

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

91985 - Oracle Enterprise Linux ELSA-2015-2657 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

Description

The scan detected that the host is missing the following update:
ELSA-2015-2657

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-December/005650.html>

<http://oss.oracle.com/pipermail/el-errata/2015-December/005651.html>

<http://oss.oracle.com/pipermail/el-errata/2015-December/005647.html>

OEL6

x86_64

firefox-38.5.0-2.0.1.el6_7

i386

firefox-38.5.0-2.0.1.el6_7

OEL5

x86_64

firefox-38.5.0-2.0.1.el5_11

i386

firefox-38.5.0-2.0.1.el5_11

OEL7

x86_64

firefox-38.5.0-3.0.1.el7_2

130347 - Debian Linux 7.0, 8.0 DSA-3422-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

Description

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

DSA-3422-1

Observation

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

<http://www.debian.org/security/2015/dsa-3422>

Debian 8.0
all
iceweasel_38.5.0esr-1~deb8u2

Debian 7.0
all
iceweasel_38.5.0esr-1~deb7u2

141042 - Red Hat Enterprise Linux RHSA-2015-2657 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

Description

The scan detected that the host is missing the following update:
RHSA-2015-2657

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2657.html>

RHEL5S
i386
firefox-38.5.0-2.el5_11
firefox-debuginfo-38.5.0-2.el5_11

x86_64
firefox-38.5.0-2.el5_11
firefox-debuginfo-38.5.0-2.el5_11

RHEL7S
x86_64
firefox-debuginfo-38.5.0-3.el7_2
firefox-38.5.0-3.el7_2

RHEL6S
i386
firefox-debuginfo-38.5.0-2.el6_7
firefox-38.5.0-2.el6_7

x86_64
firefox-debuginfo-38.5.0-2.el6_7
firefox-38.5.0-2.el6_7

RHEL6WS
x86_64

firefox-debuginfo-38.5.0-2.el6_7
firefox-38.5.0-2.el6_7

i386
firefox-debuginfo-38.5.0-2.el6_7
firefox-38.5.0-2.el6_7

RHEL5D
x86_64
firefox-38.5.0-2.el5_11
firefox-debuginfo-38.5.0-2.el5_11

i386
firefox-38.5.0-2.el5_11
firefox-debuginfo-38.5.0-2.el5_11

RHEL7D
x86_64
firefox-debuginfo-38.5.0-3.el7_2
firefox-38.5.0-3.el7_2

RHEL6D
x86_64
firefox-debuginfo-38.5.0-2.el6_7
firefox-38.5.0-2.el6_7

i386
firefox-debuginfo-38.5.0-2.el6_7
firefox-38.5.0-2.el6_7

RHEL7WS
x86_64
firefox-debuginfo-38.5.0-3.el7_2
firefox-38.5.0-3.el7_2

144094 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2335-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7202, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2335-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2015-December/001749.html>

SuSE SLED 12
x86_64
MozillaFirefox-translations-38.5.0esr-54.1
MozillaFirefox-debugsource-38.5.0esr-54.1
MozillaFirefox-38.5.0esr-54.1
MozillaFirefox-debuginfo-38.5.0esr-54.1

SuSE SLES 12
x86_64
MozillaFirefox-translations-38.5.0esr-54.1
MozillaFirefox-debugsource-38.5.0esr-54.1
MozillaFirefox-38.5.0esr-54.1
MozillaFirefox-debuginfo-38.5.0esr-54.1

144104 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2290-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6764, CVE-2015-6765, CVE-2015-6766, CVE-2015-6767, CVE-2015-6768, CVE-2015-6769, CVE-2015-6770, CVE-2015-6771, CVE-2015-6772, CVE-2015-6773, CVE-2015-6774, CVE-2015-6775, CVE-2015-6776, CVE-2015-6777, CVE-2015-6778, CVE-2015-6779, CVE-2015-6780, CVE-2015-6781, CVE-2015-6782, CVE-2015-6783, CVE-2015-6784, CVE-2015-6785, CVE-2015-6786, CVE-2015-6787, CVE-2015-6788, CVE-2015-6789, CVE-2015-6790, CVE-2015-6791

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2290-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00072.html>

SuSE Linux 13.1

x86_64
chromium-ffmpegsumo-47.0.2526.80-116.1
chromedriver-47.0.2526.80-116.1
chromium-desktop-gnome-47.0.2526.80-116.1
chromium-47.0.2526.80-116.1
chromium-desktop-kde-47.0.2526.80-116.1
chromedriver-debuginfo-47.0.2526.80-116.1
chromium-ffmpegsumo-debuginfo-47.0.2526.80-116.1
chromium-debugsource-47.0.2526.80-116.1
chromium-debuginfo-47.0.2526.80-116.1

i586

chromium-ffmpegsumo-47.0.2526.80-116.1
chromedriver-47.0.2526.80-116.1
chromium-desktop-gnome-47.0.2526.80-116.1
chromium-47.0.2526.80-116.1
chromium-desktop-kde-47.0.2526.80-116.1
chromedriver-debuginfo-47.0.2526.80-116.1
chromium-ffmpegsumo-debuginfo-47.0.2526.80-116.1
chromium-debugsource-47.0.2526.80-116.1
chromium-debuginfo-47.0.2526.80-116.1

SuSE Linux 13.2

x86_64
chromedriver-debuginfo-47.0.2526.80-61.1
chromium-ffmpegsumo-47.0.2526.80-61.1
chromedriver-47.0.2526.80-61.1
chromium-desktop-gnome-47.0.2526.80-61.1
chromium-47.0.2526.80-61.1
chromium-ffmpegsumo-debuginfo-47.0.2526.80-61.1
chromium-debugsource-47.0.2526.80-61.1

chromium-desktop-kde-47.0.2526.80-61.1
chromium-debuginfo-47.0.2526.80-61.1

i586

chromedriver-debuginfo-47.0.2526.80-61.1
chromium-ffmpegsumo-47.0.2526.80-61.1
chromedriver-47.0.2526.80-61.1
chromium-desktop-gnome-47.0.2526.80-61.1
chromium-47.0.2526.80-61.1
chromium-ffmpegsumo-debuginfo-47.0.2526.80-61.1
chromium-debugsource-47.0.2526.80-61.1
chromium-desktop-kde-47.0.2526.80-61.1
chromium-debuginfo-47.0.2526.80-61.1

160015 - CentOS 5, 6, 7 CESA-2015-2657 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

Description

The scan detected that the host is missing the following update:
CESA-2015-2657

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2015-December/021547.html>
<http://lists.centos.org/pipermail/centos-announce/2015-December/021552.html>
<http://lists.centos.org/pipermail/centos-announce/2015-December/021553.html>

CentOS 6
x86_64
firefox-38.5.0-2.el6.centos

i686
firefox-38.5.0-2.el6.centos

CentOS 7
x86_64
firefox-38.5.0-3.el7.centos

i686
firefox-38.5.0-3.el7.centos

CentOS 5
x86_64
firefox-38.5.0-2.el5.centos

i386
firefox-38.5.0-2.el5.centos

174853 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x i386/x86_64 (1512-3046)

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x i386/x86_64 (1512-3046)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=3046>

SL6
x86_64
firefox-debuginfo-38.5.0-2.el6_7
firefox-38.5.0-2.el6_7

i386
firefox-debuginfo-38.5.0-2.el6_7
firefox-38.5.0-2.el6_7

SL5
x86_64
firefox-38.5.0-2.el5_11
firefox-debuginfo-38.5.0-2.el5_11

i386
firefox-38.5.0-2.el5_11
firefox-debuginfo-38.5.0-2.el5_11

19454 - McAfee Enterprise Security Manager AD LDAP Security Bypass

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-8024

Description

A vulnerability in some versions of McAfee Enterprise Security Manager could lead to a security bypass.

Observation

A vulnerability in some versions of McAfee Enterprise Security Manager could lead to a security bypass.

The flaw lies in the handling of a specially crafted username. Successful exploitation could allow a remote attacker to bypass intended access restrictions.

19458 - (HT205653) Apple OS X Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2011-2895, CVE-2015-3807, CVE-2015-7053, CVE-2015-7058, CVE-2015-7059, CVE-2015-7060, CVE-2015-7061, CVE-2015-7064, CVE-2015-7065, CVE-2015-7066, CVE-2015-7074, CVE-2015-7075, CVE-2015-7105, CVE-2015-7107, CVE-2015-7115, CVE-2015-7116

Description

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

Observation

Apple OS X is an operating system used in Apple Mac computer.

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

19460 - (JSA10712) Juniper ScreenOS Input Validation Remote Code Execution

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-7754

Description

A vulnerability in some versions of Juniper ScreenOS could lead to remote code execution.

Observation

A vulnerability in some versions of Juniper ScreenOS could lead to remote code execution.

The flaw lies in an input validation defect. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

190114 - Fedora Linux 23 FEDORA-2015-71b291686c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7805, CVE-2015-8075

Description

The scan detected that the host is missing the following update:
FEDORA-2015-71b291686c

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174213.html>

Fedora Core 23

libsndfile-1.0.25-18.fc23

144096 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2302-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2698

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2302-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2015-December/001738.html>

SuSE SLED 12

x86_64
krb5-32bit-1.12.1-22.5
krb5-client-1.12.1-22.5
krb5-debugsource-1.12.1-22.5
krb5-1.12.1-22.5
krb5-debuginfo-1.12.1-22.5
krb5-debuginfo-32bit-1.12.1-22.5
krb5-client-debuginfo-1.12.1-22.5

SuSE SLES 12

x86_64
krb5-client-debuginfo-1.12.1-22.5
krb5-doc-1.12.1-22.5
krb5-plugin-preauth-pkinit-1.12.1-22.5
krb5-1.12.1-22.5
krb5-server-1.12.1-22.5
krb5-server-debuginfo-1.12.1-22.5
krb5-plugin-preauth-otp-debuginfo-1.12.1-22.5
krb5-debugsource-1.12.1-22.5
krb5-32bit-1.12.1-22.5
krb5-plugin-preauth-pkinit-debuginfo-1.12.1-22.5
krb5-debuginfo-1.12.1-22.5
krb5-debuginfo-32bit-1.12.1-22.5
krb5-plugin-preauth-otp-1.12.1-22.5
krb5-client-1.12.1-22.5
krb5-plugin-kdb-ldap-debuginfo-1.12.1-22.5
krb5-plugin-kdb-ldap-1.12.1-22.5

144098 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2300-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1804

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2300-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00074.html>

SuSE Linux 13.1

x86_64
libXfont1-debuginfo-1.4.6-2.15.1
libXfont-devel-1.4.6-2.15.1
libXfont-debugsource-1.4.6-2.15.1
libXfont1-1.4.6-2.15.1
libXfont-devel-32bit-1.4.6-2.15.1
libXfont1-32bit-1.4.6-2.15.1

libXfont1-debuginfo-32bit-1.4.6-2.15.1

i586

libXfont1-debuginfo-1.4.6-2.15.1

libXfont-devel-1.4.6-2.15.1

libXfont1-1.4.6-2.15.1

libXfont-debugsource-1.4.6-2.15.1

SuSE Linux 13.2

x86_64

libXfont1-1.5.0-2.7.1

libXfont-debugsource-1.5.0-2.7.1

libXfont-devel-1.5.0-2.7.1

libXfont1-32bit-1.5.0-2.7.1

libXfont1-debuginfo-1.5.0-2.7.1

libXfont1-debuginfo-32bit-1.5.0-2.7.1

libXfont-devel-32bit-1.5.0-2.7.1

i586

libXfont-debugsource-1.5.0-2.7.1

libXfont1-1.5.0-2.7.1

libXfont1-debuginfo-1.5.0-2.7.1

libXfont-devel-1.5.0-2.7.1

174850 - Scientific Linux Security ERRATA Moderate: openssh on SL7.x x86_64 (1512-13856)

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

Risk Level: High

CVE: CVE-2015-5600, CVE-2015-6563, CVE-2015-6564

Description

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

Security ERRATA Moderate: openssh on SL7.x x86_64 (1512-13856)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=13856>

SL7

x86_64

openssh-server-sysvinit-6.6.1p1-22.el7

openssh-keycat-6.6.1p1-22.el7

openssh-askpass-6.6.1p1-22.el7

openssh-debuginfo-6.6.1p1-22.el7

openssh-server-6.6.1p1-22.el7

pam_ssh_agent_auth-0.9.3-9.22.el7

openssh-clients-6.6.1p1-22.el7

openssh-6.6.1p1-22.el7

openssh-ldap-6.6.1p1-22.el7

178137 - Gentoo Linux GLSA-201512-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5352, CVE-2015-5600, CVE-2015-6563, CVE-2015-6564, CVE-2015-6565

Description

The scan detected that the host is missing the following update:
GLSA-201512-04

Observation

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

<https://security.gentoo.org/glsa/201512-04>

Affected packages:

net-misc/openssh < 7.1_p1-r2

19457 - (HT205636) Apple iTunes Multiple Vulnerabilities Prior To 12.3.2

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

Risk Level: High

CVE: CVE-2015-7048, CVE-2015-7050, CVE-2015-7095, CVE-2015-7096, CVE-2015-7097, CVE-2015-7098, CVE-2015-7099, CVE-2015-7100, CVE-2015-7101, CVE-2015-7102, CVE-2015-7103, CVE-2015-7104

Description

Multiple vulnerabilities are present in some versions of Apple iTunes.

Observation

Apple iTunes is a media management software.

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

91984 - Oracle Enterprise Linux ELSA-2015-2656 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000

Description

The scan detected that the host is missing the following update:
ELSA-2015-2656

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-December/005653.html>

OEL5

x86_64

bind-chroot-9.3.6-25.P1.el5_11.5

bind-9.3.6-25.P1.el5_11.5

bind-utils-9.3.6-25.P1.el5_11.5

bind-sdb-9.3.6-25.P1.el5_11.5

bind-devel-9.3.6-25.P1.el5_11.5

bind-libbind-devel-9.3.6-25.P1.el5_11.5

caching-nameserver-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5

i386

bind-chroot-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-sdb-9.3.6-25.P1.el5_11.5
bind-devel-9.3.6-25.P1.el5_11.5
bind-libbind-devel-9.3.6-25.P1.el5_11.5
caching-nameserver-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5

91986 - Oracle Enterprise Linux ELSA-2015-2671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

Description

The scan detected that the host is missing the following update:
ELSA-2015-2671

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-December/005654.html>

OEL5

i386
jakarta-commons-collections-tomcat5-3.2-2jpp.4
jakarta-commons-collections-3.2-2jpp.4
jakarta-commons-collections-testframework-javadoc-3.2-2jpp.4
jakarta-commons-collections-testframework-3.2-2jpp.4
jakarta-commons-collections-javadoc-3.2-2jpp.4

x86_64

jakarta-commons-collections-tomcat5-3.2-2jpp.4
jakarta-commons-collections-3.2-2jpp.4
jakarta-commons-collections-testframework-javadoc-3.2-2jpp.4
jakarta-commons-collections-testframework-3.2-2jpp.4
jakarta-commons-collections-javadoc-3.2-2jpp.4

91987 - Oracle Enterprise Linux ELSA-2015-2694 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7504, CVE-2015-7512

Description

The scan detected that the host is missing the following update:
ELSA-2015-2694

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2015-December/005655.html>

OEL6

x86_64

qemu-img-0.12.1.2-2.479.el6_7.3

qemu-kvm-tools-0.12.1.2-2.479.el6_7.3

qemu-guest-agent-0.12.1.2-2.479.el6_7.3

qemu-kvm-0.12.1.2-2.479.el6_7.3

i386

qemu-guest-agent-0.12.1.2-2.479.el6_7.3

91989 - Oracle Enterprise Linux ELSA-2015-2658 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000

Description

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

ELSA-2015-2658

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2015-December/005652.html>

OEL5

x86_64

bind97-9.7.0-21.P2.el5_11.4

bind97-devel-9.7.0-21.P2.el5_11.4

bind97-chroot-9.7.0-21.P2.el5_11.4

bind97-libs-9.7.0-21.P2.el5_11.4

bind97-utils-9.7.0-21.P2.el5_11.4

i386

bind97-9.7.0-21.P2.el5_11.4

bind97-devel-9.7.0-21.P2.el5_11.4

bind97-chroot-9.7.0-21.P2.el5_11.4

bind97-libs-9.7.0-21.P2.el5_11.4

bind97-utils-9.7.0-21.P2.el5_11.4

130339 - Debian Linux 7.0, 8.0 DSA-3429-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8327, CVE-2015-8560

Description

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

DSA-3429-1

Observation

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

<http://www.debian.org/security/2015/dsa-3429>

Debian 8.0
all
foomatic-filters_4.0.17-5+deb8u1

Debian 7.0
all
foomatic-filters_4.0.17-1+deb7u1

130345 - Debian Linux 7.0, 8.0 DSA-3423-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8369

Description

The scan detected that the host is missing the following update:
DSA-3423-1

Observation

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

<http://www.debian.org/security/2015/dsa-3423>

Debian 8.0
all
cacti_0.8.8b+dfsg-8+deb8u3

Debian 7.0
all
cacti_0.8.8a+dfsg-5+deb7u7

141044 - Red Hat Enterprise Linux RHSA-2015-2665 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6792

Description

The scan detected that the host is missing the following update:
RHSA-2015-2665

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2665.html>

RHEL6D
x86_64
chromium-browser-debuginfo-47.0.2526.106-1.el6

chromium-browser-47.0.2526.106-1.el6

i386

chromium-browser-debuginfo-47.0.2526.106-1.el6

chromium-browser-47.0.2526.106-1.el6

RHEL6S

x86_64

chromium-browser-debuginfo-47.0.2526.106-1.el6

chromium-browser-47.0.2526.106-1.el6

i386

chromium-browser-debuginfo-47.0.2526.106-1.el6

chromium-browser-47.0.2526.106-1.el6

RHEL6WS

x86_64

chromium-browser-debuginfo-47.0.2526.106-1.el6

chromium-browser-47.0.2526.106-1.el6

i386

chromium-browser-debuginfo-47.0.2526.106-1.el6

chromium-browser-47.0.2526.106-1.el6

141045 - Red Hat Enterprise Linux RHSA-2015-2694 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7504, CVE-2015-7512

Description

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

RHSA-2015-2694

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2015-2694.html>

RHEL6D

x86_64

qemu-img-0.12.1.2-2.479.el6_7.3

qemu-kvm-tools-0.12.1.2-2.479.el6_7.3

qemu-guest-agent-0.12.1.2-2.479.el6_7.3

qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.3

qemu-kvm-0.12.1.2-2.479.el6_7.3

i386

qemu-guest-agent-0.12.1.2-2.479.el6_7.3

qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.3

RHEL6S

i386

qemu-guest-agent-0.12.1.2-2.479.el6_7.3

qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.3

x86_64

qemu-img-0.12.1.2-2.479.el6_7.3
qemu-kvm-tools-0.12.1.2-2.479.el6_7.3
qemu-guest-agent-0.12.1.2-2.479.el6_7.3
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.3
qemu-kvm-0.12.1.2-2.479.el6_7.3

RHEL6WS

x86_64
qemu-img-0.12.1.2-2.479.el6_7.3
qemu-kvm-tools-0.12.1.2-2.479.el6_7.3
qemu-guest-agent-0.12.1.2-2.479.el6_7.3
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.3
qemu-kvm-0.12.1.2-2.479.el6_7.3

i386

qemu-guest-agent-0.12.1.2-2.479.el6_7.3
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.3

141046 - Red Hat Enterprise Linux RHSA-2015-2671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

Description

The scan detected that the host is missing the following update:
RHSA-2015-2671

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2671.html>

RHEL5D

x86_64
jakarta-commons-collections-debuginfo-3.2-2jpp.4
jakarta-commons-collections-tomcat5-3.2-2jpp.4

i386

jakarta-commons-collections-debuginfo-3.2-2jpp.4
jakarta-commons-collections-tomcat5-3.2-2jpp.4

RHEL5S

i386
jakarta-commons-collections-javadoc-3.2-2jpp.4
jakarta-commons-collections-3.2-2jpp.4
jakarta-commons-collections-testframework-3.2-2jpp.4
jakarta-commons-collections-testframework-javadoc-3.2-2jpp.4
jakarta-commons-collections-debuginfo-3.2-2jpp.4
jakarta-commons-collections-tomcat5-3.2-2jpp.4

x86_64

jakarta-commons-collections-javadoc-3.2-2jpp.4
jakarta-commons-collections-3.2-2jpp.4
jakarta-commons-collections-testframework-3.2-2jpp.4
jakarta-commons-collections-testframework-javadoc-3.2-2jpp.4
jakarta-commons-collections-debuginfo-3.2-2jpp.4

144095 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2345-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8547

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2345-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00099.html>

SuSE Linux 13.1

x86_64

quassel-mono-debuginfo-0.9.2-25.1
quassel-core-0.9.2-25.1
quassel-base-0.9.2-25.1
quassel-mono-0.9.2-25.1
quassel-client-0.9.2-25.1
quassel-client-debuginfo-0.9.2-25.1
quassel-core-debuginfo-0.9.2-25.1
quassel-debugsource-0.9.2-25.1

i586

quassel-mono-debuginfo-0.9.2-25.1
quassel-core-0.9.2-25.1
quassel-base-0.9.2-25.1
quassel-mono-0.9.2-25.1
quassel-client-0.9.2-25.1
quassel-client-debuginfo-0.9.2-25.1
quassel-core-debuginfo-0.9.2-25.1
quassel-debugsource-0.9.2-25.1

SuSE Linux 13.2

x86_64

quassel-mono-debuginfo-0.10.0-3.13.1
quassel-base-0.10.0-3.13.1
quassel-client-debuginfo-0.10.0-3.13.1
quassel-debugsource-0.10.0-3.13.1
quassel-client-0.10.0-3.13.1
quassel-mono-0.10.0-3.13.1
quassel-core-debuginfo-0.10.0-3.13.1
quassel-core-0.10.0-3.13.1

i586

quassel-mono-debuginfo-0.10.0-3.13.1
quassel-base-0.10.0-3.13.1
quassel-client-debuginfo-0.10.0-3.13.1
quassel-debugsource-0.10.0-3.13.1
quassel-client-0.10.0-3.13.1
quassel-mono-0.10.0-3.13.1
quassel-core-debuginfo-0.10.0-3.13.1

144097 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2304-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3223, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-5330, CVE-2015-8467

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2304-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2015-December/001740.html>

SuSE SLED 12

x86_64

libsamdb0-32bit-4.1.12-18.3.1
samba-libs-debuginfo-32bit-4.1.12-18.3.1
libsamba-hostconfig0-debuginfo-4.1.12-18.3.1
libsamdb0-4.1.12-18.3.1
libtdb1-32bit-1.3.8-2.3.1
libndr-standard0-32bit-4.1.12-18.3.1
libndr-nbt0-32bit-4.1.12-18.3.1
libsamba-hostconfig0-debuginfo-32bit-4.1.12-18.3.1
libsmbclient0-debuginfo-32bit-4.1.12-18.3.1
libsamdb0-debuginfo-4.1.12-18.3.1
libsmbclient0-debuginfo-4.1.12-18.3.1
libsmbconf0-debuginfo-32bit-4.1.12-18.3.1
libsmbldap0-debuginfo-32bit-4.1.12-18.3.1
libsmbclient-raw0-32bit-4.1.12-18.3.1
samba-debugsource-4.1.12-18.3.1
libtalloc2-2.1.5-3.4.1
samba-client-32bit-4.1.12-18.3.1
libsmbclient0-32bit-4.1.12-18.3.1
libndr-standard0-debuginfo-32bit-4.1.12-18.3.1
pytalloc-debuginfo-2.1.5-3.4.1
libndr-nbt0-debuginfo-32bit-4.1.12-18.3.1
libsmbclient0-4.1.12-18.3.1
libsmbconf0-4.1.12-18.3.1
libtevent-util0-debuginfo-32bit-4.1.12-18.3.1
libndr0-4.1.12-18.3.1
libsmbclient-raw0-debuginfo-32bit-4.1.12-18.3.1
libwbclient0-32bit-4.1.12-18.3.1
libndr-krb5pac0-debuginfo-32bit-4.1.12-18.3.1
libpdb0-debuginfo-32bit-4.1.12-18.3.1
libndr0-debuginfo-32bit-4.1.12-18.3.1
libpdb0-debuginfo-4.1.12-18.3.1
libldb1-1.1.24-4.3.1
libtevent0-32bit-0.9.26-3.3.1
samba-libs-4.1.12-18.3.1
libtevent-util0-4.1.12-18.3.1
libdcerpc-binding0-debuginfo-32bit-4.1.12-18.3.1
libwbclient0-debuginfo-4.1.12-18.3.1
libtevent0-debuginfo-0.9.26-3.3.1

libsamba-util0-debuginfo-4.1.12-18.3.1
libndr0-32bit-4.1.12-18.3.1
samba-winbind-32bit-4.1.12-18.3.1
libsamba-hostconfig0-4.1.12-18.3.1
libpdb0-32bit-4.1.12-18.3.1
libgensec0-32bit-4.1.12-18.3.1
libdcerpc-binding0-4.1.12-18.3.1
libdcerpc0-32bit-4.1.12-18.3.1
libnetapi0-debuginfo-32bit-4.1.12-18.3.1
libnetapi0-32bit-4.1.12-18.3.1
libtevent0-0.9.26-3.3.1
libsamba-credentials0-32bit-4.1.12-18.3.1
samba-4.1.12-18.3.1
tdb-debugsource-1.3.8-2.3.1
samba-debuginfo-32bit-4.1.12-18.3.1
libpdb0-4.1.12-18.3.1
samba-libs-32bit-4.1.12-18.3.1
libtalloc2-debuginfo-2.1.5-3.4.1
libndr-standard0-4.1.12-18.3.1
libsmbconf0-32bit-4.1.12-18.3.1
libsmbldap0-debuginfo-4.1.12-18.3.1
libsamba-credentials0-debuginfo-32bit-4.1.12-18.3.1
libregistry0-debuginfo-4.1.12-18.3.1
libtevent0-debuginfo-32bit-0.9.26-3.3.1
samba-winbind-debuginfo-32bit-4.1.12-18.3.1
libndr-nbt0-4.1.12-18.3.1
libsamba-util0-32bit-4.1.12-18.3.1
libndr-standard0-debuginfo-4.1.12-18.3.1
libldb1-debuginfo-32bit-1.1.24-4.3.1
samba-32bit-4.1.12-18.3.1
libnetapi0-debuginfo-4.1.12-18.3.1
libtdb1-debuginfo-32bit-1.3.8-2.3.1
libsamba-util0-debuginfo-32bit-4.1.12-18.3.1
pytalloc-2.1.5-3.4.1
samba-client-debuginfo-4.1.12-18.3.1
samba-client-debuginfo-32bit-4.1.12-18.3.1
libwbclient0-4.1.12-18.3.1
tevent-debugsource-0.9.26-3.3.1
libsamba-credentials0-debuginfo-4.1.12-18.3.1
libldb1-32bit-1.1.24-4.3.1
libtdb1-debuginfo-1.3.8-2.3.1
libwbclient0-debuginfo-32bit-4.1.12-18.3.1
libtalloc2-debuginfo-32bit-2.1.5-3.4.1
pytalloc-32bit-2.1.5-3.4.1
libndr0-debuginfo-4.1.12-18.3.1
libsmbconf0-debuginfo-4.1.12-18.3.1
libsamdb0-debuginfo-32bit-4.1.12-18.3.1
samba-debuginfo-4.1.12-18.3.1
libtevent-util0-debuginfo-4.1.12-18.3.1
libdcerpc-binding0-debuginfo-4.1.12-18.3.1
ldb-debugsource-1.1.24-4.3.1
libndr-krb5pac0-debuginfo-4.1.12-18.3.1
libsmbclient-raw0-debuginfo-4.1.12-18.3.1
samba-libs-debuginfo-4.1.12-18.3.1
libndr-krb5pac0-4.1.12-18.3.1
libsmbldap0-4.1.12-18.3.1
libtevent-util0-32bit-4.1.12-18.3.1
pytalloc-debuginfo-32bit-2.1.5-3.4.1
libgensec0-debuginfo-4.1.12-18.3.1
libsmbclient-raw0-4.1.12-18.3.1

samba-winbind-debuginfo-4.1.12-18.3.1
libgensec0-debuginfo-32bit-4.1.12-18.3.1
libgensec0-4.1.12-18.3.1
libdcerpc-binding0-32bit-4.1.12-18.3.1
libsamba-credentials0-4.1.12-18.3.1
samba-winbind-4.1.12-18.3.1
samba-client-4.1.12-18.3.1
talloc-debugsource-2.1.5-3.4.1
libtalloc2-32bit-2.1.5-3.4.1
libndr-krb5pac0-32bit-4.1.12-18.3.1
libndr-nbt0-debuginfo-4.1.12-18.3.1
libldb1-debuginfo-1.1.24-4.3.1
libregistry0-4.1.12-18.3.1
libsamba-util0-4.1.12-18.3.1
libsmbldap0-32bit-4.1.12-18.3.1
libtdb1-1.3.8-2.3.1
libdcerpc0-debuginfo-4.1.12-18.3.1
libnetapi0-4.1.12-18.3.1
libsamba-hostconfig0-32bit-4.1.12-18.3.1
libdcerpc0-4.1.12-18.3.1
libdcerpc0-debuginfo-32bit-4.1.12-18.3.1

noarch
samba-doc-4.1.12-18.3.1

SuSE SLES 12

noarch
samba-doc-4.1.12-18.3.1

x86_64

libsamdb0-32bit-4.1.12-18.3.1
libndr-krb5pac0-debuginfo-4.1.12-18.3.1
samba-libs-debuginfo-32bit-4.1.12-18.3.1
libsamba-hostconfig0-debuginfo-4.1.12-18.3.1
libsamba-credentials0-32bit-4.1.12-18.3.1
samba-libs-4.1.12-18.3.1
libsmbclient-raw0-4.1.12-18.3.1
libsamdb0-4.1.12-18.3.1
libsamba-hostconfig0-debuginfo-32bit-4.1.12-18.3.1
talloc-debugsource-2.1.5-3.4.1
libsmbclient0-debuginfo-4.1.12-18.3.1
libsmbconf0-debuginfo-32bit-4.1.12-18.3.1
libgensec0-32bit-4.1.12-18.3.1
libsmbclient-raw0-32bit-4.1.12-18.3.1
libndr-nbt0-32bit-4.1.12-18.3.1
samba-libs-32bit-4.1.12-18.3.1
libtalloc2-2.1.5-3.4.1
samba-client-32bit-4.1.12-18.3.1
libsmbclient0-32bit-4.1.12-18.3.1
libndr-standard0-debuginfo-32bit-4.1.12-18.3.1
pytalloc-debuginfo-2.1.5-3.4.1
libndr-nbt0-debuginfo-32bit-4.1.12-18.3.1
libsmbclient0-4.1.12-18.3.1
libsamdb0-debuginfo-4.1.12-18.3.1
libtevent-util0-debuginfo-32bit-4.1.12-18.3.1
libndr0-4.1.12-18.3.1
libsmbconf0-debuginfo-4.1.12-18.3.1
libsmbconf0-4.1.12-18.3.1
libwbclient0-32bit-4.1.12-18.3.1
libndr-krb5pac0-debuginfo-32bit-4.1.12-18.3.1

libldb1-debuginfo-32bit-1.1.24-4.3.1
libsmbldap0-32bit-4.1.12-18.3.1
samba-client-debuginfo-4.1.12-18.3.1
libpdb0-debuginfo-4.1.12-18.3.1
libldb1-1.1.24-4.3.1
libtevent0-32bit-0.9.26-3.3.1
libtevent-util0-4.1.12-18.3.1
libndr0-debuginfo-32bit-4.1.12-18.3.1
libdcerpc-binding0-debuginfo-32bit-4.1.12-18.3.1
samba-winbind-32bit-4.1.12-18.3.1
libtevent0-debuginfo-0.9.26-3.3.1
pytalloc-32bit-2.1.5-3.4.1
libgensec0-debuginfo-4.1.12-18.3.1
libndr0-32bit-4.1.12-18.3.1
libsamba-hostconfig0-4.1.12-18.3.1
libpdb0-32bit-4.1.12-18.3.1
libwbclient0-debuginfo-4.1.12-18.3.1
libdcerpc-binding0-4.1.12-18.3.1
libdcerpc0-32bit-4.1.12-18.3.1
libdcerpc0-4.1.12-18.3.1
libnetapi0-32bit-4.1.12-18.3.1
libnetapi0-debuginfo-32bit-4.1.12-18.3.1
libsamba-util0-debuginfo-32bit-4.1.12-18.3.1
samba-4.1.12-18.3.1
tdb-debugsource-1.3.8-2.3.1
libsmbldap0-debuginfo-32bit-4.1.12-18.3.1
libpdb0-4.1.12-18.3.1
libtdb1-32bit-1.3.8-2.3.1
samba-debuginfo-32bit-4.1.12-18.3.1
libtalloc2-debuginfo-2.1.5-3.4.1
libndr-standard0-4.1.12-18.3.1
libsmbconf0-32bit-4.1.12-18.3.1
libsamba-util0-32bit-4.1.12-18.3.1
libsamba-credentials0-debuginfo-32bit-4.1.12-18.3.1
libregistry0-debuginfo-4.1.12-18.3.1
libtevent0-debuginfo-32bit-0.9.26-3.3.1
samba-winbind-debuginfo-32bit-4.1.12-18.3.1
libndr-nbt0-4.1.12-18.3.1
libsamba-util0-debuginfo-4.1.12-18.3.1
libndr-standard0-debuginfo-4.1.12-18.3.1
libsmbclient0-debuginfo-32bit-4.1.12-18.3.1
samba-32bit-4.1.12-18.3.1
libnetapi0-debuginfo-4.1.12-18.3.1
libtdb1-debuginfo-32bit-1.3.8-2.3.1
libsmbldap0-4.1.12-18.3.1
pytalloc-2.1.5-3.4.1
libsmbclient-raw0-debuginfo-32bit-4.1.12-18.3.1

144099 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2346-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6792

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2346-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00100.html>

SuSE Linux 13.1

x86_64

chromium-ffmpegsumo-47.0.2526.106-119.1
chromium-ffmpegsumo-debuginfo-47.0.2526.106-119.1
chromium-debugsource-47.0.2526.106-119.1
chromium-debuginfo-47.0.2526.106-119.1
chromium-desktop-gnome-47.0.2526.106-119.1
chromium-47.0.2526.106-119.1
chromedriver-47.0.2526.106-119.1
chromedriver-debuginfo-47.0.2526.106-119.1
chromium-desktop-kde-47.0.2526.106-119.1

i586

chromium-ffmpegsumo-47.0.2526.106-119.1
chromium-ffmpegsumo-debuginfo-47.0.2526.106-119.1
chromium-debugsource-47.0.2526.106-119.1
chromium-debuginfo-47.0.2526.106-119.1
chromium-desktop-gnome-47.0.2526.106-119.1
chromium-47.0.2526.106-119.1
chromedriver-47.0.2526.106-119.1
chromedriver-debuginfo-47.0.2526.106-119.1
chromium-desktop-kde-47.0.2526.106-119.1

SuSE Linux 13.2

x86_64

chromium-debugsource-47.0.2526.106-64.1
chromium-desktop-gnome-47.0.2526.106-64.1
chromedriver-debuginfo-47.0.2526.106-64.1
chromedriver-47.0.2526.106-64.1
chromium-ffmpegsumo-debuginfo-47.0.2526.106-64.1
chromium-ffmpegsumo-47.0.2526.106-64.1
chromium-47.0.2526.106-64.1
chromium-desktop-kde-47.0.2526.106-64.1
chromium-debuginfo-47.0.2526.106-64.1

i586

chromium-debugsource-47.0.2526.106-64.1
chromium-desktop-gnome-47.0.2526.106-64.1
chromedriver-debuginfo-47.0.2526.106-64.1
chromedriver-47.0.2526.106-64.1
chromium-ffmpegsumo-debuginfo-47.0.2526.106-64.1
chromium-ffmpegsumo-47.0.2526.106-64.1
chromium-47.0.2526.106-64.1
chromium-desktop-kde-47.0.2526.106-64.1
chromium-debuginfo-47.0.2526.106-64.1

144100 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2328-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5307, CVE-2015-7311, CVE-2015-7504, CVE-2015-7835, CVE-2015-7969, CVE-2015-7970, CVE-2015-7971, CVE-2015-7972, CVE-2015-8104, CVE-2015-8339, CVE-2015-8340, CVE-2015-8341, CVE-2015-8345

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2328-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2015-December/001747.html>

SuSE SLED 12

x86_64
xen-libs-32bit-4.4.3_06-22.15.1
xen-4.4.3_06-22.15.1
xen-debugsource-4.4.3_06-22.15.1
xen-kmp-default-4.4.3_06_k3.12.48_52.27-22.15.1
xen-libs-4.4.3_06-22.15.1
xen-libs-debuginfo-32bit-4.4.3_06-22.15.1
xen-libs-debuginfo-4.4.3_06-22.15.1
xen-kmp-default-debuginfo-4.4.3_06_k3.12.48_52.27-22.15.1

SuSE SLES 12

x86_64
xen-libs-debuginfo-32bit-4.4.3_06-22.15.1
xen-tools-4.4.3_06-22.15.1
xen-4.4.3_06-22.15.1
xen-debugsource-4.4.3_06-22.15.1
xen-kmp-default-4.4.3_06_k3.12.48_52.27-22.15.1
xen-doc-html-4.4.3_06-22.15.1
xen-tools-debuginfo-4.4.3_06-22.15.1
xen-libs-32bit-4.4.3_06-22.15.1
xen-libs-4.4.3_06-22.15.1
xen-tools-domU-4.4.3_06-22.15.1
xen-libs-debuginfo-4.4.3_06-22.15.1
xen-tools-domU-debuginfo-4.4.3_06-22.15.1
xen-kmp-default-debuginfo-4.4.3_06_k3.12.48_52.27-22.15.1

160014 - CentOS 5 CESA-2015-2671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

Description

The scan detected that the host is missing the following update:
CESA-2015-2671

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2015-December/021558.html>

CentOS 5

x86_64
jakarta-commons-collections-tomcat5-3.2-2jpp.4
jakarta-commons-collections-3.2-2jpp.4

jakarta-commons-collections-testframework-javadoc-3.2-2jpp.4
jakarta-commons-collections-testframework-3.2-2jpp.4
jakarta-commons-collections-javadoc-3.2-2jpp.4

i386

jakarta-commons-collections-tomcat5-3.2-2jpp.4
jakarta-commons-collections-3.2-2jpp.4
jakarta-commons-collections-testframework-javadoc-3.2-2jpp.4
jakarta-commons-collections-testframework-3.2-2jpp.4
jakarta-commons-collections-javadoc-3.2-2jpp.4

160018 - CentOS 6 CESA-2015-2694 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7504, CVE-2015-7512

Description

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

CESA-2015-2694

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2015-December/021581.html>

CentOS 6

x86_64

qemu-img-0.12.1.2-2.479.el6_7.3

qemu-kvm-tools-0.12.1.2-2.479.el6_7.3

qemu-guest-agent-0.12.1.2-2.479.el6_7.3

qemu-kvm-0.12.1.2-2.479.el6_7.3

i686

qemu-guest-agent-0.12.1.2-2.479.el6_7.3

174832 - Scientific Linux Security ERRATA Moderate: wireshark on SL7.x x86_64 (1512-7014)

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

Risk Level: High

CVE: CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714, CVE-2015-0562, CVE-2015-0563, CVE-2015-0564, CVE-2015-2188, CVE-2015-2189, CVE-2015-2191, CVE-2015-3182, CVE-2015-3810, CVE-2015-3811, CVE-2015-3812, CVE-2015-3813, CVE-2015-6243, CVE-2015-6244, CVE-2015-6245, CVE-2015-6246, CVE-2015-6248

Description

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

Security ERRATA Moderate: wireshark on SL7.x x86_64 (1512-7014)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=7014>

SL7

x86_64
wireshark-gnome-1.10.14-7.el7
wireshark-1.10.14-7.el7
wireshark-devel-1.10.14-7.el7
wireshark-debuginfo-1.10.14-7.el7

174835 - Scientific Linux Security ERRATA Important: jakarta-commons-collections on SL5.x i386/x86_64 (1512-3803)

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

Risk Level: High

CVE: CVE-2015-7501

Description

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

Security ERRATA Important: jakarta-commons-collections on SL5.x i386/x86_64 (1512-3803)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=3803>

SL5

x86_64

jakarta-commons-collections-javadoc-3.2-2jpp.4
jakarta-commons-collections-3.2-2jpp.4
jakarta-commons-collections-testframework-3.2-2jpp.4
jakarta-commons-collections-testframework-javadoc-3.2-2jpp.4
jakarta-commons-collections-debuginfo-3.2-2jpp.4
jakarta-commons-collections-tomcat5-3.2-2jpp.4

i386

jakarta-commons-collections-javadoc-3.2-2jpp.4
jakarta-commons-collections-3.2-2jpp.4
jakarta-commons-collections-testframework-3.2-2jpp.4
jakarta-commons-collections-testframework-javadoc-3.2-2jpp.4
jakarta-commons-collections-debuginfo-3.2-2jpp.4
jakarta-commons-collections-tomcat5-3.2-2jpp.4

174837 - Scientific Linux Security ERRATA Moderate: libpng12 on SL7.x x86_64 (1512-18795)

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8472

Description

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

Security ERRATA Moderate: libpng12 on SL7.x x86_64 (1512-18795)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=18795>

SL7

x86_64
libpng12-debuginfo-1.2.50-7.el7_2
libpng12-1.2.50-7.el7_2
libpng12-devel-1.2.50-7.el7_2

174844 - Scientific Linux Security ERRATA Important: glibc on SL7.x x86_64 (1512-7709)

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

Risk Level: High

CVE: CVE-2015-5277

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: glibc on SL7.x x86_64 (1512-7709)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=7709>

SL7
x86_64
glibc-devel-2.17-106.el7_2.1
glibc-static-2.17-106.el7_2.1
glibc-utils-2.17-106.el7_2.1
glibc-2.17-106.el7_2.1
glibc-debuginfo-2.17-106.el7_2.1
glibc-debuginfo-common-2.17-106.el7_2.1
glibc-headers-2.17-106.el7_2.1
nscd-2.17-106.el7_2.1
glibc-common-2.17-106.el7_2.1

174846 - Scientific Linux Security ERRATA Moderate: libxml2 on SL7.x x86_64 (1512-17295)

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

Risk Level: High

CVE: CVE-2015-1819, CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libxml2 on SL7.x x86_64 (1512-17295)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=17295>

SL7
x86_64
libxml2-static-2.9.1-6.el7_2.2
libxml2-python-2.9.1-6.el7_2.2
libxml2-2.9.1-6.el7_2.2
libxml2-devel-2.9.1-6.el7_2.2

174849 - Scientific Linux Security ERRATA Moderate: tigervnc on SL7.x x86_64 (1512-4878)

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

Risk Level: High

CVE: CVE-2014-8240, CVE-2014-8241

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: tigervnc on SL7.x x86_64 (1512-4878)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=4878>

SL7
x86_64
tigervnc-1.3.1-3.el7
tigervnc-server-module-1.3.1-3.el7
tigervnc-debuginfo-1.3.1-3.el7
tigervnc-server-1.3.1-3.el7
tigervnc-server-minimal-1.3.1-3.el7

noarch
tigervnc-license-1.3.1-3.el7
tigervnc-icons-1.3.1-3.el7
tigervnc-server-applet-1.3.1-3.el7

174851 - Scientific Linux Security ERRATA Moderate: pacemaker on SL7.x x86_64 (1512-4523)

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

Risk Level: High

CVE: CVE-2015-1867

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: pacemaker on SL7.x x86_64 (1512-4523)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=4523>

SL7
x86_64
pacemaker-libs-1.1.13-10.el7
pacemaker-libs-devel-1.1.13-10.el7
pacemaker-nagios-plugins-metadata-1.1.13-10.el7
pacemaker-1.1.13-10.el7
pacemaker-doc-1.1.13-10.el7
pacemaker-cts-1.1.13-10.el7
pacemaker-cli-1.1.13-10.el7

pacemaker-remote-1.1.13-10.el7
pacemaker-debuginfo-1.1.13-10.el7
pacemaker-cluster-libs-1.1.13-10.el7

174855 - Scientific Linux Security ERRATA Moderate: cups-filters on SL7.x x86_64 (1512-6636)

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

Risk Level: High

CVE: CVE-2015-3258, CVE-2015-3279

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: cups-filters on SL7.x x86_64 (1512-6636)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=6636>

SL7
x86_64
cups-filters-libs-1.0.35-21.el7
cups-filters-1.0.35-21.el7
cups-filters-devel-1.0.35-21.el7
cups-filters-debuginfo-1.0.35-21.el7

174863 - Scientific Linux Security ERRATA Moderate: binutils on SL7.x x86_64 (1512-13035)

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

Risk Level: High

CVE: CVE-2014-8484, CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8503, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: binutils on SL7.x x86_64 (1512-13035)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=13035>

SL7
x86_64
binutils-devel-2.23.52.0.1-55.el7
binutils-2.23.52.0.1-55.el7
binutils-debuginfo-2.23.52.0.1-55.el7

174866 - Scientific Linux Security ERRATA Moderate: file on SL7.x x86_64 (1512-11400)

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

Risk Level: High

CVE: CVE-2014-0207, CVE-2014-0237, CVE-2014-0238, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-

2014-3538, CVE-2014-3587, CVE-2014-3710, CVE-2014-8116, CVE-2014-8117, CVE-2014-9652, CVE-2014-9653

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: file on SL7.x x86_64 (1512-11400)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=11400>

SL7
x86_64
file-devel-5.11-31.el7
file-libs-5.11-31.el7
file-static-5.11-31.el7
file-debuginfo-5.11-31.el7
file-5.11-31.el7

noarch
python-magic-5.11-31.el7

174867 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1512-19489)

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

Risk Level: High

CVE: CVE-2015-7504, CVE-2015-7512

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1512-19489)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=19489>

SL6
x86_64
qemu-img-0.12.1.2-2.479.el6_7.3
qemu-kvm-tools-0.12.1.2-2.479.el6_7.3
qemu-guest-agent-0.12.1.2-2.479.el6_7.3
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.3
qemu-kvm-0.12.1.2-2.479.el6_7.3

i386
qemu-guest-agent-0.12.1.2-2.479.el6_7.3
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.3

174870 - Scientific Linux Security ERRATA Moderate: glibc on SL7.x x86_64 (1512-11952)

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

Risk Level: High

CVE: CVE-2013-7423, CVE-2015-1472, CVE-2015-1473, CVE-2015-1781

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: glibc on SL7.x x86_64 (1512-11952)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=11952>

SL7
x86_64
glibc-2.17-105.el7
glibc-common-2.17-105.el7
glibc-headers-2.17-105.el7
glibc-static-2.17-105.el7
glibc-devel-2.17-105.el7
nscd-2.17-105.el7
glibc-debuginfo-2.17-105.el7
glibc-utils-2.17-105.el7
glibc-debuginfo-common-2.17-105.el7

174874 - Scientific Linux Security ERRATA Moderate: libpng on SL7.x x86_64 (1512-18455)

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

Risk Level: High

CVE: CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libpng on SL7.x x86_64 (1512-18455)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=18455>

SL7
x86_64
libpng-debuginfo-1.5.13-7.el7_2
libpng-1.5.13-7.el7_2
libpng-static-1.5.13-7.el7_2
libpng-devel-1.5.13-7.el7_2

181722 - FreeBSD cups-filters Code Execution (6dbae1a8-a4e6-11e5-b864-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2015-8327

Description

The scan detected that the host is missing the following update:
cups-filters -- code execution (6dbae1a8-a4e6-11e5-b864-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/6dbae1a8-a4e6-11e5-b864-14dae9d210b8.html>

Affected packages:

cups-filters < 1.2.0

foomatic-filters < 4.0.17_4

181727 - FreeBSD joomla Multiple Vulnerabilities (a9f60ce8-a4e0-11e5-b864-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2015-8562, CVE-2015-8563, CVE-2015-8564, CVE-2015-8565

Description

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

joomla -- multiple vulnerabilities (a9f60ce8-a4e0-11e5-b864-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/a9f60ce8-a4e0-11e5-b864-14dae9d210b8.html>

Affected packages:

joomla3 < 3.4.6

190102 - Fedora Linux 23 FEDORA-2015-09bf9e06ea Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8000, CVE-2015-8461

Description

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

FEDORA-2015-09bf9e06ea

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174144.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174146.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174145.html>

Fedora Core 23

dnperf-2.0.0.0-19.fc23

bind-dyndb-ldap-8.0-4.fc23

bind-9.10.3-7.P2.fc23

190104 - Fedora Linux 23 FEDORA-2015-8c475f7169 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126, CVE-2015-8472

Description

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

FEDORA-2015-8c475f7169

Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174105.html>

Fedora Core 23

libpng10-1.0.65-1.fc23

190106 - Fedora Linux 23 FEDORA-2015-12a089920e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7504, CVE-2015-7512, CVE-2015-8338, CVE-2015-8339, CVE-2015-8340, CVE-2015-8341, CVE-2015-8345, CVE-2015-8504

Description

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

FEDORA-2015-12a089920e

Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174017.html>

Fedora Core 23

xen-4.5.2-5.fc23

190109 - Fedora Linux 22 FEDORA-2015-3461e976cb Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126, CVE-2015-8472

Description

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

FEDORA-2015-3461e976cb

Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174127.html>

Fedora Core 22

libpng10-1.0.65-1.fc22

190113 - Fedora Linux 22 FEDORA-2015-08e4af5a20 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7504, CVE-2015-7512, CVE-2015-8338, CVE-2015-8339, CVE-2015-8340, CVE-2015-8341, CVE-2015-8345, CVE-2015-8504

Description

The scan detected that the host is missing the following update:
FEDORA-2015-08e4af5a20

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174187.html>

Fedora Core 22

xen-4.5.2-5.fc22

190123 - Fedora Linux 22 FEDORA-2015-2df40de264 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8000, CVE-2015-8461

Description

The scan detected that the host is missing the following update:
FEDORA-2015-2df40de264

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174251.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174252.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174250.html>

Fedora Core 22

dnperf-2.0.0.0-19.fc22

bind-dyndb-ldap-7.0-6.fc22

bind-9.10.3-7.P2.fc22

88728 - Slackware Linux 14.1 SSA:2015-351-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Description

The scan detected that the host is missing the following update:
SSA:2015-351-01

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=2015&m=slackware-security.346050>

Slackware 14.1
x86_64
grub-2.00-x86_64-3

130341 - Debian Linux 7.0, 8.0 DSA-3421-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Description

The scan detected that the host is missing the following update:
DSA-3421-1

Observation

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

<http://www.debian.org/security/2015/dsa-3421>

Debian 8.0
all
grub2_2.02~beta2-22+deb8u1

Debian 7.0
all
grub2_1.99-27+deb7u3

174834 - Scientific Linux Security ERRATA Moderate: chrony on SL7.x x86_64 (1512-5577)

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

Risk Level: Medium

CVE: CVE-2015-1821, CVE-2015-1822, CVE-2015-1853

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: chrony on SL7.x x86_64 (1512-5577)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=5577>

SL7
x86_64
chrony-2.1.1-1.el7
chrony-debuginfo-2.1.1-1.el7

174838 - Scientific Linux Security ERRATA Low: libssh2 on SL7.x x86_64 (1512-15335)

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

Risk Level: Medium

CVE: CVE-2015-1782

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: libssh2 on SL7.x x86_64 (1512-15335)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=15335>

SL7
x86_64
libssh2-devel-1.4.3-10.el7
libssh2-debuginfo-1.4.3-10.el7
libssh2-1.4.3-10.el7

noarch
libssh2-docs-1.4.3-10.el7

174841 - Scientific Linux Security ERRATA Moderate: abrt and libreport on SL7.x x86_64 (1512-16912)

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

Risk Level: Medium

CVE: CVE-2015-5273, CVE-2015-5287, CVE-2015-5302

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: abrt and libreport on SL7.x x86_64 (1512-16912)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=16912>

SL7
x86_64
abrt-addon-upload-watch-2.1.11-35.el7
abrt-gui-2.1.11-35.el7
libreport-newt-2.1.11-31.el7
abrt-debuginfo-2.1.11-35.el7
libreport-rhel-2.1.11-31.el7
abrt-addon-xorg-2.1.11-35.el7
libreport-web-2.1.11-31.el7
libreport-python-2.1.11-31.el7

abrt-desktop-2.1.11-35.el7
abrt-addon-kerneloops-2.1.11-35.el7
abrt-addon-python-2.1.11-35.el7
abrt-addon-ccpp-2.1.11-35.el7
libreport-anaconda-2.1.11-31.el7
libreport-compatible-2.1.11-31.el7
libreport-plugin-rhtsupport-2.1.11-31.el7
libreport-devel-2.1.11-31.el7
libreport-plugin-reportuploader-2.1.11-31.el7
libreport-rhel-bugzilla-2.1.11-31.el7
libreport-gtk-devel-2.1.11-31.el7
libreport-plugin-mailx-2.1.11-31.el7
libreport-plugin-ureport-2.1.11-31.el7
abrt-devel-2.1.11-35.el7
libreport-2.1.11-31.el7
libreport-debuginfo-2.1.11-31.el7
libreport-web-devel-2.1.11-31.el7
abrt-console-notification-2.1.11-35.el7
abrt-2.1.11-35.el7
libreport-cli-2.1.11-31.el7
abrt-addon-pstoreoops-2.1.11-35.el7
libreport-gtk-2.1.11-31.el7
abrt-gui-devel-2.1.11-35.el7
abrt-dbus-2.1.11-35.el7
abrt-libs-2.1.11-35.el7
abrt-python-2.1.11-35.el7
libreport-plugin-logger-2.1.11-31.el7
libreport-plugin-kerneloops-2.1.11-31.el7
abrt-retrace-client-2.1.11-35.el7
abrt-gui-libs-2.1.11-35.el7
libreport-rhel-anaconda-bugzilla-2.1.11-31.el7
abrt-cli-2.1.11-35.el7
libreport-plugin-bugzilla-2.1.11-31.el7
abrt-tui-2.1.11-35.el7
libreport-filesystem-2.1.11-31.el7
abrt-addon-vmcore-2.1.11-35.el7

noarch
abrt-python-doc-2.1.11-35.el7

174843 - Scientific Linux Security ERRATA Low: sssd on SL7.x x86_64 (1512-8032)

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

Risk Level: Medium

CVE: CVE-2015-5292

Description

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

Security ERRATA Low: sssd on SL7.x x86_64 (1512-8032)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=8032>

SL7

x86_64

python-sss-murmur-1.13.0-40.el7
sssd-proxy-1.13.0-40.el7
sssd-1.13.0-40.el7
sssd-ipa-1.13.0-40.el7
python-libsss_nss_idmap-1.13.0-40.el7
sssd-ldap-1.13.0-40.el7
libsss_simpleifp-devel-1.13.0-40.el7
libsss_simpleifp-1.13.0-40.el7
sssd-libwbclient-1.13.0-40.el7
sssd-client-1.13.0-40.el7
libsss_nss_idmap-devel-1.13.0-40.el7
sssd-krb5-common-1.13.0-40.el7
python-sss-1.13.0-40.el7
sssd-debuginfo-1.13.0-40.el7
sssd-common-1.13.0-40.el7
sssd-common-pac-1.13.0-40.el7
sssd-libwbclient-devel-1.13.0-40.el7
libsss_idmap-1.13.0-40.el7
libipa_hbac-1.13.0-40.el7
sssd-dbus-1.13.0-40.el7
python-libipa_hbac-1.13.0-40.el7
libsss_nss_idmap-1.13.0-40.el7
sssd-krb5-1.13.0-40.el7
libsss_idmap-devel-1.13.0-40.el7
libipa_hbac-devel-1.13.0-40.el7
sssd-ad-1.13.0-40.el7
sssd-tools-1.13.0-40.el7

noarch
python-sssdconfig-1.13.0-40.el7

174848 - Scientific Linux Security ERRATA Moderate: python on SL7.x x86_64 (1512-10966)

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

Risk Level: Medium

CVE: CVE-2013-1752, CVE-2013-1753, CVE-2014-4616, CVE-2014-4650, CVE-2014-7185, CVE-2014-9365

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: python on SL7.x x86_64 (1512-10966)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=10966>

SL7
x86_64
python-debuginfo-2.7.5-34.el7
tkinter-2.7.5-34.el7
python-tools-2.7.5-34.el7
python-devel-2.7.5-34.el7
python-test-2.7.5-34.el7
python-libs-2.7.5-34.el7
python-2.7.5-34.el7
python-debug-2.7.5-34.el7

174859 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1512-15972)

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

Risk Level: Medium

CVE: CVE-2010-5313, CVE-2013-7421, CVE-2014-3647, CVE-2014-7842, CVE-2014-8171, CVE-2014-9419, CVE-2014-9644, CVE-2015-0239, CVE-2015-2925, CVE-2015-3339, CVE-2015-4170, CVE-2015-5283, CVE-2015-6526, CVE-2015-7613, CVE-2015-7837

Description

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

Security ERRATA Important: kernel on SL7.x x86_64 (1512-15972)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=15972>

SL7

x86_64

kernel-debug-devel-3.10.0-327.el7

python-perf-debuginfo-3.10.0-327.el7

kernel-tools-3.10.0-327.el7

perf-3.10.0-327.el7

kernel-debug-3.10.0-327.el7

kernel-3.10.0-327.el7

python-perf-3.10.0-327.el7

kernel-devel-3.10.0-327.el7

kernel-tools-debuginfo-3.10.0-327.el7

kernel-debug-debuginfo-3.10.0-327.el7

kernel-headers-3.10.0-327.el7

perf-debuginfo-3.10.0-327.el7

kernel-tools-libs-devel-3.10.0-327.el7

kernel-debuginfo-common-x86_64-3.10.0-327.el7

kernel-tools-libs-3.10.0-327.el7

kernel-debuginfo-3.10.0-327.el7

noarch

kernel-abi-whitelists-3.10.0-327.el7

kernel-doc-3.10.0-327.el7

174861 - Scientific Linux Security ERRATA Moderate: grub2 on SL7.x x86_64 (1512-19156)

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

Risk Level: Medium

CVE: CVE-2015-8370

Description

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

Security ERRATA Moderate: grub2 on SL7.x x86_64 (1512-19156)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=19156>

SL7
x86_64
grub2-debuginfo-2.02-0.33.el7_2
grub2-tools-2.02-0.33.el7_2
grub2-2.02-0.33.el7_2
grub2-efi-2.02-0.33.el7_2
grub2-efi-modules-2.02-0.33.el7_2

174865 - Scientific Linux Security ERRATA Moderate: ntp on SL7.x x86_64 (1512-9091)

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

Risk Level: Medium

CVE: CVE-2014-9297, CVE-2014-9298, CVE-2014-9750, CVE-2014-9751, CVE-2015-1798, CVE-2015-1799, CVE-2015-3405

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ntp on SL7.x x86_64 (1512-9091)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=9091>

SL7
x86_64
ntp-debuginfo-4.2.6p5-22.el7
ntpdate-4.2.6p5-22.el7
ntp-4.2.6p5-22.el7
snmp-4.2.6p5-22.el7

noarch
ntp-doc-4.2.6p5-22.el7
ntp-perl-4.2.6p5-22.el7

178134 - Gentoo Linux GLSA-201512-05 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4491, CVE-2015-7673, CVE-2015-7674

Description

The scan detected that the host is missing the following update:
GLSA-201512-05

Observation

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

<https://security.gentoo.org/glsa/201512-05>

Affected packages:
x11-libs/gdk-pixbuf < 2.32.1

178135 - Gentoo Linux GLSA-201512-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Description

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

GLSA-201512-03

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201512-03>

Affected packages:

sys-boot/grub < 2.02_beta2-r8

178136 - Gentoo Linux GLSA-201512-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7337

Description

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

GLSA-201512-02

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201512-02>

Affected packages:

dev-python/ipython < 3.2.1-r1

178138 - Gentoo Linux GLSA-201512-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3294

Description

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

GLSA-201512-01

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201512-01>

Affected packages:

net-dns/dnsmasq < 2.72-r2

190115 - Fedora Linux 22 FEDORA-2015-90c27b6e91 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Description

The scan detected that the host is missing the following update:
FEDORA-2015-90c27b6e91

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174049.html>

Fedora Core 22

grub2-2.02-0.18.fc22

190122 - Fedora Linux 22 FEDORA-2015-89468612f5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5317, CVE-2015-5319, CVE-2015-5321, CVE-2015-5322, CVE-2015-5323, CVE-2015-5324, CVE-2015-5326

Description

The scan detected that the host is missing the following update:
FEDORA-2015-89468612f5

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174273.html>

Fedora Core 22

jenkins-1.609.3-4.fc22

19459 - (CTX203879) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-8104, CVE-2015-8554, CVE-2015-8555

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in multiple components. Successful exploitation

could allow an attacker to obtain sensitive information, to cause denial of service or to compromise the host.

91988 - Oracle Enterprise Linux ELSA-2015-2655 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
ELSA-2015-2655

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-December/005649.html>

<http://oss.oracle.com/pipermail/el-errata/2015-December/005646.html>

OEL7

x86_64

bind-libs-9.9.4-29.el7_2.1
bind-devel-9.9.4-29.el7_2.1
bind-9.9.4-29.el7_2.1
bind-pkcs11-utils-9.9.4-29.el7_2.1
bind-pkcs11-devel-9.9.4-29.el7_2.1
bind-chroot-9.9.4-29.el7_2.1
bind-license-9.9.4-29.el7_2.1
bind-pkcs11-libs-9.9.4-29.el7_2.1
bind-lite-devel-9.9.4-29.el7_2.1
bind-sdb-chroot-9.9.4-29.el7_2.1
bind-pkcs11-9.9.4-29.el7_2.1
bind-sdb-9.9.4-29.el7_2.1
bind-utils-9.9.4-29.el7_2.1
bind-libs-lite-9.9.4-29.el7_2.1

OEL6

x86_64

bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5

i386

bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5

130340 - Debian Linux 8.0 DSA-3428-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7810

Description

The scan detected that the host is missing the following update:
DSA-3428-1

Observation

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

<http://www.debian.org/security/2015/dsa-3428>

Debian 8.0
all
tomcat8_8.0.14-1+deb8u1

132206 - Oracle VM OVMSA-2015-0156 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
OVMSA-2015-0156

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2015-December/000404.html>

OVM3.3
x86_64
bind-utils-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5

141043 - Red Hat Enterprise Linux RHSA-2015-2655 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
RHSA-2015-2655

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2655.html>

RHEL6S
i386

bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-debuginfo-9.8.2-0.37.rc1.el6_7.5
bind-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5

x86_64

bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-debuginfo-9.8.2-0.37.rc1.el6_7.5
bind-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5

RHEL6WS

x86_64

bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-9.8.2-0.37.rc1.el6_7.5
bind-debuginfo-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5

i386

bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-9.8.2-0.37.rc1.el6_7.5
bind-debuginfo-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5

RHEL7D

x86_64

bind-libs-9.9.4-29.el7_2.1
bind-devel-9.9.4-29.el7_2.1
bind-9.9.4-29.el7_2.1
bind-pkcs11-utils-9.9.4-29.el7_2.1
bind-pkcs11-devel-9.9.4-29.el7_2.1
bind-chroot-9.9.4-29.el7_2.1
bind-pkcs11-libs-9.9.4-29.el7_2.1
bind-debuginfo-9.9.4-29.el7_2.1
bind-sdb-chroot-9.9.4-29.el7_2.1
bind-pkcs11-9.9.4-29.el7_2.1
bind-sdb-9.9.4-29.el7_2.1
bind-lite-devel-9.9.4-29.el7_2.1
bind-utils-9.9.4-29.el7_2.1
bind-libs-lite-9.9.4-29.el7_2.1

noarch

bind-license-9.9.4-29.el7_2.1

RHEL6D

x86_64

bind-9.8.2-0.37.rc1.el6_7.5
bind-debuginfo-9.8.2-0.37.rc1.el6_7.5
bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5

bind-utils-9.8.2-0.37.rc1.el6_7.5

i386

bind-9.8.2-0.37.rc1.el6_7.5
bind-debuginfo-9.8.2-0.37.rc1.el6_7.5
bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5

RHEL7WS

x86_64
bind-libs-9.9.4-29.el7_2.1
bind-devel-9.9.4-29.el7_2.1
bind-9.9.4-29.el7_2.1
bind-pkcs11-utils-9.9.4-29.el7_2.1
bind-pkcs11-devel-9.9.4-29.el7_2.1
bind-chroot-9.9.4-29.el7_2.1
bind-pkcs11-libs-9.9.4-29.el7_2.1
bind-debuginfo-9.9.4-29.el7_2.1
bind-sdb-chroot-9.9.4-29.el7_2.1
bind-pkcs11-9.9.4-29.el7_2.1
bind-sdb-9.9.4-29.el7_2.1
bind-lite-devel-9.9.4-29.el7_2.1
bind-utils-9.9.4-29.el7_2.1
bind-libs-lite-9.9.4-29.el7_2.1

noarch

bind-license-9.9.4-29.el7_2.1

141047 - Red Hat Enterprise Linux RHSA-2015-2658 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
RHSA-2015-2658

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2658.html>

RHEL5S

i386
bind97-chroot-9.7.0-21.P2.el5_11.4
bind97-utils-9.7.0-21.P2.el5_11.4
bind97-9.7.0-21.P2.el5_11.4
bind97-debuginfo-9.7.0-21.P2.el5_11.4
bind97-devel-9.7.0-21.P2.el5_11.4
bind97-libs-9.7.0-21.P2.el5_11.4

x86_64

bind97-chroot-9.7.0-21.P2.el5_11.4

bind97-utils-9.7.0-21.P2.el5_11.4
bind97-9.7.0-21.P2.el5_11.4
bind97-debuginfo-9.7.0-21.P2.el5_11.4
bind97-devel-9.7.0-21.P2.el5_11.4
bind97-libs-9.7.0-21.P2.el5_11.4

141048 - Red Hat Enterprise Linux RHSA-2015-2656 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
RHSA-2015-2656

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2656.html>

RHEL5D

x86_64
bind-debuginfo-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5
bind-sdb-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5

i386

bind-debuginfo-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5
bind-sdb-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5

RHEL5S

i386
bind-sdb-9.3.6-25.P1.el5_11.5
bind-chroot-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-debuginfo-9.3.6-25.P1.el5_11.5
bind-devel-9.3.6-25.P1.el5_11.5
bind-libbind-devel-9.3.6-25.P1.el5_11.5
caching-nameserver-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5

x86_64

bind-sdb-9.3.6-25.P1.el5_11.5
bind-chroot-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-debuginfo-9.3.6-25.P1.el5_11.5
bind-devel-9.3.6-25.P1.el5_11.5
bind-libbind-devel-9.3.6-25.P1.el5_11.5
caching-nameserver-9.3.6-25.P1.el5_11.5

144101 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2288-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2288-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00070.html>

SuSE Linux 13.1

i586

openssl-1.0.1k-11.75.1

openssl-debugsource-1.0.1k-11.75.1

libopenssl-devel-1.0.1k-11.75.1

libopenssl1_0_0-1.0.1k-11.75.1

libopenssl1_0_0-debuginfo-1.0.1k-11.75.1

openssl-debuginfo-1.0.1k-11.75.1

noarch

openssl-doc-1.0.1k-11.75.1

x86_64

libopenssl1_0_0-debuginfo-32bit-1.0.1k-11.75.1

openssl-1.0.1k-11.75.1

libopenssl-devel-32bit-1.0.1k-11.75.1

libopenssl1_0_0-32bit-1.0.1k-11.75.1

openssl-debugsource-1.0.1k-11.75.1

libopenssl-devel-1.0.1k-11.75.1

libopenssl1_0_0-1.0.1k-11.75.1

libopenssl1_0_0-debuginfo-1.0.1k-11.75.1

openssl-debuginfo-1.0.1k-11.75.1

SuSE Linux 13.2

i586

libopenssl1_0_0-hmac-1.0.1k-2.27.1

libopenssl-devel-1.0.1k-2.27.1

openssl-debuginfo-1.0.1k-2.27.1

openssl-1.0.1k-2.27.1

libopenssl1_0_0-debuginfo-1.0.1k-2.27.1

openssl-debugsource-1.0.1k-2.27.1

libopenssl1_0_0-1.0.1k-2.27.1

noarch

openssl-doc-1.0.1k-2.27.1

x86_64

libopenssl-devel-32bit-1.0.1k-2.27.1

libopenssl1_0_0-debuginfo-32bit-1.0.1k-2.27.1

libopenssl1_0_0-hmac-1.0.1k-2.27.1

libopenssl-devel-1.0.1k-2.27.1
openssl-debuginfo-1.0.1k-2.27.1
openssl-1.0.1k-2.27.1
libopenssl1_0_0-debuginfo-1.0.1k-2.27.1
openssl-debugsource-1.0.1k-2.27.1
libopenssl1_0_0-32bit-1.0.1k-2.27.1
libopenssl1_0_0-1.0.1k-2.27.1
libopenssl1_0_0-hmac-32bit-1.0.1k-2.27.1

144102 - SuSE SLED 12 SUSE-SU-2015:2342-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3195

Description

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

SUSE-SU-2015:2342-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2015-December/001758.html>

SuSE SLED 12

x86_64

libopenssl0_9_8-debuginfo-0.9.8j-87.1

libopenssl0_9_8-0.9.8j-87.1

libopenssl0_9_8-32bit-0.9.8j-87.1

compat-openssl098-debugsource-0.9.8j-87.1

libopenssl0_9_8-debuginfo-32bit-0.9.8j-87.1

144103 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2341-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

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

SUSE-SU-2015:2341-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2015-December/001757.html>

SuSE SLED 12

x86_64

bind-utils-9.9.6P1-28.6.1

bind-debugsource-9.9.6P1-28.6.1

bind-libs-debuginfo-32bit-9.9.6P1-28.6.1

bind-libs-9.9.6P1-28.6.1

bind-utils-debuginfo-9.9.6P1-28.6.1

bind-libs-debuginfo-9.9.6P1-28.6.1
bind-debuginfo-9.9.6P1-28.6.1
bind-libs-32bit-9.9.6P1-28.6.1

SuSE SLES 12

noarch
bind-doc-9.9.6P1-28.6.1

x86_64

bind-utils-9.9.6P1-28.6.1
bind-debugsource-9.9.6P1-28.6.1
bind-chrootenv-9.9.6P1-28.6.1
bind-libs-debuginfo-32bit-9.9.6P1-28.6.1
bind-libs-9.9.6P1-28.6.1
bind-utils-debuginfo-9.9.6P1-28.6.1
bind-9.9.6P1-28.6.1
bind-debuginfo-9.9.6P1-28.6.1
bind-libs-32bit-9.9.6P1-28.6.1
bind-libs-debuginfo-9.9.6P1-28.6.1

144105 - SuSE Linux 13.2 openSUSE-SU-2015:2318-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2318-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00087.html>

SuSE Linux 13.2

i586
libtls4-debuginfo-2.2.1-2.10.1
libssl33-debuginfo-2.2.1-2.10.1
libtls4-2.2.1-2.10.1
libressl-debuginfo-2.2.1-2.10.1
libssl33-2.2.1-2.10.1
libressl-devel-2.2.1-2.10.1
libressl-2.2.1-2.10.1
libressl-debugsource-2.2.1-2.10.1
libcrypto34-debuginfo-2.2.1-2.10.1
libcrypto34-2.2.1-2.10.1

noarch
libressl-devel-doc-2.2.1-2.10.1

x86_64

libtls4-debuginfo-32bit-2.2.1-2.10.1
libressl-2.2.1-2.10.1
libssl33-2.2.1-2.10.1
libressl-debugsource-2.2.1-2.10.1
libssl33-debuginfo-2.2.1-2.10.1

libssl33-32bit-2.2.1-2.10.1
libcrypto34-2.2.1-2.10.1
libtls4-2.2.1-2.10.1
libcrypto34-debuginfo-2.2.1-2.10.1
libcrypto34-32bit-2.2.1-2.10.1
libressl-devel-2.2.1-2.10.1
libcrypto34-debuginfo-32bit-2.2.1-2.10.1
libtls4-debuginfo-2.2.1-2.10.1
libtls4-32bit-2.2.1-2.10.1
libressl-devel-32bit-2.2.1-2.10.1
libssl33-debuginfo-32bit-2.2.1-2.10.1
libressl-debuginfo-2.2.1-2.10.1

160016 - CentOS 6, 7 CESA-2015-2655 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
CESA-2015-2655

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2015-December/021546.html>

<http://lists.centos.org/pipermail/centos-announce/2015-December/021549.html>

CentOS 7

i686
bind-libs-9.9.4-29.el7_2.1
bind-pkcs11-devel-9.9.4-29.el7_2.1
bind-devel-9.9.4-29.el7_2.1
bind-lite-devel-9.9.4-29.el7_2.1
bind-pkcs11-libs-9.9.4-29.el7_2.1
bind-libs-lite-9.9.4-29.el7_2.1

noarch

bind-license-9.9.4-29.el7_2.1

x86_64

bind-libs-9.9.4-29.el7_2.1
bind-devel-9.9.4-29.el7_2.1
bind-9.9.4-29.el7_2.1
bind-pkcs11-utils-9.9.4-29.el7_2.1
bind-pkcs11-devel-9.9.4-29.el7_2.1
bind-chroot-9.9.4-29.el7_2.1
bind-pkcs11-libs-9.9.4-29.el7_2.1
bind-lite-devel-9.9.4-29.el7_2.1
bind-sdb-chroot-9.9.4-29.el7_2.1
bind-pkcs11-9.9.4-29.el7_2.1
bind-sdb-9.9.4-29.el7_2.1
bind-utils-9.9.4-29.el7_2.1
bind-libs-lite-9.9.4-29.el7_2.1

CentOS 6

x86_64
bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5

i686
bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5

160017 - CentOS 5 CESA-2015-2656 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
CESA-2015-2656

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2015-December/021551.html>

CentOS 5
x86_64
bind-chroot-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-sdb-9.3.6-25.P1.el5_11.5
bind-devel-9.3.6-25.P1.el5_11.5
bind-libbind-devel-9.3.6-25.P1.el5_11.5
caching-nameserver-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5

i386
bind-chroot-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-sdb-9.3.6-25.P1.el5_11.5
bind-devel-9.3.6-25.P1.el5_11.5
bind-libbind-devel-9.3.6-25.P1.el5_11.5
caching-nameserver-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5

160019 - CentOS 5 CESA-2015-2658 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
CESA-2015-2658

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2015-December/021550.html>

CentOS 5
x86_64
bind97-9.7.0-21.P2.el5_11.4
bind97-devel-9.7.0-21.P2.el5_11.4
bind97-chroot-9.7.0-21.P2.el5_11.4
bind97-libs-9.7.0-21.P2.el5_11.4
bind97-utils-9.7.0-21.P2.el5_11.4

i386
bind97-9.7.0-21.P2.el5_11.4
bind97-devel-9.7.0-21.P2.el5_11.4
bind97-chroot-9.7.0-21.P2.el5_11.4
bind97-libs-9.7.0-21.P2.el5_11.4
bind97-utils-9.7.0-21.P2.el5_11.4

174833 - Scientific Linux Security ERRATA Moderate: cpio on SL7.x x86_64 (1512-10232)

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

Risk Level: Medium

CVE: CVE-2014-9112

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: cpio on SL7.x x86_64 (1512-10232)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=10232>

SL7
x86_64
cpio-debuginfo-2.11-24.el7
cpio-2.11-24.el7

174836 - Scientific Linux Security ERRATA Moderate: git on SL7.x x86_64 (1512-18147)

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: git on SL7.x x86_64 (1512-18147)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=18147>

SL7
x86_64
git-1.8.3.1-6.el7
git-daemon-1.8.3.1-6.el7
git-debuginfo-1.8.3.1-6.el7
git-svn-1.8.3.1-6.el7

noarch
gitweb-1.8.3.1-6.el7
emacs-git-el-1.8.3.1-6.el7
perl-Git-SVN-1.8.3.1-6.el7
git-cvs-1.8.3.1-6.el7
git-all-1.8.3.1-6.el7
git-hg-1.8.3.1-6.el7
gitk-1.8.3.1-6.el7
git-bzr-1.8.3.1-6.el7
git-email-1.8.3.1-6.el7
git-p4-1.8.3.1-6.el7
perl-Git-1.8.3.1-6.el7
git-gui-1.8.3.1-6.el7
emacs-git-1.8.3.1-6.el7

174839 - Scientific Linux Security ERRATA Moderate: pcs on SL7.x x86_64 (1512-14243)

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

Risk Level: Medium

CVE: CVE-2015-3225

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: pcs on SL7.x x86_64 (1512-14243)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=14243>

SL7
x86_64
pcs-0.9.143-15.el7
pcs-debuginfo-0.9.143-15.el7

174840 - Scientific Linux Security ERRATA Moderate: net-snmp on SL7.x x86_64 (1512-6297)

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

Risk Level: Medium

CVE: CVE-2014-3565

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: net-snmp on SL7.x x86_64 (1512-6297)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=6297>

SL7
x86_64
net-snmp-libs-5.7.2-24.el7
net-snmp-utils-5.7.2-24.el7
net-snmp-agent-libs-5.7.2-24.el7
net-snmp-sysvinit-5.7.2-24.el7
net-snmp-devel-5.7.2-24.el7
net-snmp-perl-5.7.2-24.el7
net-snmp-5.7.2-24.el7
net-snmp-gui-5.7.2-24.el7
net-snmp-debuginfo-5.7.2-24.el7
net-snmp-python-5.7.2-24.el7

174845 - Scientific Linux Security ERRATA Moderate: NetworkManager on SL7.x x86_64 (1512-8368)

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

Risk Level: Medium

CVE: CVE-2015-0272, CVE-2015-2924

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: NetworkManager on SL7.x x86_64 (1512-8368)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=8368>

SL7
x86_64
NetworkManager-libreswan-gnome-1.0.6-3.el7
NetworkManager-libreswan-1.0.6-3.el7
ModemManager-glib-1.1.0-8.git20130913.el7
libnm-gtk-1.0.6-2.el7
nm-connection-editor-1.0.6-2.el7
NetworkManager-wwan-1.0.6-27.el7
NetworkManager-1.0.6-27.el7
NetworkManager-libnm-1.0.6-27.el7
ModemManager-glib-devel-1.1.0-8.git20130913.el7
NetworkManager-glib-devel-1.0.6-27.el7
NetworkManager-config-routing-rules-1.0.6-27.el7
ModemManager-debuginfo-1.1.0-8.git20130913.el7
NetworkManager-libreswan-debuginfo-1.0.6-3.el7
network-manager-applet-1.0.6-2.el7

NetworkManager-tui-1.0.6-27.el7
NetworkManager-config-server-1.0.6-27.el7
NetworkManager-devel-1.0.6-27.el7
libnm-gtk-devel-1.0.6-2.el7
NetworkManager-bluetooth-1.0.6-27.el7
NetworkManager-libnm-devel-1.0.6-27.el7
network-manager-applet-debuginfo-1.0.6-2.el7
NetworkManager-glib-1.0.6-27.el7
ModemManager-1.1.0-8.git20130913.el7
NetworkManager-team-1.0.6-27.el7
NetworkManager-adsl-1.0.6-27.el7
ModemManager-vala-1.1.0-8.git20130913.el7
NetworkManager-wifi-1.0.6-27.el7
NetworkManager-debuginfo-1.0.6-27.el7
ModemManager-devel-1.1.0-8.git20130913.el7

174847 - Scientific Linux Security ERRATA Low: xfsprogs on SL7.x x86_64 (1512-9537)

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

Risk Level: Medium

CVE: CVE-2012-2150

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: xfsprogs on SL7.x x86_64 (1512-9537)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=9537>

SL7
x86_64
xfsprogs-3.2.2-2.el7
xfsprogs-devel-3.2.2-2.el7
xfsprogs-qa-devel-3.2.2-2.el7
xfsprogs-debuginfo-3.2.2-2.el7

174852 - Scientific Linux Security ERRATA Moderate: rubygem-bundler and rubygem-thor on SL7.x (noarch) (1512-10563)

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

Risk Level: Medium

CVE: CVE-2013-0334

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: rubygem-bundler and rubygem-thor on SL7.x (noarch) (1512-10563)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=10563>

SL7

noarch
rubygem-thor-doc-0.19.1-1.el7
rubygem-bundler-doc-1.7.8-3.el7
rubygem-bundler-1.7.8-3.el7
rubygem-thor-0.19.1-1.el7

174856 - Scientific Linux Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1512-2398)

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1512-2398)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=2398>

SL5
x86_64
bind97-chroot-9.7.0-21.P2.el5_11.4
bind97-utils-9.7.0-21.P2.el5_11.4
bind97-9.7.0-21.P2.el5_11.4
bind97-debuginfo-9.7.0-21.P2.el5_11.4
bind97-devel-9.7.0-21.P2.el5_11.4
bind97-libs-9.7.0-21.P2.el5_11.4

i386
bind97-chroot-9.7.0-21.P2.el5_11.4
bind97-utils-9.7.0-21.P2.el5_11.4
bind97-9.7.0-21.P2.el5_11.4
bind97-debuginfo-9.7.0-21.P2.el5_11.4
bind97-devel-9.7.0-21.P2.el5_11.4
bind97-libs-9.7.0-21.P2.el5_11.4

174857 - Scientific Linux Security ERRATA Moderate: netcf on SL7.x x86_64 (1512-13508)

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

Risk Level: Medium

CVE: CVE-2014-8119

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: netcf on SL7.x x86_64 (1512-13508)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=13508>

SL7

x86_64
netcf-devel-0.2.8-1.el7
netcf-debuginfo-0.2.8-1.el7
netcf-0.2.8-1.el7
netcf-libs-0.2.8-1.el7

174858 - Scientific Linux Security ERRATA Moderate: curl on SL7.x x86_64 (1512-14587)

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

Risk Level: Medium

CVE: CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, CVE-2015-3148

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: curl on SL7.x x86_64 (1512-14587)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=14587>

SL7
x86_64
curl-debuginfo-7.29.0-25.el7
libcurl-devel-7.29.0-25.el7
libcurl-7.29.0-25.el7
curl-7.29.0-25.el7

174860 - Scientific Linux Security ERRATA Important: bind on SL5.x i386/x86_64 (1512-2724)

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL5.x i386/x86_64 (1512-2724)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=2724>

SL5
x86_64
bind-debuginfo-9.3.6-25.P1.el5_11.5
bind-chroot-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-sdb-9.3.6-25.P1.el5_11.5
bind-devel-9.3.6-25.P1.el5_11.5
bind-libbind-devel-9.3.6-25.P1.el5_11.5
caching-nameserver-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5

i386
bind-debuginfo-9.3.6-25.P1.el5_11.5
bind-chroot-9.3.6-25.P1.el5_11.5
bind-9.3.6-25.P1.el5_11.5
bind-utils-9.3.6-25.P1.el5_11.5
bind-sdb-9.3.6-25.P1.el5_11.5
bind-devel-9.3.6-25.P1.el5_11.5
bind-libbind-devel-9.3.6-25.P1.el5_11.5
caching-nameserver-9.3.6-25.P1.el5_11.5
bind-libs-9.3.6-25.P1.el5_11.5

174862 - Scientific Linux Security ERRATA Moderate: openldap on SL7.x x86_64 (1512-9879)

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

Risk Level: Medium

CVE: CVE-2015-3276

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openldap on SL7.x x86_64 (1512-9879)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=9879>

SL7
x86_64
openldap-servers-2.4.40-8.el7
openldap-servers-sql-2.4.40-8.el7
openldap-2.4.40-8.el7
openldap-debuginfo-2.4.40-8.el7
openldap-clients-2.4.40-8.el7
openldap-devel-2.4.40-8.el7

174868 - Scientific Linux Security ERRATA Important: bind on SL6.x i386/x86_64 (1512-3481)

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL6.x i386/x86_64 (1512-3481)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=3481>

SL6
x86_64
bind-9.8.2-0.37.rc1.el6_7.5

bind-debuginfo-9.8.2-0.37.rc1.el6_7.5
bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5

i386

bind-9.8.2-0.37.rc1.el6_7.5
bind-debuginfo-9.8.2-0.37.rc1.el6_7.5
bind-chroot-9.8.2-0.37.rc1.el6_7.5
bind-devel-9.8.2-0.37.rc1.el6_7.5
bind-sdb-9.8.2-0.37.rc1.el6_7.5
bind-libs-9.8.2-0.37.rc1.el6_7.5
bind-utils-9.8.2-0.37.rc1.el6_7.5

174875 - Scientific Linux Security ERRATA Moderate: realmd on SL7.x x86_64 (1512-16562)

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

Risk Level: Medium

CVE: CVE-2015-2704

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: realmd on SL7.x x86_64 (1512-16562)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=16562>

SL7
x86_64
realmd-devel-docs-0.16.1-5.el7
realmd-debuginfo-0.16.1-5.el7
realmd-0.16.1-5.el7

174876 - Scientific Linux Security ERRATA Moderate: krb5 on SL7.x x86_64 (1512-12350)

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

Risk Level: Medium

CVE: CVE-2014-5355, CVE-2015-2694

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: krb5 on SL7.x x86_64 (1512-12350)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=12350>

SL7
x86_64

krb5-server-ldap-1.13.2-10.el7
krb5-workstation-1.13.2-10.el7
krb5-server-1.13.2-10.el7
krb5-devel-1.13.2-10.el7
krb5-pkinit-1.13.2-10.el7
krb5-libs-1.13.2-10.el7
krb5-debuginfo-1.13.2-10.el7

185093 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2845-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3925, CVE-2015-7529

Description

The scan detected that the host is missing the following update:
USN-2845-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003234.html>

Ubuntu 15.04

sosreport_3.2-2ubuntu0.1

Ubuntu 15.10

sosreport_3.2-2ubuntu1.1

Ubuntu 14.04

sosreport_3.1-1ubuntu2.2

190118 - Fedora Linux 23 FEDORA-2015-40882ddfb1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
FEDORA-2015-40882ddfb1

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174143.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174142.html>

Fedora Core 23

bind99-9.9.8-1.P2.fc23

190121 - Fedora Linux 22 FEDORA-2015-d5cc306730 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1038

Description

The scan detected that the host is missing the following update:
FEDORA-2015-d5cc306730

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174245.html>

Fedora Core 22

p7zip-15.09-4.fc22

19464 - MariaDB Multiple Vulnerabilities Prior To 5.5.46

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

Risk Level: Medium

CVE: CVE-2015-4792, CVE-2015-4802, CVE-2015-4807, CVE-2015-4815, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4913

Description

Multiple vulnerabilities are present in some versions of MariaDB.

Observation

MariaDB is a widely used relational database management system.

Multiple vulnerabilities are present in some versions of MariaDB. The flaws are due to errors in multiple components. Successful exploitation could allow an attacker to cause denial of service on the affected software.

130346 - Debian Linux 7.0, 8.0 DSA-3426-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7446, CVE-2015-7799, CVE-2015-7833, CVE-2015-8104, CVE-2015-8374, CVE-2015-8543

Description

The scan detected that the host is missing the following update:
DSA-3426-1

Observation

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

Debian 8.0

all

ntfs-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
ntfs-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt20-1+deb8u1
isofs-modules-3.16.0-4-versatile-di_3.16.7-ckt20-1+deb8u1
serial-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt20-1+deb8u1
nic-shared-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt20-1+deb8u1
jfs-modules-3.16.0-4-powerpc64-di_3.16.7-ckt20-1+deb8u1
crypto-dm-modules-3.16.0-4-versatile-di_3.16.7-ckt20-1+deb8u1
pcmcia-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
crc-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
udf-modules-3.16.0-4-loongson-3-di_3.16.7-ckt20-1+deb8u1
firewire-core-modules-3.16.0-4-amd64-di_3.16.7-ckt20-1+deb8u1
crypto-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
usb-storage-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt20-1+deb8u1
ata-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt20-1+deb8u1
xfs-modules-3.16.0-4-amd64-di_3.16.7-ckt20-1+deb8u1
kernel-image-3.16.0-4-octeon-di_3.16.7-ckt20-1+deb8u1
efi-modules-3.16.0-4-arm64-di_3.16.7-ckt20-1+deb8u1
nbd-modules-3.16.0-4-powerpc64-di_3.16.7-ckt20-1+deb8u1
nbd-modules-3.16.0-4-r5k-ip32-di_3.16.7-ckt20-1+deb8u1
md-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
usb-storage-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
uinput-modules-3.16.0-4-amd64-di_3.16.7-ckt20-1+deb8u1
nic-shared-modules-3.16.0-4-r4k-ip22-di_3.16.7-ckt20-1+deb8u1
nbd-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
linux-compiler-gcc-4.8-s390_3.16.7-ckt20-1+deb8u1
scsi-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt20-1+deb8u1
virtio-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
crypto-modules-3.16.0-4-s390x-di_3.16.7-ckt20-1+deb8u1
ata-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt20-1+deb8u1
isofs-modules-3.16.0-4-586-di_3.16.7-ckt20-1+deb8u1
nic-shared-modules-3.16.0-4-arm64-di_3.16.7-ckt20-1+deb8u1
ext4-modules-3.16.0-4-s390x-di_3.16.7-ckt20-1+deb8u1
multipath-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt20-1+deb8u1
nic-shared-modules-3.16.0-4-r5k-ip32-di_3.16.7-ckt20-1+deb8u1
sound-modules-3.16.0-4-amd64-di_3.16.7-ckt20-1+deb8u1
kernel-image-3.16.0-4-powerpc64-di_3.16.7-ckt20-1+deb8u1
sata-modules-3.16.0-4-kirkwood-di_3.16.7-ckt20-1+deb8u1
fat-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
crypto-dm-modules-3.16.0-4-powerpc64-di_3.16.7-ckt20-1+deb8u1
udf-modules-3.16.0-4-kirkwood-di_3.16.7-ckt20-1+deb8u1
crypto-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
crypto-dm-modules-3.16.0-4-arm64-di_3.16.7-ckt20-1+deb8u1
ppp-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt20-1+deb8u1
loop-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt20-1+deb8u1
loop-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
fat-modules-3.16.0-4-versatile-di_3.16.7-ckt20-1+deb8u1
isofs-modules-3.16.0-4-kirkwood-di_3.16.7-ckt20-1+deb8u1
nic-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
hfs-modules-3.16.0-4-loongson-3-di_3.16.7-ckt20-1+deb8u1
kernel-image-3.16.0-4-versatile-di_3.16.7-ckt20-1+deb8u1
jfs-modules-3.16.0-4-loongson-3-di_3.16.7-ckt20-1+deb8u1
md-modules-3.16.0-4-s390x-di_3.16.7-ckt20-1+deb8u1
md-modules-3.16.0-4-kirkwood-di_3.16.7-ckt20-1+deb8u1
xfs-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt20-1+deb8u1
loop-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt20-1+deb8u1
core-modules-3.16.0-4-kirkwood-di_3.16.7-ckt20-1+deb8u1

usb-modules-3.16.0-4-versatile-di_3.16.7-ckt20-1+deb8u1
linux-headers-3.16.0-4-versatile_3.16.7-ckt20-1+deb8u1
btrfs-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt20-1+deb8u1
mouse-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
usb-storage-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt20-1+deb8u1
linux-headers-3.16.0-4-all-s390x_3.16.7-ckt20-1+deb8u1
linux-image-3.16.0-4-r4k-ip22_3.16.7-ckt20-1+deb8u1
usb-serial-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
udf-modules-3.16.0-4-r4k-ip22-di_3.16.7-ckt20-1+deb8u1
udf-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
udf-modules-3.16.0-4-586-di_3.16.7-ckt20-1+deb8u1
linux-image-3.16.0-4-sb1-bcm91250a_3.16.7-ckt20-1+deb8u1
event-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt20-1+deb8u1
linux-headers-3.16.0-4-amd64_3.16.7-ckt20-1+deb8u1
scsi-core-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
usb-storage-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt20-1+deb8u1
mmc-modules-3.16.0-4-amd64-di_3.16.7-ckt20-1+deb8u1
event-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt20-1+deb8u1
scsi-common-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt20-1+deb8u1
multipath-modules-3.16.0-4-versatile-di_3.16.7-ckt20-1+deb8u1
usb-storage-modules-3.16.0-4-586-di_3.16.7-ckt20-1+deb8u1
hfs-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
fb-modules-3.16.0-4-kirkwood-di_3.16.7-ckt20-1+deb8u1
ata-modules-3.16.0-4-arm64-di_3.16.7-ckt20-1+deb8u1
fat-modules-3.16.0-4-586-di_3.16.7-ckt20-1+deb8u1
squashfs-modules-3.16.0-4-octeon-di_3.16.7-ckt20-1+deb8u1
udf-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
ata-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt20-1+deb8u1
btrfs-modules-3.16.0-4-r4k-ip22-di_3.16.7-ckt20-1+deb8u1
scsi-core-modules-3.16.0-4-s390x-di_3.16.7-ckt20-1+deb8u1
fuse-modules-3.16.0-4-s390x-di_3.16.7-ckt20-1+deb8u1
multipath-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
linux-headers-3.16.0-4-all-i386_3.16.7-ckt20-1+deb8u1
jfs-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt20-1+deb8u1
ext4-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
usb-modules-3.16.0-4-amd64-di_3.16.7-ckt20-1+deb8u1
loop-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt20-1+deb8u1
fuse-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
fuse-modules-3.16.0-4-loongson-3-di_3.16.7-ckt20-1+deb8u1
minix-modules-3.16.0-4-orion5x-di_3.16.7-ckt20-1+deb8u1
scsi-common-modules-3.16.0-4-586-di_3.16.7-ckt20-1+deb8u1
i2c-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt20-1+deb8u1
serial-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
hfs-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt20-1+deb8u1
sata-modules-3.16.0-4-loongson-3-di_3.16.7-ckt20-1+deb8u1
udf-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt20-1+deb8u1
pata-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt20-1+deb8u1
nic-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
scsi-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
btrfs-modules-3.16.0-4-octeon-di_3.16.7-ckt20-1+deb8u1
multipath-modules-3.16.0-4-loongson-3-di_3.16.7-ckt20-1+deb8u1
speakup-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt20-1+deb8u1
nic-usb-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1
fuse-modules-3.16.0-4-amd64-di_3.16.7-ckt20-1+deb8u1
crypto-dm-modules-3.16.0-4-octeon-di_3.16.7-ckt20-1+deb8u1
mmc-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
rtc-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt20-1+deb8u1
btrfs-modules-3.16.0-4-586-di_3.16.7-ckt20-1+deb8u1
serial-modules-3.16.0-4-powerpc64-di_3.16.7-ckt20-1+deb8u1
nic-pcmcia-modules-3.16.0-4-686-pae-di_3.16.7-ckt20-1+deb8u1

jfs-modules-3.16.0-4-powerpc-di_3.16.7-ckt20-1+deb8u1
input-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt20-1+deb8u1
ppp-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt20-1+deb8u1
sata-modules-3.16.0-4-armmp-di_3.16.7-ckt20-1+deb8u1
btrfs-modules-3.16.0-4-loongson-3-di_3.16.7-ckt20-1+deb8u1

Debian 7.0

all
multipath-modules-3.2.0-4-loongson-2f-di_3.2.73-2+deb7u1

174871 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1512-17791)

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1512-17791)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=17791>

SL7

x86_64

python-perf-3.10.0-327.3.1.el7
kernel-tools-3.10.0-327.3.1.el7
kernel-3.10.0-327.3.1.el7
kernel-debug-debuginfo-3.10.0-327.3.1.el7
kernel-headers-3.10.0-327.3.1.el7
kernel-devel-3.10.0-327.3.1.el7
kernel-tools-libs-devel-3.10.0-327.3.1.el7
kernel-debuginfo-3.10.0-327.3.1.el7
perf-debuginfo-3.10.0-327.3.1.el7
kernel-tools-libs-3.10.0-327.3.1.el7
perf-3.10.0-327.3.1.el7
python-perf-debuginfo-3.10.0-327.3.1.el7
kernel-debug-devel-3.10.0-327.3.1.el7
kernel-debuginfo-common-x86_64-3.10.0-327.3.1.el7
kernel-debug-3.10.0-327.3.1.el7
kernel-tools-debuginfo-3.10.0-327.3.1.el7

noarch

kernel-doc-3.10.0-327.3.1.el7
kernel-abi-whitelists-3.10.0-327.3.1.el7

174872 - Scientific Linux Security ERRATA Low: unbound on SL7.x x86_64 (1512-5249)

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

Risk Level: Medium

CVE: CVE-2014-8602

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: unbound on SL7.x x86_64 (1512-5249)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=5249>

SL7
x86_64
unbound-debuginfo-1.4.20-26.el7
unbound-libs-1.4.20-26.el7
unbound-python-1.4.20-26.el7
unbound-1.4.20-26.el7
unbound-devel-1.4.20-26.el7

174877 - Scientific Linux Security ERRATA Moderate: autofs on SL7.x x86_64 (1512-4175)

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

Risk Level: Medium

CVE: CVE-2014-8169

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: autofs on SL7.x x86_64 (1512-4175)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=4175>

SL7
x86_64
autofs-5.0.7-54.el7
autofs-debuginfo-5.0.7-54.el7

185085 - Ubuntu Linux 14.04 USN-2841-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7799, CVE-2015-7885, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
USN-2841-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003225.html>

Ubuntu 14.04

linux-image-3.13.0-73-powerpc-e500mc_3.13.0-73.116
linux-image-3.13.0-73-generic_3.13.0-73.116
linux-image-3.13.0-73-lowlatency_3.13.0-73.116
linux-image-3.13.0-73-powerpc-smp_3.13.0-73.116
linux-image-3.13.0-73-powerpc-e500_3.13.0-73.116
linux-image-3.13.0-73-generic-lpae_3.13.0-73.116
linux-image-3.13.0-73-powerpc64-smp_3.13.0-73.116
linux-image-3.13.0-73-powerpc64-emb_3.13.0-73.116

185090 - Ubuntu Linux 15.04 USN-2842-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7799, CVE-2015-7884, CVE-2015-7885, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
USN-2842-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003227.html>

Ubuntu 15.04

linux-image-3.19.0-41-generic-lpae_3.19.0-41.46
linux-image-3.19.0-41-powerpc-e500mc_3.19.0-41.46
linux-image-3.19.0-41-powerpc64-smp_3.19.0-41.46
linux-image-3.19.0-41-generic_3.19.0-41.46
linux-image-3.19.0-41-lowlatency_3.19.0-41.46
linux-image-3.19.0-41-powerpc-smp_3.19.0-41.46
linux-image-3.19.0-41-powerpc64-emb_3.19.0-41.46

185092 - Ubuntu Linux 12.04 USN-2840-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7872, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
USN-2840-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003224.html>

Ubuntu 12.04

linux-image-3.2.0-96-omap_3.2.0-96.136
linux-image-3.2.0-96-highbank_3.2.0-96.136

linux-image-3.2.0-96-powerpc-smp_3.2.0-96.136
linux-image-3.2.0-96-generic-pae_3.2.0-96.136
linux-image-3.2.0-96-generic_3.2.0-96.136
linux-image-3.2.0-96-powerpc64-smp_3.2.0-96.136
linux-image-3.2.0-96-virtual_3.2.0-96.136

185095 - Ubuntu Linux 15.10 USN-2843-3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7799, CVE-2015-7872, CVE-2015-7884, CVE-2015-7885

Description

The scan detected that the host is missing the following update:
USN-2843-3

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003232.html>

Ubuntu 15.10

linux-image-4.2.0-1016-raspi2_4.2.0-1016.23

185096 - Ubuntu Linux 14.04 USN-2842-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7799, CVE-2015-7884, CVE-2015-7885, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
USN-2842-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003228.html>

Ubuntu 14.04

linux-image-3.19.0-41-generic-lpae_3.19.0-41.46~14.04.2
linux-image-3.19.0-41-powerpc-e500mc_3.19.0-41.46~14.04.2
linux-image-3.19.0-41-powerpc-smp_3.19.0-41.46~14.04.2
linux-image-3.19.0-41-generic_3.19.0-41.46~14.04.2
linux-image-3.19.0-41-powerpc64-emb_3.19.0-41.46~14.04.2
linux-image-3.19.0-41-powerpc64-smp_3.19.0-41.46~14.04.2
linux-image-3.19.0-41-lowlatency_3.19.0-41.46~14.04.2

185098 - Ubuntu Linux 12.04 USN-2841-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7799, CVE-2015-7885, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
USN-2841-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003226.html>

Ubuntu 12.04

linux-image-3.13.0-73-generic_3.13.0-73.116~precise1
linux-image-3.13.0-73-generic-lpae_3.13.0-73.116~precise1

185099 - Ubuntu Linux 14.04 USN-2843-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7799, CVE-2015-7872, CVE-2015-7884, CVE-2015-7885, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
USN-2843-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003231.html>

Ubuntu 14.04

linux-image-4.2.0-21-powerpc64-emb_4.2.0-21.25~14.04.1
linux-image-4.2.0-21-powerpc-smp_4.2.0-21.25~14.04.1
linux-image-4.2.0-21-powerpc-e500mc_4.2.0-21.25~14.04.1
linux-image-4.2.0-21-generic_4.2.0-21.25~14.04.1
linux-image-4.2.0-21-lowlatency_4.2.0-21.25~14.04.1
linux-image-4.2.0-21-generic-lpae_4.2.0-21.25~14.04.1
linux-image-4.2.0-21-powerpc64-smp_4.2.0-21.25~14.04.1

185106 - Ubuntu Linux 15.10 USN-2843-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7799, CVE-2015-7872, CVE-2015-7884, CVE-2015-7885, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
USN-2843-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003229.html>

Ubuntu 15.10

linux-image-4.2.0-21-generic-lpae_4.2.0-21.25
linux-image-4.2.0-21-powerpc-smp_4.2.0-21.25
linux-image-4.2.0-21-powerpc64-smp_4.2.0-21.25
linux-image-4.2.0-21-lowlatency_4.2.0-21.25
linux-image-4.2.0-21-generic_4.2.0-21.25
linux-image-4.2.0-21-powerpc64-emb_4.2.0-21.25
linux-image-4.2.0-21-powerpc-e500mc_4.2.0-21.25

185107 - Ubuntu Linux 14.04 USN-2844-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7799, CVE-2015-7885, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
USN-2844-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003230.html>

Ubuntu 14.04

linux-image-3.16.0-56-lowlatency_3.16.0-56.75~14.04.1
linux-image-3.16.0-56-powerpc-e500mc_3.16.0-56.75~14.04.1
linux-image-3.16.0-56-generic-lpae_3.16.0-56.75~14.04.1
linux-image-3.16.0-56-powerpc64-emb_3.16.0-56.75~14.04.1
linux-image-3.16.0-56-powerpc64-smp_3.16.0-56.75~14.04.1
linux-image-3.16.0-56-powerpc-smp_3.16.0-56.75~14.04.1
linux-image-3.16.0-56-generic_3.16.0-56.75~14.04.1

33318 - Oracle Solaris 152249-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152249-01

Observation

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

<https://getupdates.oracle.com/readme/152249-01>

SunOS 5.10(x86): rsync Patch

SOLARIS_10_x86

SUNWrsync:11.10.0,REV=2011.10.26.08.35

33319 - Oracle Solaris 151913-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
151913-02

Observation

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

<https://getupdates.oracle.com/readme/151913-02>

SunOS 5.10(x86): OpenSSL 1.0.1 patch

SOLARIS_10_x86

SUNWopenssl-include:11.10.0,REV=2005.01.21.16.34

SUNWopensslr:11.10.0,REV=2005.01.21.16.34

SUNWopenssl-commands:11.10.0,REV=2005.01.21.16.34

SUNWopenssl-libraries:11.10.0,REV=2005.01.21.16.34

33320 - Oracle Solaris 152248-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152248-01

Observation

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

<https://getupdates.oracle.com/readme/152248-01>

SunOS 5.10: rsync Patch

SOLARIS_10

SUNWrsync:11.10.0,REV=2011.10.26.12.14

33321 - Oracle Solaris 151722-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
151722-01

Observation

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

<https://getupdates.oracle.com/readme/151722-01>

GNOME 2.6.0(x86): GDK-PixBuf library Patch

SOLARIS_10_x86

SUNWgnome-base-libs:2.6.0,REV=10.0.3.2004.12.16.15.19

33322 - Oracle Solaris 152251-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152251-01

Observation

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

<https://getupdates.oracle.com/readme/152251-01>

SunOS 5.10(x86): rsync Source Patch

SOLARIS_10_x86

SUNWrsyncS:11.10.0,REV=2011.10.26.08.35

33323 - Oracle Solaris 151912-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
151912-02

Observation

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

<https://getupdates.oracle.com/readme/151912-02>

SunOS 5.10: OpenSSL 1.0.1 patch

SOLARIS_10

SUNWopenssl-commands:11.10.0,REV=2005.01.21.15.53

SUNWopenssl-include:11.10.0,REV=2005.01.21.15.53

SUNWopensslr:11.10.0,REV=2005.01.21.15.53

SUNWopenssl-libraries:11.10.0,REV=2005.01.21.15.53

33324 - Oracle Solaris 152250-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
152250-01

Observation

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

<https://getupdates.oracle.com/readme/152250-01>

SunOS 5.10: rsync Source Patch

SOLARIS_10

SUNWrsyncS:11.10.0,REV=2011.10.26.12.14

33325 - Oracle Solaris 151721-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
151721-01

Observation

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

<https://getupdates.oracle.com/readme/151721-01>

GNOME 2.6.0: GDK-PixBuf library Patch

SOLARIS_10

SUNWgnome-base-libs:2.6.0,REV=10.0.3.2004.12.15.15.24

88729 - Slackware Linux 13.37, 14.0, 14.1 SSA:2015-356-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8612

Description

The scan detected that the host is missing the following update:
SSA:2015-356-01

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=2015&m=slackware-security.421085>

Slackware 14.0
x86_64
blueman-r708-x86_64-3

Slackware 14.1
x86_64
blueman-r708-x86_64-4

Slackware 13.37
x86_64
blueman-r708-x86_64-2

88730 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2015-351-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8540

Description

The scan detected that the host is missing the following update:
SSA:2015-351-02

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=2015&m=slackware-security.498464>

Slackware 14.0
x86_64
libpng-1.4.19-x86_64-1

Slackware 13.0
x86_64
libpng-1.2.56-x86_64-1

Slackware 13.1
x86_64
libpng-1.4.19-x86_64-1

Slackware 14.1
x86_64
libpng-1.4.19-x86_64-1

Slackware 13.37
x86_64
libpng-1.4.19-x86_64-1

130342 - Debian Linux 8.0 DSA-3425-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-0861

Description

The scan detected that the host is missing the following update:
DSA-3425-1

Observation

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

<http://www.debian.org/security/2015/dsa-3425>

Debian 8.0
all
tryton-server_3.4.0-3+deb8u1

130343 - Debian Linux 8.0 DSA-3424-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5343

Description

The scan detected that the host is missing the following update:
DSA-3424-1

Observation

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

<http://www.debian.org/security/2015/dsa-3424>

Debian 8.0
all
subversion_1.8.10-6+deb8u2

130344 - Debian Linux 7.0, 8.0 DSA-3427-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8612

Description

The scan detected that the host is missing the following update:
DSA-3427-1

Observation

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

<http://www.debian.org/security/2015/dsa-3427>

Debian 8.0

all

blueman_1.99~alpha1-1+deb8u1

Debian 7.0

all

blueman_1.23-1+deb7u1

174864 - Scientific Linux Security ERRATA Low: openhpi on SL7.x x86_64 (1512-8750)

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

Risk Level: Low

CVE: CVE-2015-3248

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: openhpi on SL7.x x86_64 (1512-8750)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=8750>

SL7

x86_64

openhpi-devel-3.4.0-2.el7

openhpi-debuginfo-3.4.0-2.el7

openhpi-3.4.0-2.el7

openhpi-libs-3.4.0-2.el7

174873 - Scientific Linux Security ERRATA Low: rest on SL7.x x86_64 (1512-15662)

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

Risk Level: Low

CVE: CVE-2015-2675

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: rest on SL7.x x86_64 (1512-15662)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=15662>

SL7
x86_64
rest-devel-0.7.92-3.el7
rest-debuginfo-0.7.92-3.el7
rest-0.7.92-3.el7

181718 - FreeBSD libsvg2 Denial Of Service Vulnerability (da634091-a84a-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-7557

Description

The scan detected that the host is missing the following update:
libsvg2 -- denial of service vulnerability (da634091-a84a-11e5-8f5c-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/da634091-a84a-11e5-8f5c-002590263bf5.html>

Affected packages:
libsvg2 < 2.40.7

181719 - FreeBSD Bugzilla Security Issues (54075861-a95a-11e5-8b40-20cf30e32f6d)

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

Risk Level: Low

CVE: CVE-2015-8508, CVE-2015-8509

Description

The scan detected that the host is missing the following update:
Bugzilla security issues (54075861-a95a-11e5-8b40-20cf30e32f6d)

Observation

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

<http://www.vuxml.org/freebsd/54075861-a95a-11e5-8b40-20cf30e32f6d.html>

Affected packages:
bugzilla44 < 4.4.11
bugzilla50 < 5.0.2

181720 - FreeBSD py-amf Input Sanitization Errors (1fbd6db1-a4e4-11e5-b864-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-8549

Description

The scan detected that the host is missing the following update:
py-amf -- input sanitization errors (1fbd6db1-a4e4-11e5-b864-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/1fbd6db1-a4e4-11e5-b864-14dae9d210b8.html>

Affected packages:

py27-amf < 0.8.0

py32-amf < 0.8.0

py33-amf < 0.8.0

py34-amf < 0.8.0

181721 - FreeBSD quassel Remote Denial Of Service (9e7306b9-a5c3-11e5-b864-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-8547

Description

The scan detected that the host is missing the following update:
quassel -- remote denial of service (9e7306b9-a5c3-11e5-b864-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/9e7306b9-a5c3-11e5-b864-14dae9d210b8.html>

Affected packages:

quassel < 0.12.2_1

181723 - FreeBSD cups-filters Code Execution (7329938b-a4e6-11e5-b864-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-8560

Description

The scan detected that the host is missing the following update:
cups-filters -- code execution (7329938b-a4e6-11e5-b864-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/7329938b-a4e6-11e5-b864-14dae9d210b8.html>

Affected packages:

cups-filters < 1.4.0

181724 - FreeBSD chromium Multiple Vulnerabilities (bb7d4791-a5bf-11e5-a0e5-00262d5ed8ee)

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

Risk Level: Low

CVE: CVE-2015-6792

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (bb7d4791-a5bf-11e5-a0e5-00262d5ed8ee)

Observation

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

<http://www.vuxml.org/freebsd/bb7d4791-a5bf-11e5-a0e5-00262d5ed8ee.html>

Affected packages:

chromium < 47.0.2526.106

chromium-npapi < 47.0.2526.106

chromium-pulse < 47.0.2526.106

181725 - FreeBSD libsvg2 Denial Of Service Vulnerability (d6c51737-a84b-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-7558

Description

The scan detected that the host is missing the following update:
libsvg2 -- denial of service vulnerability (d6c51737-a84b-11e5-8f5c-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/d6c51737-a84b-11e5-8f5c-002590263bf5.html>

Affected packages:

libsvg2 < 2.40.12

181726 - FreeBSD samba Multiple Vulnerabilities (ef434839-a6a4-11e5-8275-000c292e4fd8)

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

Risk Level: Low

CVE: CVE-2015-3223, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-5330, CVE-2015-7540, CVE-2015-8467

Description

The scan detected that the host is missing the following update:
samba -- multiple vulnerabilities (ef434839-a6a4-11e5-8275-000c292e4fd8)

Observation

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

<http://www.vuxml.org/freebsd/ef434839-a6a4-11e5-8275-000c292e4fd8.html>

Affected packages:

3.6.0 <= samba36 <= 3.6.25
4.0.0 <= samba4 <= 4.0.26
4.1.0 <= samba41 < 4.1.22
4.2.0 <= samba42 < 4.2.7
4.3.0 <= samba43 < 4.3.3
1.0.0 <= ldb < 1.1.24

181728 - FreeBSD libvirt ACL Bypass Using ../ To Access Beyond Storage Pool (f714b4c9-a6c1-11e5-88d7-047d7b492d07)

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

Risk Level: Low

CVE: CVE-2015-5313

Description

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

libvirt -- ACL bypass using ../ to access beyond storage pool (f714b4c9-a6c1-11e5-88d7-047d7b492d07)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/f714b4c9-a6c1-11e5-88d7-047d7b492d07.html>

Affected packages:

1.1.0 <= libvirt < 1.2.19_2
1.2.20 <= libvirt < 1.3.0

185086 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2838-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8560

Description

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

USN-2838-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003221.html>

Ubuntu 15.04

cups-filters_1.0.67-0ubuntu2.6

Ubuntu 15.10

cups-filters_1.0.76-1ubuntu0.2

Ubuntu 14.04

cups-filters_1.0.52-0ubuntu1.7

185087 - Ubuntu Linux 15.10 USN-2852-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-2852-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003241.html>

Ubuntu 15.10

linux-image-4.2.0-1017-raspi2_4.2.0-1017.24

185088 - Ubuntu Linux 14.04 USN-2839-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-2839-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003223.html>

Ubuntu 14.04

cups_1.7.2-0ubuntu1.7

185089 - Ubuntu Linux 15.04 USN-2850-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8551, CVE-2015-8552

Description

The scan detected that the host is missing the following update:
USN-2850-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003239.html>

Ubuntu 15.04

linux-image-3.19.0-42-lowlatency_3.19.0-42.48
linux-image-3.19.0-42-powerpc64-smp_3.19.0-42.48
linux-image-3.19.0-42-powerpc64-emb_3.19.0-42.48
linux-image-3.19.0-42-generic-lpae_3.19.0-42.48
linux-image-3.19.0-42-powerpc-smp_3.19.0-42.48
linux-image-3.19.0-42-generic_3.19.0-42.48
linux-image-3.19.0-42-powerpc-e500mc_3.19.0-42.48

185091 - Ubuntu Linux 12.04 USN-2847-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8551, CVE-2015-8552

Description

The scan detected that the host is missing the following update:
USN-2847-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003235.html>

Ubuntu 12.04

linux-image-3.13.0-74-generic_3.13.0-74.118~precise1
linux-image-3.13.0-74-generic-lpae_3.13.0-74.118~precise1

185094 - Ubuntu Linux 14.04 USN-2849-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8551, CVE-2015-8552

Description

The scan detected that the host is missing the following update:
USN-2849-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003238.html>

Ubuntu 14.04

linux-image-3.16.0-57-generic_3.16.0-57.77~14.04.1
linux-image-3.16.0-57-generic-lpae_3.16.0-57.77~14.04.1
linux-image-3.16.0-57-lowlatency_3.16.0-57.77~14.04.1
linux-image-3.16.0-57-powerpc64-smp_3.16.0-57.77~14.04.1
linux-image-3.16.0-57-powerpc64-emb_3.16.0-57.77~14.04.1
linux-image-3.16.0-57-powerpc-e500mc_3.16.0-57.77~14.04.1
linux-image-3.16.0-57-powerpc-smp_3.16.0-57.77~14.04.1

185097 - Ubuntu Linux 14.04 USN-2848-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8551, CVE-2015-8552

Description

The scan detected that the host is missing the following update:
USN-2848-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003237.html>

Ubuntu 14.04

linux-image-3.13.0-74-generic-lpae_3.13.0-74.118
linux-image-3.13.0-74-powerpc64-smp_3.13.0-74.118
linux-image-3.13.0-74-generic_3.13.0-74.118
linux-image-3.13.0-74-powerpc64-emb_3.13.0-74.118
linux-image-3.13.0-74-powerpc-e500mc_3.13.0-74.118
linux-image-3.13.0-74-powerpc-smp_3.13.0-74.118
linux-image-3.13.0-74-powerpc-e500_3.13.0-74.118
linux-image-3.13.0-74-lowlatency_3.13.0-74.118

185100 - Ubuntu Linux 14.04 USN-2853-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8551, CVE-2015-8552

Description

The scan detected that the host is missing the following update:
USN-2853-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003242.html>

Ubuntu 14.04

linux-image-4.2.0-22-powerpc64-smp_4.2.0-22.27~14.04.1
linux-image-4.2.0-22-lowlatency_4.2.0-22.27~14.04.1
linux-image-4.2.0-22-powerpc-e500mc_4.2.0-22.27~14.04.1

linux-image-4.2.0-22-powerpc-smp_4.2.0-22.27~14.04.1
linux-image-4.2.0-22-generic-lpae_4.2.0-22.27~14.04.1
linux-image-4.2.0-22-powerpc64-emb_4.2.0-22.27~14.04.1
linux-image-4.2.0-22-generic_4.2.0-22.27~14.04.1

185101 - Ubuntu Linux 14.04 USN-2854-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8551, CVE-2015-8552

Description

The scan detected that the host is missing the following update:
USN-2854-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003243.html>

Ubuntu 14.04

linux-image-3.19.0-42-powerpc-smp_3.19.0-42.48~14.04.1
linux-image-3.19.0-42-lowlatency_3.19.0-42.48~14.04.1
linux-image-3.19.0-42-generic-lpae_3.19.0-42.48~14.04.1
linux-image-3.19.0-42-powerpc64-smp_3.19.0-42.48~14.04.1
linux-image-3.19.0-42-powerpc-e500mc_3.19.0-42.48~14.04.1
linux-image-3.19.0-42-generic_3.19.0-42.48~14.04.1
linux-image-3.19.0-42-powerpc64-emb_3.19.0-42.48~14.04.1

185102 - Ubuntu Linux 12.04 USN-2846-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8551, CVE-2015-8552

Description

The scan detected that the host is missing the following update:
USN-2846-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003236.html>

Ubuntu 12.04

linux-image-3.2.0-97-generic-pae_3.2.0-97.137
linux-image-3.2.0-97-virtual_3.2.0-97.137
linux-image-3.2.0-97-highbank_3.2.0-97.137
linux-image-3.2.0-97-powerpc64-smp_3.2.0-97.137
linux-image-3.2.0-97-powerpc-smp_3.2.0-97.137
linux-image-3.2.0-97-omap_3.2.0-97.137
linux-image-3.2.0-97-generic_3.2.0-97.137

185103 - Ubuntu Linux 15.10 USN-2851-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8551, CVE-2015-8552

Description

The scan detected that the host is missing the following update:
USN-2851-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003240.html>

Ubuntu 15.10

linux-image-4.2.0-22-powerpc-smp_4.2.0-22.27

linux-image-4.2.0-22-generic_4.2.0-22.27

linux-image-4.2.0-22-powerpc64-emb_4.2.0-22.27

linux-image-4.2.0-22-powerpc64-smp_4.2.0-22.27

linux-image-4.2.0-22-powerpc-e500mc_4.2.0-22.27

linux-image-4.2.0-22-lowlatency_4.2.0-22.27

linux-image-4.2.0-22-generic-lpae_4.2.0-22.27

185104 - Ubuntu Linux 12.04 USN-2838-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8560

Description

The scan detected that the host is missing the following update:
USN-2838-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003222.html>

Ubuntu 12.04

foomatic-filters_4.0.16-0ubuntu0.4

190103 - Fedora Linux 23 FEDORA-2015-51b1105902 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-2015-51b1105902

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174083.html>

Fedora Core 23

firefox-43.0-1.fc23

190105 - Fedora Linux 22 FEDORA-2015-7ab3d3afcf 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-2015-7ab3d3afcf

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174253.html>

Fedora Core 22

firefox-43.0-1.fc22

190107 - Fedora Linux 22 FEDORA-2015-020f4b9400 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-2015-020f4b9400

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174199.html>

Fedora Core 22

xsuplicant-2.2.0-13.fc22

190108 - Fedora Linux 22 FEDORA-2015-af140eefbc Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5330

Description

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

FEDORA-2015-af140eefbc

Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174116.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174119.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174117.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174118.html>

Fedora Core 22

libtdb-1.3.8-1.fc22

libtevent-0.9.26-1.fc22

libtalloc-2.1.5-2.fc22

libldb-1.1.24-1.fc22

190110 - Fedora Linux 23 FEDORA-2015-a108c34086 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8560

Description

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

FEDORA-2015-a108c34086

Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174153.html>

Fedora Core 23

cups-filters-1.4.0-1.fc23

190111 - Fedora Linux 23 FEDORA-2015-c59710b05d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-7446, CVE-2015-7550, CVE-2015-8543

Description

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

FEDORA-2015-c59710b05d

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174290.html>

Fedora Core 23

kernel-4.2.8-300.fc23

190112 - Fedora Linux 23 FEDORA-2015-d8253e2b1d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8550, CVE-2015-8554, CVE-2015-8555

Description

The scan detected that the host is missing the following update:
FEDORA-2015-d8253e2b1d

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174288.html>

Fedora Core 23

xen-4.5.2-6.fc23

190116 - Fedora Linux 23 FEDORA-2015-7229638357 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-2015-7229638357

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174175.html>

Fedora Core 23

xsupplicant-2.2.0-13.fc23

190117 - Fedora Linux 23 FEDORA-2015-2773b85b49 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7504, CVE-2015-7512, CVE-2015-8345

Description

The scan detected that the host is missing the following update:
FEDORA-2015-2773b85b49

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174026.html>

Fedora Core 23

qemu-2.4.1-2.fc23

190119 - Fedora Linux 23 FEDORA-2015-afdb0e8aaa Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5259, CVE-2015-5343

Description

The scan detected that the host is missing the following update:
FEDORA-2015-afdb0e8aaa

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174293.html>

Fedora Core 23

subversion-1.9.3-1.fc23

190120 - Fedora Linux 23 FEDORA-2015-b36076d32e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3223, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-7540

Description

The scan detected that the host is missing the following update:
FEDORA-2015-b36076d32e

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174076.html>

Fedora Core 23

samba-4.3.3-0.fc23

190124 - Fedora Linux 22 FEDORA-2015-c1c2f5e168 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-7446, CVE-2015-7550, CVE-2015-8543

Description

The scan detected that the host is missing the following update:
FEDORA-2015-c1c2f5e168

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174249.html>

Fedora Core 22

kernel-4.2.8-200.fc22

190125 - Fedora Linux 23 FEDORA-2015-b960ca78bf Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5330

Description

The scan detected that the host is missing the following update:
FEDORA-2015-b960ca78bf

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174077.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174080.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174079.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174078.html>

Fedora Core 23

libtevent-0.9.26-1.fc23

libtalloc-2.1.5-2.fc23

libldb-1.1.24-1.fc23

libtdb-1.3.8-1.fc23

174842 - Scientific Linux Security ERRATA Moderate: squid on SL7.x x86_64 (1512-15001)

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

Risk Level: Low

CVE: CVE-2015-3455

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: squid on SL7.x x86_64 (1512-15001)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=15001>

SL7
x86_64
squid-3.3.8-26.el7
squid-debuginfo-3.3.8-26.el7
squid-sysvinit-3.3.8-26.el7

174854 - Scientific Linux Security ERRATA Low: grep on SL7.x x86_64 (1512-12713)

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

Risk Level: Low

CVE: CVE-2015-1345

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: grep on SL7.x x86_64 (1512-12713)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=12713>

SL7
x86_64
grep-2.20-2.el7
grep-debuginfo-2.20-2.el7

174869 - Scientific Linux Security ERRATA Low: grub2 on SL7.x x86_64 (1512-5960)

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

Risk Level: Low

CVE: CVE-2015-5281

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: grub2 on SL7.x x86_64 (1512-5960)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=5960>

SL7
x86_64
grub2-efi-2.02-0.29.el7

grub2-debuginfo-2.02-0.29.el7
grub2-tools-2.02-0.29.el7
grub2-efi-modules-2.02-0.29.el7
grub2-2.02-0.29.el7

185105 - Ubuntu Linux 12.04 USN-2840-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7872

Description

The scan detected that the host is missing the following update:
USN-2840-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003233.html>

Ubuntu 12.04

linux-image-3.2.0-1475-omap4_3.2.0-1475.97

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.

19134 - (APSB15-24) Vulnerabilities In Adobe Reader And Acrobat

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

Risk Level: High

CVE: CVE-2015-5583, CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6685, CVE-2015-6686, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-6692, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, CVE-2015-6696, CVE-2015-6697, CVE-2015-6698, CVE-2015-6699, CVE-2015-6700, CVE-2015-6701, CVE-2015-6702, CVE-2015-6703, CVE-2015-6704, CVE-2015-6705, CVE-2015-6706, CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7615, CVE-2015-7616, CVE-2015-7617, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, CVE-2015-7621, CVE-2015-7622, CVE-2015-7623, CVE-2015-7624, CVE-2015-8458

Update Details

CVE is updated

33058 - Oracle Solaris 148076-16 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33307 - Oracle Solaris 151934-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

181517 - FreeBSD php-phar Multiple Vulnerabilities (8b1f53f3-2da5-11e5-86ff-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-5589, CVE-2015-5590

Update Details

FASLScript is updated

14393 - Microsoft Internet Explorer Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14460 - Adobe Reader Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

45001 - ShellInitialize.fasl3

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

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.

Copyright 2015 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates