunderbird-translations-other-45.5.1-55.1

MozillaThunderbird-translations-common-45.5.1-55.1

MozillaThunderbird-debuginfo-45.5.1-55.1

MozillaThunderbird-devel-45.5.1-55.1

MozillaThunderbird-buildsymbols-45.5.1-55.1

i586

MozillaThunderbird-45.5.1-55.1

MozillaThunderbird-debugsource-45.5.1-55.1

MozillaThunderbird-translations-other-45.5.1-55.1

MozillaThunderbird-translations-common-45.5.1-55.1

MozillaThunderbird-debuginfo-45.5.1-55.1

MozillaThunderbird-devel-45.5.1-55.1

MozillaThunderbird-buildsymbols-45.5.1-55.1

145045 - SuSE Linux 13.2 openSUSE-SU-2016:2994-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9078, CVE-2016-9079

Description

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

openSUSE-SU-2016:2994-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00020.html>

SuSE Linux 13.2

x86_64

MozillaFirefox-translations-common-50.0.2-91.1

MozillaFirefox-buildsymbols-50.0.2-91.1

MozillaFirefox-50.0.2-91.1

MozillaFirefox-devel-50.0.2-91.1

MozillaFirefox-translations-other-50.0.2-91.1

MozillaFirefox-debuginfo-50.0.2-91.1
MozillaFirefox-debugsource-50.0.2-91.1
MozillaFirefox-branding-upstream-50.0.2-91.1

i586

MozillaFirefox-translations-common-50.0.2-91.1
MozillaFirefox-buildsymbols-50.0.2-91.1
MozillaFirefox-50.0.2-91.1
MozillaFirefox-devel-50.0.2-91.1
MozillaFirefox-translations-other-50.0.2-91.1
MozillaFirefox-debuginfo-50.0.2-91.1
MozillaFirefox-debugsource-50.0.2-91.1
MozillaFirefox-branding-upstream-50.0.2-91.1

145049 - SuSE SLED 12 SP1, 12 SP2 SUSE-SU-2016:2975-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5773, CVE-2016-9137

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2975-1

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-December/002438.html>

SuSE SLED 12 SP2

x86_64
imap-debuginfo-2007e_suse-22.1
libc-client2007e_suse-2007e_suse-22.1
libc-client2007e_suse-debuginfo-2007e_suse-22.1
imap-debugsource-2007e_suse-22.1

SuSE SLED 12 SP1

x86_64
imap-debuginfo-2007e_suse-22.1
libc-client2007e_suse-2007e_suse-22.1
libc-client2007e_suse-debuginfo-2007e_suse-22.1
imap-debugsource-2007e_suse-22.1

160175 - CentOS 5, 6 CESA-2016-2825 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5290

Description

The scan detected that the host is missing the following update:
CESA-2016-2825

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-December/022165.html>

<http://lists.centos.org/pipermail/centos-announce/2016-December/022163.html>

CentOS 5
x86_64
thunderbird-45.5.0-1.el5.centos

i386
thunderbird-45.5.0-1.el5.centos

CentOS 6
x86_64
thunderbird-45.5.0-1.el6.centos

i686
thunderbird-45.5.0-1.el6.centos

163233 - Oracle Enterprise Linux ELSA-2016-2850 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9079

Description

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

ELSA-2016-2850

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-December/006552.html>

<http://oss.oracle.com/pipermail/el-errata/2016-December/006551.html>

OEL7
x86_64
thunderbird-45.5.1-1.0.1.el7_3

OEL6
x86_64
thunderbird-45.5.1-1.0.1.el6_8

i386
thunderbird-45.5.1-1.0.1.el6_8

178251 - Gentoo Linux GLSA-201611-22 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8865, CVE-2016-3074, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544, CVE-2016-5385, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297, CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128, CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132, CVE-2016-7133, CVE-2016-7134, CVE-2016-7411, CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417, CVE-2016-7418

Description

The scan detected that the host is missing the following update:
GLSA-201611-22

Observation

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

<https://security.gentoo.org/glsa/201611-22>

Affected packages:
dev-lang/php < 5.6.28

178257 - Gentoo Linux GLSA-201612-09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5766, CVE-2016-6128, CVE-2016-6132, CVE-2016-6207, CVE-2016-7568

Description

The scan detected that the host is missing the following update:
GLSA-201612-09

Observation

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

<https://security.gentoo.org/glsa/201612-09>

Affected packages:
media-libs/gd < 2.2.3

178259 - Gentoo Linux GLSA-201612-07 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0860

Description

The scan detected that the host is missing the following update:
GLSA-201612-07

Observation

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

<https://security.gentoo.org/glsa/201612-07>

Affected packages:
app-arch/dpkg < 1.17.26

178262 - Gentoo Linux GLSA-201612-15 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0556, CVE-2015-0557, CVE-2015-2782

Description

The scan detected that the host is missing the following update:
GLSA-201612-15

Observation

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

<https://security.gentoo.org/glsa/201612-15>

Affected packages:

app-arch/arj < 3.10.22-r5

178266 - Gentoo Linux GLSA-201612-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4362

Description

The scan detected that the host is missing the following update:
GLSA-201612-02

Observation

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

<https://security.gentoo.org/glsa/201612-02>

Affected packages:

net-fs/davfs2 < 1.5.2

182189 - FreeBSD qemu Denial Of Service Vulnerability (a228c7a0-ba66-11e6-b1cf-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2015-1779

Description

The scan detected that the host is missing the following update:
qemu -- denial of service vulnerability (a228c7a0-ba66-11e6-b1cf-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/a228c7a0-ba66-11e6-b1cf-14dae9d210b8.html>

Affected packages:

qemu < 2.3.0

qemu-devel < 2.3.0

182199 - FreeBSD xen-kernel X86: Mishandling Of Instruction Pointer Truncation During Emulation (49211361-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-7093

Description

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

xen-kernel -- x86: Mishandling of instruction pointer truncation during emulation (49211361-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/49211361-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel == 4.5.3

xen-kernel == 4.6.3

4.7.0 <= xen-kernel < 4.7.1

182200 - FreeBSD xen-kernel Use After Free In FIFO Event Channel Code (4bf57137-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-7154

Description

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

xen-kernel -- use after free in FIFO event channel code (4bf57137-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/4bf57137-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

4.4 <= xen-kernel < 4.5

185495 - Ubuntu Linux 12.04 USN-3145-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7425, CVE-2016-8658

Description

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

USN-3145-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003648.html>

Ubuntu 12.04

linux-image-3.13.0-103-generic_3.13.0-103.150~precise1
linux-image-generic-lpae-lts-trusty_3.13.0.103.94
linux-image-3.13.0-103-generic-lpae_3.13.0-103.150~precise1
linux-image-generic-lts-trusty_3.13.0.103.94

185499 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3143-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5180

Description

The scan detected that the host is missing the following update:
USN-3143-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003643.html>

Ubuntu 12.04

libc-ares2_1.7.5-1ubuntu0.1

Ubuntu 16.04

libc-ares2_1.10.0-3ubuntu0.1

Ubuntu 14.04

libc-ares2_1.10.0-2ubuntu0.1

Ubuntu 16.10

libc-ares2_1.11.0-1ubuntu0.1

185501 - Ubuntu Linux 12.04 USN-3144-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7425

Description

The scan detected that the host is missing the following update:
USN-3144-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003645.html>

Ubuntu 12.04

linux-image-virtual_3.2.0.116.132
linux-image-3.2.0-116-powerpc-smp_3.2.0-116.158
linux-image-highbank_3.2.0.116.132
linux-image-3.2.0-116-virtual_3.2.0-116.158
linux-image-3.2.0-116-omap_3.2.0-116.158
linux-image-generic-pae_3.2.0.116.132
linux-image-omap_3.2.0.116.132
linux-image-3.2.0-116-powerpc64-smp_3.2.0-116.158
linux-image-generic_3.2.0.116.132
linux-image-3.2.0-116-highbank_3.2.0-116.158
linux-image-powerpc-smp_3.2.0.116.132
linux-image-3.2.0-116-generic-pae_3.2.0-116.158
linux-image-powerpc64-smp_3.2.0.116.132
linux-image-3.2.0-116-generic_3.2.0-116.158

185507 - Ubuntu Linux 16.10 USN-3147-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7097, CVE-2016-7425

Description

The scan detected that the host is missing the following update:
USN-3147-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003651.html>

Ubuntu 16.10

linux-image-4.8.0-28-lowlatency_4.8.0-28.30
linux-image-4.8.0-28-powerpc-e500mc_4.8.0-28.30
linux-image-generic-lpae_4.8.0.28.37
linux-image-lowlatency_4.8.0.28.37
linux-image-powerpc-smp_4.8.0.28.37
linux-image-powerpc64-emb_4.8.0.28.37
linux-image-4.8.0-28-powerpc-smp_4.8.0-28.30
linux-image-generic_4.8.0.28.37
linux-image-4.8.0-28-generic-lpae_4.8.0-28.30
linux-image-4.8.0-28-generic_4.8.0-28.30
linux-image-4.8.0-28-powerpc64-emb_4.8.0-28.30
linux-image-powerpc-e500mc_4.8.0.28.37

185508 - Ubuntu Linux 12.04 USN-3144-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7425

Description

The scan detected that the host is missing the following update:
USN-3144-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003646.html>

Ubuntu 12.04

linux-image-3.2.0-1494-omap4_3.2.0-1494.121
linux-image-omap4_3.2.0.1494.89

185513 - Ubuntu Linux 14.04 USN-3145-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7425, CVE-2016-8658

Description

The scan detected that the host is missing the following update:
USN-3145-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003647.html>

Ubuntu 14.04

linux-image-generic-lpae_3.13.0.103.111
linux-image-powerpc-e500mc_3.13.0.103.111
linux-image-3.13.0-103-powerpc-e500mc_3.13.0-103.150
linux-image-omap_3.13.0.103.111
linux-image-3.13.0-103-powerpc64-emb_3.13.0-103.150
linux-image-powerpc64-emb_3.13.0.103.111
linux-image-generic_3.13.0.103.111
linux-image-3.13.0-103-powerpc64-smp_3.13.0-103.150
linux-image-powerpc64-smp_3.13.0.103.111
linux-image-powerpc-smp_3.13.0.103.111
linux-image-3.13.0-103-powerpc-smp_3.13.0-103.150
linux-image-3.13.0-103-generic-lpae_3.13.0-103.150
linux-image-3.13.0-103-lowlatency_3.13.0-103.150
linux-image-3.13.0-103-generic_3.13.0-103.150
linux-image-lowlatency_3.13.0.103.111
linux-image-3.13.0-103-powerpc-e500_3.13.0-103.150

191422 - Fedora Linux 23 FEDORA-2016-2edfd75312 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7504, CVE-2016-7505, CVE-2016-7506, CVE-2016-9017, CVE-2016-9108, CVE-2016-9109, CVE-2016-9294

Description

The scan detected that the host is missing the following update:
FEDORA-2016-2edfd75312

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 23

mujs-0-6.20161031gita0ceaf5.fc23
zathura-pdf-mupdf-0.3.0-3.fc23

191431 - Fedora Linux 24 FEDORA-2016-5608472a90 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0860

Description

The scan detected that the host is missing the following update:
FEDORA-2016-5608472a90

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 24

dpkg-1.17.27-1.fc24

191446 - Fedora Linux 23 FEDORA-2016-10ec03ed27 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0860

Description

The scan detected that the host is missing the following update:
FEDORA-2016-10ec03ed27

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 23

dpkg-1.17.27-1.fc23

191449 - Fedora Linux 25 FEDORA-2016-0918477a60 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0860

Description

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

FEDORA-2016-0918477a60

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

dpkg-1.17.27-1.fc25

130641 - Debian Linux 8.0 DSA-3727-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4330, CVE-2016-4331, CVE-2016-4332, CVE-2016-4333

Description

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

DSA-3727-1

Observation

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

For more information see:

<http://www.debian.org/security/2016/dsa-3727>

Debian 8.0

all

libhdf5-openmpi-8-dbg_1.8.13+docs-15+deb8u1

hdf5-helpers_1.8.13+docs-15+deb8u1

libhdf5-doc_1.8.13+docs-15+deb8u1

libhdf5-cpp-8-dbg_1.8.13+docs-15+deb8u1

libhdf5-openmpi-dev_1.8.13+docs-15+deb8u1

libhdf5-mpich-8_1.8.13+docs-15+deb8u1

hdf5-tools_1.8.13+docs-15+deb8u1

libhdf5-openmpi-8_1.8.13+docs-15+deb8u1

libhdf5-mpich2-dev_1.8.13+docs-15+deb8u1

libhdf5-mpich-dev_1.8.13+docs-15+deb8u1

libhdf5-8_1.8.13+docs-15+deb8u1

libhdf5-serial-dev_1.8.13+docs-15+deb8u1

libhdf5-cpp-8_1.8.13+docs-15+deb8u1

libhdf5-mpi-dev_1.8.13+docs-15+deb8u1

libhdf5-mpich-8-dbg_1.8.13+docs-15+deb8u1

libhdf5-8-dbg_1.8.13+docs-15+deb8u1

libhdf5-dev_1.8.13+docs-15+deb8u1

145035 - SuSE SLES 11 SP4 SUSE-SU-2016:2958-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-0689, CVE-2012-3543

Description

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

SUSE-SU-2016:2958-1

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-December/002433.html>

SuSE SLES 11 SP4

i586

mono-data-2.6.7-0.18.1

mono-winform-2.6.7-0.18.1

mono-nunit-2.6.7-0.18.1

mono-web-2.6.7-0.18.1

mono-data-postgresql-2.6.7-0.18.1

mono-data-sqlite-2.6.7-0.18.1

mono-locale-extras-2.6.7-0.18.1

mono-core-2.6.7-0.18.1

x86_64

mono-data-2.6.7-0.18.1

mono-winform-2.6.7-0.18.1

mono-nunit-2.6.7-0.18.1

mono-web-2.6.7-0.18.1

mono-data-postgresql-2.6.7-0.18.1

mono-data-sqlite-2.6.7-0.18.1

mono-locale-extras-2.6.7-0.18.1

mono-core-2.6.7-0.18.1

145046 - SuSE Linux 13.2 openSUSE-SU-2016:2992-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1248

Description

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

openSUSE-SU-2016:2992-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00018.html>

SuSE Linux 13.2

i586

vim-7.4.461.hg.6253-3.1

vim-debugsource-7.4.461.hg.6253-3.1
vim-debuginfo-7.4.461.hg.6253-3.1
gvim-7.4.461.hg.6253-3.1
gvim-debuginfo-7.4.461.hg.6253-3.1

noarch
vim-data-7.4.461.hg.6253-3.1

x86_64
vim-7.4.461.hg.6253-3.1
vim-debugsource-7.4.461.hg.6253-3.1
vim-debuginfo-7.4.461.hg.6253-3.1
gvim-7.4.461.hg.6253-3.1
gvim-debuginfo-7.4.461.hg.6253-3.1

182185 - FreeBSD xen-kernel X86: Disallow L3 Recursive Pagetable For 32-bit PV Guests (45ca25b5-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-7092

Description

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

xen-kernel -- x86: Disallow L3 recursive pagetable for 32-bit PV guests (45ca25b5-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/45ca25b5-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.1

182193 - FreeBSD Pillow Multiple Vulnerabilities (bc4898d5-a794-11e6-b2d3-60a44ce6887b)

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

Risk Level: Medium

CVE: CVE-2016-9189, CVE-2016-9190

Description

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

Pillow -- multiple vulnerabilities (bc4898d5-a794-11e6-b2d3-60a44ce6887b)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/bc4898d5-a794-11e6-b2d3-60a44ce6887b.html>

Affected packages:

py27-pillow < 3.3.2

py33-pillow < 3.3.2

py34-pillow < 3.3.2

py35-pillow < 3.3.2

182202 - FreeBSD wget Access List Bypass / Race Condition (479c5b91-b6cc-11e6-a04e-3417eb99b9a0)

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

Risk Level: Medium

CVE: CVE-2016-7098

Description

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

wget -- Access List Bypass / Race Condition (479c5b91-b6cc-11e6-a04e-3417eb99b9a0)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/479c5b91-b6cc-11e6-a04e-3417eb99b9a0.html>

Affected packages:

wget <= 1.17

20934 - (VMSA-2016-0021) VMware vRealize Automation Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-5334

Description

An information disclosure vulnerability is present in some versions of VMware vRealize Automation.

Observation

VMware vRealize Automation integrates with VMware vCloud Suite and automates IT tasks.

An information disclosure vulnerability is present in some versions of VMware vRealize Automation. The flaw lies in an unspecified component. Successful exploitation could allow an attacker to retrieve sensitive data.

20935 - (VMSA-2016-0021) VMware Identity Manager Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-5334

Description

An information disclosure vulnerability is present in some versions of VMware Identity Manager.

Observation

VMware Identity Manager is an Identity as a Service solution for cloud-based mobile software.

An information disclosure vulnerability is present in some versions of VMware Identity Manager. The flaw lies in an unspecified component. Successful exploitation could allow an attacker to retrieve sensitive data.

20940 - IBM AIX pconsole Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-0266

Description

A vulnerability is present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

A vulnerability is present in some versions of IBM AIX. The TLS version in IBM AIX doesn't default to the latest version. Successful exploitation could allow an attacker to obtain sensitive information.

20943 - (SOL48042976) F5 BIG-IP SSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-4545

Description

A denial of service vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

A denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Virtual servers with SSL profile enabled. Successful exploitation could allow an attacker to cause a denial of service condition.

20948 - Mozilla Firefox URL Redirection Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-9078

Description

A security bypass vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A security bypass vulnerability is present in some versions of Mozilla Firefox. The flaw occurs due to data: URL inherit wrong origin after an HTTP redirection. Successful exploitation could allow an attacker to bypass same-origin policy.

20949 - Mozilla Firefox URL Redirection Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-9078

Description

A security bypass vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A security bypass vulnerability is present in some versions of Mozilla Firefox. The flaw occurs due to data: URL inherit wrong origin after an HTTP redirection. Successful exploitation could allow an attacker to bypass same-origin policy.

141377 - Red Hat Enterprise Linux RHSA-2016-2872 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

Description

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

RHSA-2016-2872

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2872.html>

RHEL6S

i386

sudo-debuginfo-1.8.6p3-25.el6_8

sudo-devel-1.8.6p3-25.el6_8

sudo-1.8.6p3-25.el6_8

x86_64

sudo-debuginfo-1.8.6p3-25.el6_8

sudo-devel-1.8.6p3-25.el6_8

sudo-1.8.6p3-25.el6_8

RHEL6WS

x86_64

sudo-debuginfo-1.8.6p3-25.el6_8

sudo-1.8.6p3-25.el6_8

i386

sudo-debuginfo-1.8.6p3-25.el6_8

sudo-1.8.6p3-25.el6_8

RHEL7D

x86_64

sudo-devel-1.8.6p7-21.el7_3

sudo-debuginfo-1.8.6p7-21.el7_3

sudo-1.8.6p7-21.el7_3

RHEL6D

x86_64

sudo-debuginfo-1.8.6p3-25.el6_8

sudo-devel-1.8.6p3-25.el6_8

sudo-1.8.6p3-25.el6_8

i386

sudo-debuginfo-1.8.6p3-25.el6_8

sudo-devel-1.8.6p3-25.el6_8

sudo-1.8.6p3-25.el6_8

RHEL7WS

x86_64

sudo-devel-1.8.6p7-21.el7_3

sudo-debuginfo-1.8.6p7-21.el7_3

sudo-1.8.6p7-21.el7_3

141378 - Red Hat Enterprise Linux RHSA-2016-2871 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
RHSA-2016-2871

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2871.html>

RHEL6_2S

x86_64

bind-debuginfo-9.7.3-8.P3.el6_2.6

bind-devel-9.7.3-8.P3.el6_2.6

bind-sdb-9.7.3-8.P3.el6_2.6

178254 - Gentoo Linux GLSA-201612-13 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1544

Description

The scan detected that the host is missing the following update:
GLSA-201612-13

Observation

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

<https://security.gentoo.org/glsa/201612-13>

Affected packages:

net-libs/nghttp2 < 1.7.1

178256 - Gentoo Linux GLSA-201612-14 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9114

Description

The scan detected that the host is missing the following update:
GLSA-201612-14

Observation

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

<https://security.gentoo.org/glsa/201612-14>

Affected packages:

sys-apps/util-linux < 2.26

178258 - Gentoo Linux GLSA-201612-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

Description

The scan detected that the host is missing the following update:
GLSA-201612-01

Observation

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

<https://security.gentoo.org/glsa/201612-01>

Affected packages:

app-crypt/gnupg < 1.4.21

178261 - Gentoo Linux GLSA-201612-11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

Description

The scan detected that the host is missing the following update:
GLSA-201612-11

Observation

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

<https://security.gentoo.org/glsa/201612-11>

Affected packages:

www-client/chromium < 55.0.2883.75

178264 - Gentoo Linux GLSA-201612-04 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2147, CVE-2016-2148

Description

The scan detected that the host is missing the following update:
GLSA-201612-04

Observation

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

<https://security.gentoo.org/glsa/201612-04>

Affected packages:

sys-apps/busybox < 1.24.2

178265 - Gentoo Linux GLSA-201612-12 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201612-12

Observation

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

<https://security.gentoo.org/glsa/201612-12>

Affected packages:

sys-devel/patch < 2.7.4

182186 - FreeBSD Apache httpd Denial Of Service In HTTP/2 (cb0bf1ec-bb92-11e6-a9a5-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2016-8740

Description

The scan detected that the host is missing the following update:
Apache httpd -- denial of service in HTTP/2 (cb0bf1ec-bb92-11e6-a9a5-b499baebfeaf)

Observation

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

<http://www.vuxml.org/freebsd/cb0bf1ec-bb92-11e6-a9a5-b499baebfeaf.html>

Affected packages:
2.4.17 <= apache24 <= 2.4.23_1
mod_http2-devel < 1.8.3

182190 - FreeBSD p7zip Null Pointer Dereference (48e83187-b6e9-11e6-b6cf-5453ed2e2b49)

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

Risk Level: Medium

CVE: CVE-2016-9296

Description

The scan detected that the host is missing the following update:
p7zip -- Null pointer dereference (48e83187-b6e9-11e6-b6cf-5453ed2e2b49)

Observation

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

<http://www.vuxml.org/freebsd/48e83187-b6e9-11e6-b6cf-5453ed2e2b49.html>

Affected packages:

p7zip < 15.14_2

191423 - Fedora Linux 24 FEDORA-2016-d4573a5c53 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9296

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d4573a5c53

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

p7zip-16.02-2.fc24

191432 - Fedora Linux 23 FEDORA-2016-1ca07cdcde Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9296

Description

The scan detected that the host is missing the following update:
FEDORA-2016-1ca07cdcde

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 23

p7zip-16.02-2.fc23

20932 - IBM Tivoli Storage Manager for Virtual Environments Authentication Bypass Vulnerability (swg21988781)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-2988

Description

An authentication bypass vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments.

Observation

IBM Tivoli Storage Manager for Virtual Environments is a software solution for administrative tasks of storage instances in virtualization environments.

An authentication bypass vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments. The flaw lies in the component known as Data Protection for VMware GUI. Successful exploitation could allow a malicious user without elevated privileges to execute tasks that require Tivoli Storage Manager administrative permissions, such as: backup scheduling and configuration tasks.

182192 - FreeBSD wireshark Multiple Vulnerabilities (7fff2b16-b0ee-11e6-86b8-589cfc054129)

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

Risk Level: Medium

CVE: CVE-2016-9372, CVE-2016-9373, CVE-2016-9374, CVE-2016-9375, CVE-2016-9376

Description

The scan detected that the host is missing the following update:
wireshark -- multiple vulnerabilities (7fff2b16-b0ee-11e6-86b8-589cfc054129)

Observation

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

<http://www.vuxml.org/freebsd/7fff2b16-b0ee-11e6-86b8-589cfc054129.html>

Affected packages:

tshark < 2.2.2

tshark-lite < 2.2.2

wireshark < 2.2.2

wireshark-lite < 2.2.2

wireshark-qt5 < 2.2.2

191426 - Fedora Linux 25 FEDORA-2016-6afdd2b61d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8650

Description

The scan detected that the host is missing the following update:
FEDORA-2016-6afdd2b61d

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

kernel-4.8.11-300.fc25

191438 - Fedora Linux 25 FEDORA-2016-cde4525fab Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7146, CVE-2016-7148, CVE-2016-9119

Description

The scan detected that the host is missing the following update:
FEDORA-2016-cde4525fab

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 25

moin-1.9.9-1.fc25

191439 - Fedora Linux 23 FEDORA-2016-a820774fc2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8650

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a820774fc2

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 23

kernel-4.8.11-100.fc23

191441 - Fedora Linux 24 FEDORA-2016-d40c768095 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7146, CVE-2016-7148

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d40c768095

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 24

moin-1.9.9-1.fc24

191443 - Fedora Linux 23 FEDORA-2016-a77985b7c7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7146, CVE-2016-7148, CVE-2016-9119

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a77985b7c7

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 23

moin-1.9.9-1.fc23

191452 - Fedora Linux 24 FEDORA-2016-b18410c59c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8650

Description

The scan detected that the host is missing the following update:
FEDORA-2016-b18410c59c

Observation

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

Fedora Core 24

kernel-4.8.11-200.fc24

88825 - Slackware Linux 14.1, 14.2 SSA:2016-336-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9079

Description

The scan detected that the host is missing the following update:
SSA:2016-336-01

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.403767>

Slackware 14.1

x86_64

mozilla-firefox-45.5.1esr-x86_64-1

Slackware 14.2

x86_64

mozilla-firefox-45.5.1esr-x86_64-1

i586

mozilla-firefox-45.5.1esr-i586-1

88826 - Slackware Linux 14.1, 14.2 SSA:2016-336-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9079

Description

The scan detected that the host is missing the following update:
SSA:2016-336-02

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.408458>

Slackware 14.1

x86_64

mozilla-thunderbird-45.5.1-x86_64-1

Slackware 14.2

x86_64

mozilla-thunderbird-45.5.1-x86_64-1

i586
mozilla-thunderbird-45.5.1-i586-1

130642 - Debian Linux 8.0 DSA-3728-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-9079

Description

The scan detected that the host is missing the following update:
DSA-3728-1

Observation

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

<http://www.debian.org/security/2016/dsa-3728>

Debian 8.0
all
firefox-esr_45.5.1esr-1~deb8u1

182187 - FreeBSD xen-kernel X86 64-bit Bit Test Instruction Emulation Broken (56f0f11e-ba4d-11e6-ae1b-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-9383

Description

The scan detected that the host is missing the following update:
xen-kernel -- x86 64-bit bit test instruction emulation broken (56f0f11e-ba4d-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/56f0f11e-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:
xen-kernel < 4.7.1

182191 - FreeBSD Mozilla SVG Animation Remote Code Execution (18f39fb6-7400-4063-acaf-0806e92c094f)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-9079

Description

The scan detected that the host is missing the following update:
Mozilla -- SVG Animation Remote Code Execution (18f39fb6-7400-4063-acaf-0806e92c094f)

Observation

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

<http://www.vuxml.org/freebsd/18f39fb6-7400-4063-acaf-0806e92c094f.html>

Affected packages:

firefox < 50.0.2.1
firefox-esr < 45.5.1.1
linux-firefox < 45.5.1.2
libxul < 45.5.1
thunderbird < 45.5.1
linux-thunderbird < 45.5.1

182194 - FreeBSD chromium Multiple Vulnerabilities (603fe0a1-bb26-11e6-8e5a-3065ec8fd3ec)

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

Risk Level: Low

CVE: CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (603fe0a1-bb26-11e6-8e5a-3065ec8fd3ec)

Observation

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

<http://www.vuxml.org/freebsd/603fe0a1-bb26-11e6-8e5a-3065ec8fd3ec.html>

Affected packages:

chromium < 55.0.2883.75
chromium-npapi < 55.0.2883.75
chromium-pulse < 55.0.2883.75

182195 - FreeBSD ImageMagick7 Multiple Vulnerabilities (e1f67063-aab4-11e6-b2d3-60a44ce6887b)

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

Risk Level: Low

CVE: CVE-2016-8862, CVE-2016-8866, CVE-2016-9298

Description

The scan detected that the host is missing the following update:
ImageMagick7 -- multiple vulnerabilities (e1f67063-aab4-11e6-b2d3-60a44ce6887b)

Observation

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

<http://www.vuxml.org/freebsd/e1f67063-aab4-11e6-b2d3-60a44ce6887b.html>

Affected packages:

ImageMagick7 < 7.0.3.6
ImageMagick7-nox11 < 7.0.3.6

182196 - FreeBSD xen-kernel X86 Null Segments Not Always Treated As Unusable (50ac2e96-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-9386

Description

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

xen-kernel -- x86 null segments not always treated as unusable (50ac2e96-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/50ac2e96-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.1

182197 - FreeBSD xen-tools Qemu Incautious About Shared Ring Processing (58685e23-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-9381

Description

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

xen-tools -- qemu incautious about shared ring processing (58685e23-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/58685e23-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-tools < 4.7.1

182198 - FreeBSD xen-kernel X86 Segment Base Write Emulation Lacking Canonical Address Checks (53dbd096-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-9385

Description

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

xen-kernel -- x86 segment base write emulation lacking canonical address checks (53dbd096-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/53dbd096-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

4.4 <= xen-kernel < 4.7.1

182201 - FreeBSD ImageMagick Heap Overflow Vulnerability (19d35b0f-ba73-11e6-b1cf-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-9298

Description

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

ImageMagick -- heap overflow vulnerability (19d35b0f-ba73-11e6-b1cf-14dae9d210b8)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/19d35b0f-ba73-11e6-b1cf-14dae9d210b8.html>

Affected packages:

ImageMagick < 6.9.6.4,1

ImageMagick-nox11 < 6.9.6.4,1

ImageMagick7 < 7.0.3.7

ImageMagick7-nox11 < 7.0.3.7

182203 - FreeBSD xen-kernel X86 Task Switch To VM86 Mode Mis-handled (523bb0b7-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-9382

Description

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

xen-kernel -- x86 task switch to VM86 mode mis-handled (523bb0b7-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/523bb0b7-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.1

182204 - FreeBSD py-cryptography Vulnerable HKDF Key Generation (e5dcb942-ba6f-11e6-b1cf-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-9243

Description

The scan detected that the host is missing the following update:
py-cryptography -- vulnerable HKDF key generation (e5dcb942-ba6f-11e6-b1cf-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/e5dcb942-ba6f-11e6-b1cf-14dae9d210b8.html>

Affected packages:

py27-cryptography < 1.5.3
py33-cryptography < 1.5.3
py34-cryptography < 1.5.3
py35-cryptography < 1.5.3

182205 - FreeBSD xen-kernel Guest 32-bit ELF Symbol Table Load Leaking Host Data (5555120d-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-9384

Description

The scan detected that the host is missing the following update:
xen-kernel -- guest 32-bit ELF symbol table load leaking host data (5555120d-ba4d-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/5555120d-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

4.7 <= xen-kernel < 4.7.1

182206 - FreeBSD xen-kernel CR0.TS And CR0.EM Not Always Honored For X86 HVM Guests (4d7cf654-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-7777

Description

The scan detected that the host is missing the following update:
xen-kernel -- CR0.TS and CR0.EM not always honored for x86 HVM guests (4d7cf654-ba4d-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/4d7cf654-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.1

182207 - FreeBSD xen-tools Delimiter Injection Vulnerabilities In Pygrub (59f79c99-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-9379, CVE-2016-9380

Description

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

xen-tools -- delimiter injection vulnerabilities in pygrub (59f79c99-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/59f79c99-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-tools < 4.7.1

185496 - Ubuntu Linux 14.04 USN-3149-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

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

USN-3149-1

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-December/003656.html>

Ubuntu 14.04

linux-image-powerpc-e500_3.13.0.105.113
linux-image-3.13.0-105-lowlatency_3.13.0-105.152
linux-image-powerpc-smp_3.13.0.105.113
linux-image-3.13.0-105-powerpc-e500_3.13.0-105.152
linux-image-generic-lpae_3.13.0.105.113
linux-image-powerpc64-smp_3.13.0.105.113
linux-image-powerpc64-emb_3.13.0.105.113
linux-image-lowlatency_3.13.0.105.113
linux-image-3.13.0-105-powerpc64-smp_3.13.0-105.152
linux-image-3.13.0-105-powerpc-smp_3.13.0-105.152
linux-image-3.13.0-105-generic_3.13.0-105.152
linux-image-3.13.0-105-generic-lpae_3.13.0-105.152
linux-image-3.13.0-105-powerpc64-emb_3.13.0-105.152
linux-image-generic_3.13.0.105.113
linux-image-powerpc-e500mc_3.13.0.105.113
linux-image-3.13.0-105-powerpc-e500mc_3.13.0-105.152

185498 - Ubuntu Linux 12.04 USN-3149-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

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

USN-3149-2

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-December/003657.html>

Ubuntu 12.04

linux-image-3.13.0-105-generic-lpae_3.13.0-105.152~precise1

linux-image-generic-lpae-lts-trusty_3.13.0.105.96

linux-image-generic-lts-trusty_3.13.0.105.96

linux-image-3.13.0-105-generic_3.13.0-105.152~precise1

185500 - Ubuntu Linux 16.04 USN-3151-4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

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

USN-3151-4

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-December/003663.html>

Ubuntu 16.04

linux-image-raspi2_4.4.0.1034.33

linux-image-4.4.0-1034-raspi2_4.4.0-1034.41

185502 - Ubuntu Linux 12.04 USN-3150-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

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

USN-3150-2

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-December/003664.html>

Ubuntu 12.04

linux-image-3.2.0-1496-omap4_3.2.0-1496.123

linux-image-omap4_3.2.0.1496.91

185503 - Ubuntu Linux 16.10 USN-3152-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

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

USN-3152-2

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-December/003665.html>

Ubuntu 16.10

linux-image-raspi2_4.8.0.1020.23

linux-image-4.8.0-1020-raspi2_4.8.0-1020.23

185504 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3133-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5198, CVE-2016-5199, CVE-2016-5200, CVE-2016-5202

Description

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

USN-3133-1

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-December/003654.html>

Ubuntu 16.04

liboxideqtcore0_1.18.5-0ubuntu0.16.04.1

Ubuntu 14.04

liboxideqtcore0_1.18.5-0ubuntu0.14.04.1

Ubuntu 16.10

185505 - Ubuntu Linux 16.04 USN-3151-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

The scan detected that the host is missing the following update:
USN-3151-1

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-December/003659.html>

Ubuntu 16.04

linux-image-powerpc64-emb_4.4.0.53.56
linux-image-4.4.0-53-powerpc64-emb_4.4.0-53.74
linux-image-4.4.0-53-powerpc-e500mc_4.4.0-53.74
linux-image-4.4.0-53-lowlatency_4.4.0-53.74
linux-image-generic_4.4.0.53.56
linux-image-powerpc64-smp_4.4.0.53.56
linux-image-4.4.0-53-powerpc64-smp_4.4.0-53.74
linux-image-powerpc-smp_4.4.0.53.56
linux-image-4.4.0-53-powerpc-smp_4.4.0-53.74
linux-image-4.4.0-53-generic_4.4.0-53.74
linux-image-4.4.0-53-generic-lpae_4.4.0-53.74
linux-image-generic-lpae_4.4.0.53.56
linux-image-lowlatency_4.4.0.53.56
linux-image-powerpc-e500mc_4.4.0.53.56

185506 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3141-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5290, CVE-2016-5291, CVE-2016-5296, CVE-2016-5297, CVE-2016-9066, CVE-2016-9079

Description

The scan detected that the host is missing the following update:
USN-3141-1

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-December/003653.html>

Ubuntu 12.04

thunderbird_45.5.1+build1-0ubuntu0.12.04.1

Ubuntu 16.04

thunderbird_45.5.1+build1-0ubuntu0.16.04.1

Ubuntu 14.04

thunderbird_45.5.1+build1-0ubuntu0.14.04.1

Ubuntu 16.10

thunderbird_45.5.1+build1-0ubuntu0.16.10.1

185509 - Ubuntu Linux 16.10 USN-3152-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

The scan detected that the host is missing the following update:
USN-3152-1

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-December/003661.html>

Ubuntu 16.10

linux-image-powerpc-smp_4.8.0.30.39
linux-image-4.8.0-30-powerpc-smp_4.8.0-30.32
linux-image-powerpc64-emb_4.8.0.30.39
linux-image-generic_4.8.0.30.39
linux-image-4.8.0-30-generic-lpae_4.8.0-30.32
linux-image-powerpc-e500mc_4.8.0.30.39
linux-image-4.8.0-30-generic_4.8.0-30.32
linux-image-4.8.0-30-powerpc64-emb_4.8.0-30.32
linux-image-4.8.0-30-lowlatency_4.8.0-30.32
linux-image-4.8.0-30-powerpc-e500mc_4.8.0-30.32
linux-image-generic-lpae_4.8.0.30.39
linux-image-lowlatency_4.8.0.30.39

185510 - Ubuntu Linux 14.04 USN-3151-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

The scan detected that the host is missing the following update:
USN-3151-2

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-December/003660.html>

Ubuntu 14.04

linux-image-4.4.0-53-generic-lpae_4.4.0-53.74~14.04.1
linux-image-generic-lpae-lts-xenial_4.4.0.53.40
linux-image-powerpc64-smp-lts-xenial_4.4.0.53.40
linux-image-generic-lts-xenial_4.4.0.53.40
linux-image-powerpc-e500mc-lts-xenial_4.4.0.53.40
linux-image-4.4.0-53-powerpc64-smp_4.4.0-53.74~14.04.1
linux-image-4.4.0-53-generic_4.4.0-53.74~14.04.1
linux-image-powerpc64-emb-lts-xenial_4.4.0.53.40
linux-image-4.4.0-53-lowlatency_4.4.0-53.74~14.04.1
linux-image-4.4.0-53-powerpc-smp_4.4.0-53.74~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.53.40
linux-image-powerpc-smp-lts-xenial_4.4.0.53.40
linux-image-4.4.0-53-powerpc64-emb_4.4.0-53.74~14.04.1
linux-image-4.4.0-53-powerpc-e500mc_4.4.0-53.74~14.04.1

185511 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3142-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7799, CVE-2016-7906, CVE-2016-8677, CVE-2016-8862, CVE-2016-9556

Description

The scan detected that the host is missing the following update:
USN-3142-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003642.html>

Ubuntu 12.04

libmagickcore4_6.6.9.7-5ubuntu3.6
libmagickcore4-extra_6.6.9.7-5ubuntu3.6
imagemagick_6.6.9.7-5ubuntu3.6

Ubuntu 16.04

imagemagick-6.q16_6.8.9.9-7ubuntu5.3
libmagickcore-6.q16-2_6.8.9.9-7ubuntu5.3
libmagickcore-6.q16-2-extra_6.8.9.9-7ubuntu5.3
imagemagick_6.8.9.9-7ubuntu5.3

Ubuntu 14.04

imagemagick_6.7.7.10-6ubuntu3.3
libmagickcore5-extra_6.7.7.10-6ubuntu3.3
libmagickcore5_6.7.7.10-6ubuntu3.3

Ubuntu 16.10

libmagickcore-6.q16-2-extra_6.8.9.9-7ubuntu8.2
imagemagick_6.8.9.9-7ubuntu8.2

libmagickcore-6.q16-2_6.8.9.9-7ubuntu8.2
imagemagick-6.q16_6.8.9.9-7ubuntu8.2

185514 - Ubuntu Linux 12.04 USN-3150-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

The scan detected that the host is missing the following update:
USN-3150-1

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-December/003658.html>

Ubuntu 12.04

linux-image-3.2.0-118-generic-pae_3.2.0-118.161
linux-image-3.2.0-118-generic_3.2.0-118.161
linux-image-3.2.0-118-highbank_3.2.0-118.161
linux-image-powerpc-smp_3.2.0.118.133
linux-image-generic-pae_3.2.0.118.133
linux-image-3.2.0-118-powerpc64-smp_3.2.0-118.161
linux-image-3.2.0-118-virtual_3.2.0-118.161
linux-image-3.2.0-118-powerpc-smp_3.2.0-118.161
linux-image-3.2.0-118-omap_3.2.0-118.161
linux-image-highbank_3.2.0.118.133
linux-image-powerpc64-smp_3.2.0.118.133
linux-image-virtual_3.2.0.118.133
linux-image-generic_3.2.0.118.133
linux-image-omap_3.2.0.118.133

185515 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3140-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9078, CVE-2016-9079

Description

The scan detected that the host is missing the following update:
USN-3140-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003652.html>

Ubuntu 12.04

firefox_50.0.2+build1-0ubuntu0.12.04.1

Ubuntu 16.04

firefox_50.0.2+build1-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_50.0.2+build1-0ubuntu0.14.04.1

Ubuntu 16.10

firefox_50.0.2+build1-0ubuntu0.16.10.1

185516 - Ubuntu Linux 16.04 USN-3151-3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8655

Description

The scan detected that the host is missing the following update:
USN-3151-3

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-December/003662.html>

Ubuntu 16.04

linux-image-4.4.0-1039-snapdragon_4.4.0-1039.43

linux-image-snapdragon_4.4.0.1039.31

191424 - Fedora Linux 23 FEDORA-2016-d2cbcd602d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d2cbcd602d

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 23

firefox-50.0.2-1.fc23

191425 - Fedora Linux 25 FEDORA-2016-561a937494 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2016-561a937494

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 25

calamares-2.4.4-5.fc25

191427 - Fedora Linux 24 FEDORA-2016-5c7e9b8778 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2016-5c7e9b8778

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 24

calamares-2.4.4-5.fc24

191428 - Fedora Linux 25 FEDORA-2016-a82e35272c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9445

Description

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

FEDORA-2016-a82e35272c

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

gstreamer1-plugins-bad-free-1.10.1-1.fc25

191429 - Fedora Linux 24 FEDORA-2016-dbbd3d43fe Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-dbbd3d43fe

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 24

drupal8-8.2.3-1.fc24

191430 - Fedora Linux 25 FEDORA-2016-999e1a6927 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9377, CVE-2016-9378, CVE-2016-9379, CVE-2016-9380, CVE-2016-9381, CVE-2016-9382, CVE-2016-9383, CVE-2016-9384, CVE-2016-9385, CVE-2016-9386

Description

The scan detected that the host is missing the following update:
FEDORA-2016-999e1a6927

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

xen-4.7.1-3.fc25

191433 - Fedora Linux 24 FEDORA-2016-fde083842e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-fde083842e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

thunderbird-45.5.1-1.fc24

191434 - Fedora Linux 24 FEDORA-2016-5748592807 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-5748592807

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

firefox-50.0.2-1.fc24

191435 - Fedora Linux 25 FEDORA-2016-c883d07fba Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2016-c883d07fba

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

gstreamer1-plugins-good-1.10.1-2.fc25

191436 - Fedora Linux 24 FEDORA-2016-95c104a4c6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9377, CVE-2016-9378, CVE-2016-9379, CVE-2016-9380, CVE-2016-9381, CVE-2016-9382, CVE-2016-9383, CVE-2016-9385, CVE-2016-9386

Description

The scan detected that the host is missing the following update:
FEDORA-2016-95c104a4c6

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

xen-4.6.4-2.fc24

191437 - Fedora Linux 25 FEDORA-2016-411f8b961e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-411f8b961e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 25

drupal8-8.2.3-1.fc25

191440 - Fedora Linux 25 FEDORA-2016-0bfa836087 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-0bfa836087

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

thunderbird-45.5.1-1.fc25

191442 - Fedora Linux 25 FEDORA-2016-6576a8536b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4412

Description

The scan detected that the host is missing the following update:
FEDORA-2016-6576a8536b

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

phpMyAdmin-4.6.5.1-2.fc25

191444 - Fedora Linux 24 FEDORA-2016-c4004fe99e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9445

Description

The scan detected that the host is missing the following update:
FEDORA-2016-c4004fe99e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 24

gststreamer1-plugins-bad-free-1.8.3-2.fc24

191445 - Fedora Linux 25 FEDORA-2016-2967f5f965 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2016-2967f5f965

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

firefox-50.0.2-1.fc25

191447 - Fedora Linux 25 FEDORA-2016-fdedfc86d0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9447

Description

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

FEDORA-2016-fdedfc86d0

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

gststreamer-plugins-bad-free-0.10.23-34.fc25

191448 - Fedora Linux 24 FEDORA-2016-3a45d79132 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9808

Description

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

FEDORA-2016-3a45d79132

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 24

gststreamer1-plugins-good-1.8.3-2.fc24

191450 - Fedora Linux 23 FEDORA-2016-68b71978a1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9377, CVE-2016-9378, CVE-2016-9379, CVE-2016-9380, CVE-2016-9381, CVE-2016-9382, CVE-2016-9383, CVE-2016-9385, CVE-2016-9386

Description

The scan detected that the host is missing the following update:
FEDORA-2016-68b71978a1

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 23

xen-4.5.5-4.fc23

191451 - Fedora Linux 25 FEDORA-2016-368780879d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9299

Description

The scan detected that the host is missing the following update:
FEDORA-2016-368780879d

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=3>

Fedora Core 25

jenkins-1.651.3-2.fc25

jenkins-remoting-2.62.3-1.fc25

178260 - Gentoo Linux GLSA-201612-10 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5313

Description

The scan detected that the host is missing the following update:
GLSA-201612-10

Observation

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

<https://security.gentoo.org/glsa/201612-10>

Affected packages:

app-emulation/libvirt < 1.2.21-r1

182188 - FreeBSD xen-kernel X86 HVM: Overflow Of Sh_ctxt->seg_reg[] (4aae54be-ba4d-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-7094

Description

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

xen-kernel -- x86 HVM: Overflow of sh_ctxt->seg_reg[] (4aae54be-ba4d-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/4aae54be-ba4d-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.1

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.

20471 - (SOL20225390) F5 BIG-IP Multiple PCRE Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-2327, CVE-2015-2328, CVE-2015-3217, CVE-2015-8380, CVE-2015-8381, CVE-2015-8382, CVE-2015-8383, CVE-2015-8384, CVE-2015-8385, CVE-2015-8386, CVE-2015-8387, CVE-2015-8388, CVE-2015-8389, CVE-2015-8390, CVE-2015-8391, CVE-2015-8392, CVE-2015-8394, CVE-2015-8395

Update Details

FASLScript is updated

19827 - (SOL62012529) F5 BIG-IP BIND Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-1286

Update Details

FASLScript is updated

20859 - (SOL01276005) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-2182

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

20443 - (SOL30971148) F5 BIG-IP Apache Tomcat Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-5174, CVE-2015-5345, CVE-2016-0706, CVE-2016-0714

Update Details

FASLScript is updated

182007 - FreeBSD expat2 Denial Of Service (ff76f0e0-3f11-11e6-b3c8-14dae9d210b8)

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

Risk Level: Medium

CVE: CVE-2016-4472

Update Details

FASLScript is updated

20587 - (SOL05428062) F5 BIG-IP Pcregrep In PCRE Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8393

Update Details

Observation is updated FASLScript is updated

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

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

Risk Level: Medium

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

Update Details

CVE is updated

163204 - Oracle Enterprise Linux ELSA-2016-2583 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5211, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-

2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7974, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8158, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

Update Details

CVE is updated

19875 - (SOL71245322) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8138

Update Details

FASLScript is updated

182098 - FreeBSD gnupg Attacker Who Obtains 4640 Bits From The RNG Can Trivially Predict The Next 160 Bits Of Output (e1c71d8d-64d9-11e6-

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

Risk Level: Low

CVE: CVE-2016-6313

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.

MCAFFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.