

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

22622 - Oracle Java SE Critical Patch Update October 2017

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2016-9841, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10293, CVE-2017-10295, CVE-2017-10309, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

Multiple vulnerabilities are present in some versions of Oracle Java SE.

Observation

Oracle Java SE is used to run Java applications.

Multiple vulnerabilities are present in some versions of Oracle Java SE. The flaws lie in multiple components. Successful exploitation could allow an attacker to gain elevated privileges and or affect confidentiality, integrity and availability of the target system.

132404 - Oracle VM OVMSA-2017-0153 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10013, CVE-2016-10024, CVE-2016-7777, CVE-2016-9379, CVE-2016-9380, CVE-2016-9382, CVE-2016-9383, CVE-2016-9385, CVE-2016-9386, CVE-2016-9603, CVE-2017-10912, CVE-2017-10913, CVE-2017-10914, CVE-2017-10915, CVE-2017-10917, CVE-2017-10918, CVE-2017-10920, CVE-2017-10921, CVE-2017-10922, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855, CVE-2017-14316, CVE-2017-14317, CVE-2017-14319, CVE-2017-2615, CVE-2017-2620, CVE-2017-7228, CVE-2017-8903, CVE-2017-8904, CVE-2017-8905

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0153

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-October/000786.html>

OVM3.4
x86_64
xen-tools-4.4.4-105.0.24.el6
xen-4.4.4-105.0.24.el6

141746 - Red Hat Enterprise Linux RHSA-2017-2899 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11292

Description

The scan detected that the host is missing the following update:
RHSA-2017-2899

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-October/msg00015.html>

RHEL6D
x86_64
flash-plugin-27.0.0.170-1.el6_9

i386
flash-plugin-27.0.0.170-1.el6_9

RHEL6S
x86_64
flash-plugin-27.0.0.170-1.el6_9

i386
flash-plugin-27.0.0.170-1.el6_9

RHEL6WS
x86_64
flash-plugin-27.0.0.170-1.el6_9

i386
flash-plugin-27.0.0.170-1.el6_9

145985 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:2747-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14867

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2747-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-October/003301.html>

SuSE SLES 12 SP3
x86_64
git-debugsource-2.12.3-27.9.1

git-core-debuginfo-2.12.3-27.9.1
git-core-2.12.3-27.9.1

SuSE SLES 12 SP2
noarch
git-doc-2.12.3-27.9.1

x86_64
git-debugsource-2.12.3-27.9.1
git-core-debuginfo-2.12.3-27.9.1
git-core-2.12.3-27.9.1

178524 - Gentoo Linux GLSA-201710-14 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7006, CVE-2017-7011, CVE-2017-7012, CVE-2017-7018, CVE-2017-7019, CVE-2017-7020, CVE-2017-7030, CVE-2017-7034, CVE-2017-7037, CVE-2017-7038, CVE-2017-7039, CVE-2017-7040, CVE-2017-7041, CVE-2017-7042, CVE-2017-7043

Description

The scan detected that the host is missing the following update:
GLSA-201710-14

Observation

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

<https://security.gentoo.org/glsa/201710-14>

Affected packages:
net-libs/webkit-gtk < 2.16.6

22604 - Wireshark Multiple Vulnerabilities Prior To 2.2.10

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

Risk Level: High

CVE: CVE-2017-15191, CVE-2017-15192, CVE-2017-15193

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

130908 - Debian Linux 9.0 DSA-3996-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14054, CVE-2017-14055, CVE-2017-14056, CVE-2017-14057, CVE-2017-14058, CVE-2017-14059, CVE-2017-14169, CVE-2017-14170, CVE-2017-14171, CVE-2017-14222, CVE-2017-14223, CVE-2017-14225, CVE-2017-14767

Description

The scan detected that the host is missing the following update:
DSA-3996-1

Observation

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

<http://www.debian.org/security/2017/dsa-3996>

Debian 9.0
all
ffmpeg_7:3.2.8-1~deb9u1

130909 - Debian Linux 8.0, 9.0 DSA-3997-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14718, CVE-2017-14719, CVE-2017-14720, CVE-2017-14721, CVE-2017-14722, CVE-2017-14723, CVE-2017-14724, CVE-2017-14725, CVE-2017-14726, CVE-2017-14990

Description

The scan detected that the host is missing the following update:
DSA-3997-1

Observation

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

<http://www.debian.org/security/2017/dsa-3997>

Debian 8.0
all
wordpress_4.1+dfsg-1+deb8u15

Debian 9.0
all
wordpress_4.7.5+dfsg-2+deb9u1

141745 - Red Hat Enterprise Linux RHSA-2017-2886 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5483, CVE-2016-6664, CVE-2016-8327, CVE-2017-3238, CVE-2017-3244, CVE-2017-3251, CVE-2017-3256, CVE-2017-3257, CVE-2017-3258, CVE-2017-3273, CVE-2017-3291, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3319, CVE-2017-3320, CVE-2017-3331, CVE-2017-3450, CVE-2017-3453, CVE-2017-3454, CVE-2017-3455, CVE-2017-3456, CVE-2017-3457, CVE-2017-3458, CVE-2017-3459, CVE-2017-3460, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3465, CVE-2017-3467, CVE-2017-3468, CVE-2017-3529, CVE-2017-3599, CVE-2017-3600, CVE-2017-3633, CVE-2017-3634, CVE-2017-3637, CVE-2017-3638, CVE-2017-3639, CVE-2017-3640, CVE-2017-3641, CVE-2017-3642, CVE-2017-3643, CVE-2017-3644, CVE-2017-3645, CVE-2017-3646, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3650, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Description

The scan detected that the host is missing the following update:
RHSA-2017-2886

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-October/msg00012.html>

RHEL6_7S

x86_64

rh-mysql57-mysql-common-5.7.19-6.el6
rh-mysql57-mysql-config-5.7.19-6.el6
rh-mysql57-mysql-test-5.7.19-6.el6
rh-mysql57-mysql-server-5.7.19-6.el6
rh-mysql57-mysql-debuginfo-5.7.19-6.el6
rh-mysql57-mysql-5.7.19-6.el6
rh-mysql57-mysql-devel-5.7.19-6.el6
rh-mysql57-mysql-errmsg-5.7.19-6.el6

RHEL6S

x86_64

rh-mysql57-mysql-common-5.7.19-6.el6
rh-mysql57-mysql-config-5.7.19-6.el6
rh-mysql57-mysql-test-5.7.19-6.el6
rh-mysql57-mysql-server-5.7.19-6.el6
rh-mysql57-mysql-debuginfo-5.7.19-6.el6
rh-mysql57-mysql-5.7.19-6.el6
rh-mysql57-mysql-devel-5.7.19-6.el6
rh-mysql57-mysql-errmsg-5.7.19-6.el6

RHEL6WS

x86_64

rh-mysql57-mysql-common-5.7.19-6.el6
rh-mysql57-mysql-config-5.7.19-6.el6
rh-mysql57-mysql-test-5.7.19-6.el6
rh-mysql57-mysql-server-5.7.19-6.el6
rh-mysql57-mysql-debuginfo-5.7.19-6.el6
rh-mysql57-mysql-5.7.19-6.el6
rh-mysql57-mysql-devel-5.7.19-6.el6
rh-mysql57-mysql-errmsg-5.7.19-6.el6

RHEL7S

x86_64

rh-mysql57-mysql-errmsg-5.7.19-6.el7
rh-mysql57-mysql-test-5.7.19-6.el7
rh-mysql57-mysql-server-5.7.19-6.el7
rh-mysql57-mysql-config-5.7.19-6.el7
rh-mysql57-mysql-debuginfo-5.7.19-6.el7
rh-mysql57-mysql-devel-5.7.19-6.el7
rh-mysql57-mysql-5.7.19-6.el7
rh-mysql57-mysql-common-5.7.19-6.el7

RHEL7WS

x86_64

rh-mysql57-mysql-errmsg-5.7.19-6.el7
rh-mysql57-mysql-test-5.7.19-6.el7
rh-mysql57-mysql-server-5.7.19-6.el7
rh-mysql57-mysql-config-5.7.19-6.el7
rh-mysql57-mysql-debuginfo-5.7.19-6.el7
rh-mysql57-mysql-devel-5.7.19-6.el7
rh-mysql57-mysql-5.7.19-6.el7

141748 - Red Hat Enterprise Linux RHSA-2017-2885 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7793, CVE-2017-7810, CVE-2017-7814, CVE-2017-7818, CVE-2017-7819, CVE-2017-7823, CVE-2017-7824

Description

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

RHSA-2017-2885

Observation

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

For more information see:

<http://www.redhat.com/archives/rhlsa-announce/2017-October/msg00011.html>

RHEL7S

x86_64

thunderbird-debuginfo-52.4.0-2.el7_4

thunderbird-52.4.0-2.el7_4

RHEL6S

i386

thunderbird-debuginfo-52.4.0-2.el6_9

thunderbird-52.4.0-2.el6_9

x86_64

thunderbird-debuginfo-52.4.0-2.el6_9

thunderbird-52.4.0-2.el6_9

RHEL6WS

x86_64

thunderbird-debuginfo-52.4.0-2.el6_9

thunderbird-52.4.0-2.el6_9

i386

thunderbird-debuginfo-52.4.0-2.el6_9

thunderbird-52.4.0-2.el6_9

RHEL7D

x86_64

thunderbird-debuginfo-52.4.0-2.el7_4

thunderbird-52.4.0-2.el7_4

RHEL6D

x86_64

thunderbird-debuginfo-52.4.0-2.el6_9

thunderbird-52.4.0-2.el6_9

i386

thunderbird-debuginfo-52.4.0-2.el6_9

thunderbird-52.4.0-2.el6_9

RHEL7WS

x86_64

thunderbird-debuginfo-52.4.0-2.el7_4

145982 - SuSE SLES 11 SP4 SUSE-SU-2017:2749-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2749-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-October/003302.html>

SuSE SLES 11 SP4

noarch

xerces-j2-2.8.1-238.29.5.2

xerces-j2-xml-apis-2.8.1-238.29.5.2

xerces-j2-xml-resolver-2.8.1-238.29.5.2

145983 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2744-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2744-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-October/003299.html>

SuSE SLES 12 SP2

noarch

xerces-j2-xml-apis-2.8.1-268.6.2

xerces-j2-xml-resolver-2.8.1-268.6.2

xerces-j2-2.8.1-268.6.2

SuSE SLED 12 SP3

noarch

xerces-j2-2.8.1-268.6.2

SuSE SLED 12 SP2

noarch

xerces-j2-2.8.1-268.6.2

SuSE SLES 12 SP3

noarch

xerces-j2-xml-apis-2.8.1-268.6.2
xerces-j2-xml-resolver-2.8.1-268.6.2
xerces-j2-2.8.1-268.6.2

145984 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2745-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13087, CVE-2017-13088

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2745-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-October/003300.html>

SuSE SLES 12 SP2

x86_64
wpa_supplicant-debuginfo-2.2-15.3.1
wpa_supplicant-2.2-15.3.1
wpa_supplicant-debugsource-2.2-15.3.1

SuSE SLED 12 SP3

x86_64
wpa_supplicant-debuginfo-2.2-15.3.1
wpa_supplicant-2.2-15.3.1
wpa_supplicant-debugsource-2.2-15.3.1

SuSE SLED 12 SP2

x86_64
wpa_supplicant-debuginfo-2.2-15.3.1
wpa_supplicant-2.2-15.3.1
wpa_supplicant-debugsource-2.2-15.3.1

SuSE SLES 12 SP3

x86_64
wpa_supplicant-debuginfo-2.2-15.3.1
wpa_supplicant-2.2-15.3.1
wpa_supplicant-debugsource-2.2-15.3.1

145986 - SuSE Linux 42.2 openSUSE-SU-2017:2708-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2708-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00037.html>

SuSE Linux 42.2

x86_64

libvirt-daemon-driver-storage-2.0.0-13.9.1
libvirt-daemon-debuginfo-2.0.0-13.9.1
libvirt-client-debuginfo-32bit-2.0.0-13.9.1
libvirt-daemon-driver-nwfilter-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-libxl-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-secret-debuginfo-2.0.0-13.9.1
libvirt-nss-2.0.0-13.9.1
libvirt-devel-2.0.0-13.9.1
libvirt-doc-2.0.0-13.9.1
libvirt-daemon-driver-interface-2.0.0-13.9.1
libvirt-debugsource-2.0.0-13.9.1
libvirt-daemon-driver-network-2.0.0-13.9.1
libvirt-daemon-qemu-2.0.0-13.9.1
libvirt-nss-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-nodedev-2.0.0-13.9.1
libvirt-2.0.0-13.9.1
libvirt-daemon-driver-uml-2.0.0-13.9.1
libvirt-daemon-config-nwfilter-2.0.0-13.9.1
libvirt-daemon-driver-qemu-debuginfo-2.0.0-13.9.1
libvirt-daemon-config-network-2.0.0-13.9.1
libvirt-daemon-driver-storage-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-lxc-2.0.0-13.9.1
libvirt-lock-sanlock-2.0.0-13.9.1
libvirt-daemon-vbox-2.0.0-13.9.1
libvirt-client-debuginfo-2.0.0-13.9.1
libvirt-daemon-lxc-2.0.0-13.9.1
libvirt-daemon-driver-nodedev-debuginfo-2.0.0-13.9.1
libvirt-lock-sanlock-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-vbox-debuginfo-2.0.0-13.9.1
libvirt-devel-32bit-2.0.0-13.9.1
libvirt-daemon-driver-lxc-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-vbox-2.0.0-13.9.1
libvirt-daemon-driver-nwfilter-2.0.0-13.9.1
libvirt-daemon-uml-2.0.0-13.9.1
libvirt-client-32bit-2.0.0-13.9.1
libvirt-daemon-xen-2.0.0-13.9.1
libvirt-daemon-driver-interface-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-network-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-secret-2.0.0-13.9.1
libvirt-client-2.0.0-13.9.1
libvirt-daemon-driver-libxl-2.0.0-13.9.1
libvirt-daemon-driver-qemu-2.0.0-13.9.1
libvirt-daemon-2.0.0-13.9.1
libvirt-daemon-driver-uml-debuginfo-2.0.0-13.9.1

i586

libvirt-daemon-driver-storage-2.0.0-13.9.1
libvirt-daemon-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-nwfilter-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-secret-debuginfo-2.0.0-13.9.1
libvirt-nss-2.0.0-13.9.1
libvirt-devel-2.0.0-13.9.1
libvirt-doc-2.0.0-13.9.1
libvirt-daemon-driver-interface-2.0.0-13.9.1

libvirt-debugsource-2.0.0-13.9.1
libvirt-daemon-driver-network-2.0.0-13.9.1
libvirt-daemon-qemu-2.0.0-13.9.1
libvirt-nss-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-nodedev-2.0.0-13.9.1
libvirt-2.0.0-13.9.1
libvirt-daemon-driver-uml-2.0.0-13.9.1
libvirt-daemon-config-nwfilter-2.0.0-13.9.1
libvirt-daemon-driver-qemu-debuginfo-2.0.0-13.9.1
libvirt-daemon-config-network-2.0.0-13.9.1
libvirt-daemon-driver-storage-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-lxc-2.0.0-13.9.1
libvirt-lock-sanlock-2.0.0-13.9.1
libvirt-daemon-vbox-2.0.0-13.9.1
libvirt-client-debuginfo-2.0.0-13.9.1
libvirt-daemon-lxc-2.0.0-13.9.1
libvirt-daemon-driver-nodedev-debuginfo-2.0.0-13.9.1
libvirt-lock-sanlock-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-vbox-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-lxc-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-vbox-2.0.0-13.9.1
libvirt-daemon-driver-nwfilter-2.0.0-13.9.1
libvirt-daemon-uml-2.0.0-13.9.1
libvirt-daemon-driver-interface-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-network-debuginfo-2.0.0-13.9.1
libvirt-daemon-driver-secret-2.0.0-13.9.1
libvirt-client-2.0.0-13.9.1
libvirt-daemon-driver-qemu-2.0.0-13.9.1
libvirt-daemon-2.0.0-13.9.1
libvirt-daemon-driver-uml-debuginfo-2.0.0-13.9.1

145988 - SuSE SLES 11 SP4 SUSE-SU-2017:2752-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13087, CVE-2017-13088

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2752-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-October/003304.html>

SuSE SLES 11 SP4

i586

wpa_supplicant-0.7.1-6.18.3.1

x86_64

wpa_supplicant-0.7.1-6.18.3.1

145990 - SuSE Linux 42.2 openSUSE-SU-2017:2713-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12150, CVE-2017-12151, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2713-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00042.html>

SuSE Linux 42.2

i586

libnetapi-devel-4.4.2-11.12.1
libdcerpc-samr-devel-4.4.2-11.12.1
samba-winbind-debuginfo-4.4.2-11.12.1
samba-test-4.4.2-11.12.1
libsamba-credentials-devel-4.4.2-11.12.1
libsamba-hostconfig-devel-4.4.2-11.12.1
libsmbldap-devel-4.4.2-11.12.1
libsamba-errors0-debuginfo-4.4.2-11.12.1
libndr-nbt-devel-4.4.2-11.12.1
libsamba-hostconfig0-4.4.2-11.12.1
libndr0-4.4.2-11.12.1
libdcerpc-samr0-4.4.2-11.12.1
samba-debuginfo-4.4.2-11.12.1
libndr-standard0-debuginfo-4.4.2-11.12.1
libsamba-passdb-devel-4.4.2-11.12.1
libsmbclient0-debuginfo-4.4.2-11.12.1
libsamba-policy0-debuginfo-4.4.2-11.12.1
samba-pidl-4.4.2-11.12.1
samba-python-debuginfo-4.4.2-11.12.1
samba-core-devel-4.4.2-11.12.1
libsamba-util0-debuginfo-4.4.2-11.12.1
libsamba-hostconfig0-debuginfo-4.4.2-11.12.1
libtevent-util0-4.4.2-11.12.1
ctdb-tests-4.4.2-11.12.1
samba-winbind-4.4.2-11.12.1
libsmbconf0-4.4.2-11.12.1
libsamdb0-4.4.2-11.12.1
libndr-krb5pac0-4.4.2-11.12.1
libwbclient0-4.4.2-11.12.1
samba-client-debuginfo-4.4.2-11.12.1
ctdb-debuginfo-4.4.2-11.12.1
libsamba-credentials0-4.4.2-11.12.1
libsmbclient0-4.4.2-11.12.1
libtevent-util0-debuginfo-4.4.2-11.12.1
libtevent-util-devel-4.4.2-11.12.1
libndr-nbt0-4.4.2-11.12.1
libndr-krb5pac0-debuginfo-4.4.2-11.12.1
libsamba-errors0-4.4.2-11.12.1
libdcerpc-samr0-debuginfo-4.4.2-11.12.1
libnetapi0-4.4.2-11.12.1
libsamba-policy-devel-4.4.2-11.12.1
libwbclient-devel-4.4.2-11.12.1
samba-libs-4.4.2-11.12.1
libsmbldap0-debuginfo-4.4.2-11.12.1

libdcerpc-binding0-debuginfo-4.4.2-11.12.1
libsamba-credentials0-debuginfo-4.4.2-11.12.1
libsamba-util0-4.4.2-11.12.1
ctdb-4.4.2-11.12.1
libsamba-policy0-4.4.2-11.12.1
libsamba-passdb0-debuginfo-4.4.2-11.12.1
libsmbldap0-4.4.2-11.12.1
libsamba-passdb0-4.4.2-11.12.1
libndr0-debuginfo-4.4.2-11.12.1
samba-debugsource-4.4.2-11.12.1
samba-python-4.4.2-11.12.1
libsmbclient-devel-4.4.2-11.12.1
libdcerpc0-4.4.2-11.12.1
libndr-nbt0-debuginfo-4.4.2-11.12.1
libwbclient0-debuginfo-4.4.2-11.12.1
libndr-standard0-4.4.2-11.12.1
ctdb-tests-debuginfo-4.4.2-11.12.1
libndr-devel-4.4.2-11.12.1
libsmbconf-devel-4.4.2-11.12.1
libsmbconf0-debuginfo-4.4.2-11.12.1
libdcerpc-devel-4.4.2-11.12.1
libndr-standard-devel-4.4.2-11.12.1
samba-client-4.4.2-11.12.1
libsamba-util-devel-4.4.2-11.12.1
samba-test-debuginfo-4.4.2-11.12.1
libsamba-errors-devel-4.4.2-11.12.1
samba-libs-debuginfo-4.4.2-11.12.1
libdcerpc-binding0-4.4.2-11.12.1
libndr-krb5pac-devel-4.4.2-11.12.1
libsamdb-devel-4.4.2-11.12.1
libdcerpc0-debuginfo-4.4.2-11.12.1
libsamdb0-debuginfo-4.4.2-11.12.1
samba-4.4.2-11.12.1
libnetapi0-debuginfo-4.4.2-11.12.1

noarch
samba-doc-4.4.2-11.12.1

x86_64
libsamba-credentials0-debuginfo-32bit-4.4.2-11.12.1
libsamba-credentials0-32bit-4.4.2-11.12.1
libnetapi-devel-4.4.2-11.12.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-11.12.1
libdcerpc-samr-devel-4.4.2-11.12.1
samba-winbind-debuginfo-4.4.2-11.12.1
samba-test-4.4.2-11.12.1
libsamba-credentials-devel-4.4.2-11.12.1
libsamba-hostconfig-devel-4.4.2-11.12.1
libsmbldap-devel-4.4.2-11.12.1
samba-winbind-32bit-4.4.2-11.12.1
libsamba-errors0-debuginfo-4.4.2-11.12.1
libndr-nbt-devel-4.4.2-11.12.1
libsamba-hostconfig0-4.4.2-11.12.1
libsmbldap0-32bit-4.4.2-11.12.1
libndr-standard0-32bit-4.4.2-11.12.1
libndr-standard0-debuginfo-32bit-4.4.2-11.12.1
libndr0-4.4.2-11.12.1
libsamba-hostconfig0-debuginfo-32bit-4.4.2-11.12.1
libndr0-32bit-4.4.2-11.12.1
libsamba-passdb0-32bit-4.4.2-11.12.1

libndr-krb5pac0-32bit-4.4.2-11.12.1
libsamba-passdb0-debuginfo-32bit-4.4.2-11.12.1
libwbclient0-debuginfo-32bit-4.4.2-11.12.1
libdcerpc-samr0-4.4.2-11.12.1
samba-debuginfo-4.4.2-11.12.1
libndr-standard0-debuginfo-4.4.2-11.12.1
libsamba-passdb-devel-4.4.2-11.12.1
libsmbclient0-debuginfo-4.4.2-11.12.1
libsamba-policy0-debuginfo-4.4.2-11.12.1
samba-pidl-4.4.2-11.12.1
libndr0-debuginfo-32bit-4.4.2-11.12.1
samba-python-debuginfo-4.4.2-11.12.1
samba-core-devel-4.4.2-11.12.1
libsamba-util0-debuginfo-4.4.2-11.12.1
libtevent-util0-32bit-4.4.2-11.12.1
libsamba-hostconfig0-debuginfo-4.4.2-11.12.1
libnetapi0-32bit-4.4.2-11.12.1
libdcerpc-samr0-32bit-4.4.2-11.12.1
libtevent-util0-4.4.2-11.12.1
ctdb-tests-4.4.2-11.12.1
samba-winbind-debuginfo-32bit-4.4.2-11.12.1
samba-winbind-4.4.2-11.12.1
libsmbconf0-4.4.2-11.12.1
libsamdb0-4.4.2-11.12.1
libndr-krb5pac0-4.4.2-11.12.1
libwbclient0-4.4.2-11.12.1
samba-client-debuginfo-4.4.2-11.12.1
ctdb-debuginfo-4.4.2-11.12.1
libsamba-credentials0-4.4.2-11.12.1
libdcerpc0-32bit-4.4.2-11.12.1
libsmbclient0-4.4.2-11.12.1
libsmbclient0-32bit-4.4.2-11.12.1
libtevent-util0-debuginfo-4.4.2-11.12.1
libtevent-util-devel-4.4.2-11.12.1
libndr-nbt0-4.4.2-11.12.1
libsamdb0-32bit-4.4.2-11.12.1
libndr-krb5pac0-debuginfo-4.4.2-11.12.1
libsamba-errors0-4.4.2-11.12.1
libdcerpc-samr0-debuginfo-4.4.2-11.12.1
libtevent-util0-debuginfo-32bit-4.4.2-11.12.1
libnetapi0-4.4.2-11.12.1
libsamba-policy-devel-4.4.2-11.12.1
libwbclient-devel-4.4.2-11.12.1
samba-libs-4.4.2-11.12.1
libwbclient0-32bit-4.4.2-11.12.1
libsmbldap0-debuginfo-4.4.2-11.12.1
libdcerpc-binding0-debuginfo-4.4.2-11.12.1
libsamba-credentials0-debuginfo-4.4.2-11.12.1
libsmbconf0-debuginfo-32bit-4.4.2-11.12.1
libsamba-errors0-32bit-4.4.2-11.12.1
libsamba-util0-4.4.2-11.12.1
ctdb-4.4.2-11.12.1
libsamba-policy0-4.4.2-11.12.1
libsamba-passdb0-debuginfo-4.4.2-11.12.1
libdcerpc-binding0-32bit-4.4.2-11.12.1
libndr-nbt0-debuginfo-32bit-4.4.2-11.12.1
libsamba-errors0-debuginfo-32bit-4.4.2-11.12.1
libsmbldap0-4.4.2-11.12.1
libsamba-policy0-debuginfo-32bit-4.4.2-11.12.1
libdcerpc-samr0-debuginfo-32bit-4.4.2-11.12.1

libsamba-passdb0-4.4.2-11.12.1
libndr0-debuginfo-4.4.2-11.12.1
libnetapi0-debuginfo-32bit-4.4.2-11.12.1
samba-debugsource-4.4.2-11.12.1
libndr-krb5pac0-debuginfo-32bit-4.4.2-11.12.1
samba-python-4.4.2-11.12.1
libsmbldap0-debuginfo-32bit-4.4.2-11.12.1
libsmbclient-devel-4.4.2-11.12.1
libsamdb0-debuginfo-32bit-4.4.2-11.12.1
libdcerpc0-4.4.2-11.12.1
libndr-nbt0-debuginfo-4.4.2-11.12.1
libwbclient0-debuginfo-4.4.2-11.12.1
samba-libs-debuginfo-32bit-4.4.2-11.12.1
libndr-standard0-4.4.2-11.12.1
ctdb-tests-debuginfo-4.4.2-11.12.1
libndr-devel-4.4.2-11.12.1
libsmbconf-devel-4.4.2-11.12.1
libsamba-util0-debuginfo-32bit-4.4.2-11.12.1
libsmbconf0-debuginfo-4.4.2-11.12.1
libsamba-policy0-32bit-4.4.2-11.12.1
libdcerpc-devel-4.4.2-11.12.1
libndr-standard-devel-4.4.2-11.12.1
samba-client-4.4.2-11.12.1
libsamba-util-devel-4.4.2-11.12.1
libsamba-util0-32bit-4.4.2-11.12.1
libsmbclient0-debuginfo-32bit-4.4.2-11.12.1
libdcerpc0-debuginfo-32bit-4.4.2-11.12.1
samba-test-debuginfo-4.4.2-11.12.1
samba-libs-32bit-4.4.2-11.12.1
libsamba-errors-devel-4.4.2-11.12.1
samba-client-32bit-4.4.2-11.12.1
samba-libs-debuginfo-4.4.2-11.12.1
libdcerpc-binding0-4.4.2-11.12.1
libndr-krb5pac-devel-4.4.2-11.12.1
libsamdb-devel-4.4.2-11.12.1
libdcerpc0-debuginfo-4.4.2-11.12.1
libsamdb0-debuginfo-4.4.2-11.12.1
samba-4.4.2-11.12.1

145991 - SuSE SLES 11 SP4 SUSE-SU-2017:2723-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2723-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-October/003296.html>

SuSE SLES 11 SP4

i586

kernel-source-3.0.101-108.13.1

kernel-pae-devel-3.0.101-108.13.1
kernel-pae-3.0.101-108.13.1
kernel-syms-3.0.101-108.13.1
kernel-default-base-3.0.101-108.13.1
kernel-pae-base-3.0.101-108.13.1
kernel-default-devel-3.0.101-108.13.1
kernel-xen-3.0.101-108.13.1
kernel-trace-base-3.0.101-108.13.1
kernel-trace-3.0.101-108.13.1
kernel-ec2-base-3.0.101-108.13.1
kernel-xen-devel-3.0.101-108.13.1
kernel-default-3.0.101-108.13.1
kernel-xen-base-3.0.101-108.13.1
kernel-trace-devel-3.0.101-108.13.1
kernel-ec2-devel-3.0.101-108.13.1
kernel-ec2-3.0.101-108.13.1

x86_64

kernel-source-3.0.101-108.13.1
kernel-syms-3.0.101-108.13.1
kernel-default-base-3.0.101-108.13.1
kernel-default-devel-3.0.101-108.13.1
kernel-xen-3.0.101-108.13.1
kernel-trace-base-3.0.101-108.13.1
kernel-trace-3.0.101-108.13.1
kernel-ec2-base-3.0.101-108.13.1
kernel-xen-devel-3.0.101-108.13.1
kernel-default-3.0.101-108.13.1
kernel-xen-base-3.0.101-108.13.1
kernel-trace-devel-3.0.101-108.13.1
kernel-ec2-devel-3.0.101-108.13.1
kernel-ec2-3.0.101-108.13.1

145992 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2710-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7793, CVE-2017-7805, CVE-2017-7810, CVE-2017-7814, CVE-2017-7818, CVE-2017-7819, CVE-2017-7823, CVE-2017-7824, CVE-2017-7825

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2710-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00039.html>

SuSE Linux 42.2

x86_64

MozillaThunderbird-buildsymbols-52.4.0-41.18.1
MozillaThunderbird-translations-common-52.4.0-41.18.1
MozillaThunderbird-52.4.0-41.18.1
MozillaThunderbird-translations-other-52.4.0-41.18.1
MozillaThunderbird-devel-52.4.0-41.18.1
MozillaThunderbird-debugsource-52.4.0-41.18.1

MozillaThunderbird-debuginfo-52.4.0-41.18.1

i586

MozillaThunderbird-buildsymbols-52.4.0-41.18.1

MozillaThunderbird-translations-common-52.4.0-41.18.1

MozillaThunderbird-52.4.0-41.18.1

MozillaThunderbird-translations-other-52.4.0-41.18.1

MozillaThunderbird-devel-52.4.0-41.18.1

MozillaThunderbird-debugsource-52.4.0-41.18.1

MozillaThunderbird-debuginfo-52.4.0-41.18.1

SuSE Linux 42.3

x86_64

MozillaThunderbird-debuginfo-52.4.0-47.1

MozillaThunderbird-translations-common-52.4.0-47.1

MozillaThunderbird-debugsource-52.4.0-47.1

MozillaThunderbird-devel-52.4.0-47.1

MozillaThunderbird-buildsymbols-52.4.0-47.1

MozillaThunderbird-translations-other-52.4.0-47.1

MozillaThunderbird-52.4.0-47.1

i586

MozillaThunderbird-debuginfo-52.4.0-47.1

MozillaThunderbird-translations-common-52.4.0-47.1

MozillaThunderbird-debugsource-52.4.0-47.1

MozillaThunderbird-devel-52.4.0-47.1

MozillaThunderbird-buildsymbols-52.4.0-47.1

MozillaThunderbird-translations-other-52.4.0-47.1

MozillaThunderbird-52.4.0-47.1

145993 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2712-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11462

Description

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

openSUSE-SU-2017:2712-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00041.html>

SuSE Linux 42.2

x86_64

krb5-server-debuginfo-1.12.5-6.3.1

krb5-doc-1.12.5-6.3.1

krb5-plugin-preauth-pkinit-1.12.5-6.3.1

krb5-debugsource-1.12.5-6.3.1

krb5-client-debuginfo-1.12.5-6.3.1

krb5-debuginfo-32bit-1.12.5-6.3.1

krb5-mini-debugsource-1.12.5-6.3.1

krb5-mini-debuginfo-1.12.5-6.3.1

krb5-server-1.12.5-6.3.1

krb5-1.12.5-6.3.1

krb5-32bit-1.12.5-6.3.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-6.3.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-6.3.1
krb5-debuginfo-1.12.5-6.3.1
krb5-mini-devel-1.12.5-6.3.1
krb5-client-1.12.5-6.3.1
krb5-plugin-kdb-ldap-1.12.5-6.3.1
krb5-plugin-preauth-otp-1.12.5-6.3.1
krb5-devel-32bit-1.12.5-6.3.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-6.3.1
krb5-devel-1.12.5-6.3.1
krb5-mini-1.12.5-6.3.1

i586

krb5-server-debuginfo-1.12.5-6.3.1
krb5-doc-1.12.5-6.3.1
krb5-plugin-preauth-pkinit-1.12.5-6.3.1
krb5-debugsource-1.12.5-6.3.1
krb5-client-debuginfo-1.12.5-6.3.1
krb5-mini-debugsource-1.12.5-6.3.1
krb5-mini-debuginfo-1.12.5-6.3.1
krb5-server-1.12.5-6.3.1
krb5-1.12.5-6.3.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-6.3.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-6.3.1
krb5-debuginfo-1.12.5-6.3.1
krb5-mini-devel-1.12.5-6.3.1
krb5-client-1.12.5-6.3.1
krb5-plugin-kdb-ldap-1.12.5-6.3.1
krb5-plugin-preauth-otp-1.12.5-6.3.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-6.3.1
krb5-devel-1.12.5-6.3.1
krb5-mini-1.12.5-6.3.1

SuSE Linux 42.3

x86_64

krb5-mini-devel-1.12.5-9.1
krb5-debuginfo-32bit-1.12.5-9.1
krb5-server-debuginfo-1.12.5-9.1
krb5-mini-debugsource-1.12.5-9.1
krb5-32bit-1.12.5-9.1
krb5-client-1.12.5-9.1
krb5-debugsource-1.12.5-9.1
krb5-devel-32bit-1.12.5-9.1
krb5-debuginfo-1.12.5-9.1
krb5-devel-1.12.5-9.1
krb5-doc-1.12.5-9.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-9.1
krb5-plugin-preauth-pkinit-1.12.5-9.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-9.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-9.1
krb5-mini-1.12.5-9.1
krb5-plugin-kdb-ldap-1.12.5-9.1
krb5-client-debuginfo-1.12.5-9.1
krb5-1.12.5-9.1
krb5-server-1.12.5-9.1
krb5-plugin-preauth-otp-1.12.5-9.1
krb5-mini-debuginfo-1.12.5-9.1

i586

krb5-mini-devel-1.12.5-9.1
krb5-server-debuginfo-1.12.5-9.1
krb5-mini-debugsource-1.12.5-9.1
krb5-client-1.12.5-9.1
krb5-debugsource-1.12.5-9.1
krb5-debuginfo-1.12.5-9.1
krb5-devel-1.12.5-9.1
krb5-doc-1.12.5-9.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-9.1
krb5-plugin-preauth-pkinit-1.12.5-9.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-9.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-9.1
krb5-mini-1.12.5-9.1
krb5-plugin-kdb-ldap-1.12.5-9.1
krb5-client-debuginfo-1.12.5-9.1
krb5-1.12.5-9.1
krb5-server-1.12.5-9.1
krb5-plugin-preauth-otp-1.12.5-9.1
krb5-mini-debuginfo-1.12.5-9.1

145994 - SuSE Linux 42.3 openSUSE-SU-2017:2706-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12150, CVE-2017-12151, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2706-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00035.html>

SuSE Linux 42.3

i586

samba-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-krb5pac-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-hostconfig0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-libs-debuginfo-4.6.7+git.51.327af8d0a11-6.1
ctdb-tests-4.6.7+git.51.327af8d0a11-6.1
libnetapi-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-credentials-devel-4.6.7+git.51.327af8d0a11-6.1
libwbclient-devel-4.6.7+git.51.327af8d0a11-6.1
libwbclient0-4.6.7+git.51.327af8d0a11-6.1
libndr0-4.6.7+git.51.327af8d0a11-6.1
libndr-nbt0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsamdb-devel-4.6.7+git.51.327af8d0a11-6.1
libsmbclient0-4.6.7+git.51.327af8d0a11-6.1
libsamba-hostconfig0-4.6.7+git.51.327af8d0a11-6.1
libndr-nbt0-4.6.7+git.51.327af8d0a11-6.1
libsmbldap0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-devel-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-samr0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-errors0-4.6.7+git.51.327af8d0a11-6.1

samba-pidl-4.6.7+git.51.327af8d0a11-6.1
libndr-krb5pac0-4.6.7+git.51.327af8d0a11-6.1
ctdb-tests-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsamba-errors0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libtevent-util0-4.6.7+git.51.327af8d0a11-6.1
libsmbconf-devel-4.6.7+git.51.327af8d0a11-6.1
samba-winbind-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-nbt-devel-4.6.7+git.51.327af8d0a11-6.1
samba-libs-4.6.7+git.51.327af8d0a11-6.1
libsmbldap-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-hostconfig-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-passsdb-devel-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-samr0-4.6.7+git.51.327af8d0a11-6.1
samba-debugsource-4.6.7+git.51.327af8d0a11-6.1
ctdb-4.6.7+git.51.327af8d0a11-6.1
ctdb-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-test-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-4.6.7+git.51.327af8d0a11-6.1
libsamba-util0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsamba-util0-4.6.7+git.51.327af8d0a11-6.1
libwbclient0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-samr-devel-4.6.7+git.51.327af8d0a11-6.1
samba-test-4.6.7+git.51.327af8d0a11-6.1
libsmbclient0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsamba-util-devel-4.6.7+git.51.327af8d0a11-6.1
libtevent-util0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-standard0-4.6.7+git.51.327af8d0a11-6.1
libsamba-errors-devel-4.6.7+git.51.327af8d0a11-6.1
libnetapi0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-client-4.6.7+git.51.327af8d0a11-6.1
libsmbclient-devel-4.6.7+git.51.327af8d0a11-6.1
libndr-standard0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-winbind-4.6.7+git.51.327af8d0a11-6.1
libsmbconf0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-core-devel-4.6.7+git.51.327af8d0a11-6.1
libsmbconf0-4.6.7+git.51.327af8d0a11-6.1
libndr-krb5pac0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-binding0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libnetapi0-4.6.7+git.51.327af8d0a11-6.1
libtevent-util-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-policy0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsamba-credentials0-4.6.7+git.51.327af8d0a11-6.1
libdcerpc0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsamdb0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsmbldap0-4.6.7+git.51.327af8d0a11-6.1
libsamba-passsdb0-4.6.7+git.51.327af8d0a11-6.1
libsamba-policy-devel-4.6.7+git.51.327af8d0a11-6.1
samba-python-4.6.7+git.51.327af8d0a11-6.1
libsamdb0-4.6.7+git.51.327af8d0a11-6.1
libsamba-credentials0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-binding0-4.6.7+git.51.327af8d0a11-6.1
libsamba-passsdb0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsamba-policy0-4.6.7+git.51.327af8d0a11-6.1
libdcerpc0-4.6.7+git.51.327af8d0a11-6.1
samba-client-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-standard-devel-4.6.7+git.51.327af8d0a11-6.1
samba-python-debuginfo-4.6.7+git.51.327af8d0a11-6.1

samba-doc-4.6.7+git.51.327af8d0a11-6.1

x86_64

samba-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-krb5pac-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-hostconfig0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-libs-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-standard0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
ctdb-tests-4.6.7+git.51.327af8d0a11-6.1
libnetapi-devel-4.6.7+git.51.327af8d0a11-6.1
libndr0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libsamba-credentials-devel-4.6.7+git.51.327af8d0a11-6.1
libwbclient-devel-4.6.7+git.51.327af8d0a11-6.1
libsmbclient0-32bit-4.6.7+git.51.327af8d0a11-6.1
libwbclient0-4.6.7+git.51.327af8d0a11-6.1
libwbclient0-32bit-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-samr0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libndr0-4.6.7+git.51.327af8d0a11-6.1
samba-libs-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libsamba-passsdb0-32bit-4.6.7+git.51.327af8d0a11-6.1
libndr-nbt0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libtevent-util0-32bit-4.6.7+git.51.327af8d0a11-6.1
libsamdb-devel-4.6.7+git.51.327af8d0a11-6.1
samba-client-32bit-4.6.7+git.51.327af8d0a11-6.1
libsmbclient0-4.6.7+git.51.327af8d0a11-6.1
libsamba-hostconfig0-4.6.7+git.51.327af8d0a11-6.1
libndr-nbt0-4.6.7+git.51.327af8d0a11-6.1
libsmbldap0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-ceph-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-devel-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-samr0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-util0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libsamba-errors0-4.6.7+git.51.327af8d0a11-6.1
libsamba-passsdb0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libtevent-util0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libndr-nbt0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
samba-pidl-4.6.7+git.51.327af8d0a11-6.1
samba-libs-32bit-4.6.7+git.51.327af8d0a11-6.1
libsamba-credentials0-32bit-4.6.7+git.51.327af8d0a11-6.1
libsamdb0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libndr-krb5pac0-4.6.7+git.51.327af8d0a11-6.1
ctdb-tests-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsamba-errors0-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libsmbldap0-32bit-4.6.7+git.51.327af8d0a11-6.1
libndr-standard0-32bit-4.6.7+git.51.327af8d0a11-6.1
libsamba-hostconfig0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-binding0-32bit-4.6.7+git.51.327af8d0a11-6.1
libsamba-hostconfig0-32bit-4.6.7+git.51.327af8d0a11-6.1
libdcerpc0-32bit-4.6.7+git.51.327af8d0a11-6.1
libtevent-util0-4.6.7+git.51.327af8d0a11-6.1
libsmbldap0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-6.1
libsmbconf-devel-4.6.7+git.51.327af8d0a11-6.1
samba-winbind-debuginfo-4.6.7+git.51.327af8d0a11-6.1
libndr-nbt-devel-4.6.7+git.51.327af8d0a11-6.1
samba-libs-4.6.7+git.51.327af8d0a11-6.1
libsmbldap-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-hostconfig-devel-4.6.7+git.51.327af8d0a11-6.1
libsamba-passsdb-devel-4.6.7+git.51.327af8d0a11-6.1
libdcerpc-samr0-4.6.7+git.51.327af8d0a11-6.1

libsamba-util0-32bit-4.6.7+git.51.327af8d0a11-6.1
samba-debugsource-4.6.7+git.51.327af8d0a11-6.1
ctdb-4.6.7+git.51.327af8d0a11-6.1
ctdb-debuginfo-4.6.7+git.51.327af8d0a11-6.1
samba-test-debuginfo-4.6.7+git.51.327af8d0a11-6.1

145996 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2735-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14532, CVE-2017-15033

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2735-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00049.html>

SuSE Linux 42.2

x86_64

GraphicsMagick-debuginfo-1.3.25-11.27.1
libGraphicsMagick-Q16-3-1.3.25-11.27.1
perl-GraphicsMagick-1.3.25-11.27.1
GraphicsMagick-1.3.25-11.27.1
libGraphicsMagick++-Q16-12-1.3.25-11.27.1
libGraphicsMagick3-config-1.3.25-11.27.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.27.1
GraphicsMagick-devel-1.3.25-11.27.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.27.1
perl-GraphicsMagick-debuginfo-1.3.25-11.27.1
libGraphicsMagickWand-Q16-2-1.3.25-11.27.1
GraphicsMagick-debugsource-1.3.25-11.27.1
libGraphicsMagick++-devel-1.3.25-11.27.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.27.1

i586

GraphicsMagick-debuginfo-1.3.25-11.27.1
libGraphicsMagick-Q16-3-1.3.25-11.27.1
perl-GraphicsMagick-1.3.25-11.27.1
GraphicsMagick-1.3.25-11.27.1
libGraphicsMagick++-Q16-12-1.3.25-11.27.1
libGraphicsMagick3-config-1.3.25-11.27.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.27.1
GraphicsMagick-devel-1.3.25-11.27.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.27.1
perl-GraphicsMagick-debuginfo-1.3.25-11.27.1
libGraphicsMagickWand-Q16-2-1.3.25-11.27.1
GraphicsMagick-debugsource-1.3.25-11.27.1
libGraphicsMagick++-devel-1.3.25-11.27.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.27.1

SuSE Linux 42.3

x86_64

libGraphicsMagick-Q16-3-1.3.25-27.1

libGraphicsMagick-Q16-3-debuginfo-1.3.25-27.1
perl-GraphicsMagick-1.3.25-27.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-27.1
libGraphicsMagickWand-Q16-2-1.3.25-27.1
libGraphicsMagick++-devel-1.3.25-27.1
perl-GraphicsMagick-debuginfo-1.3.25-27.1
GraphicsMagick-1.3.25-27.1
GraphicsMagick-devel-1.3.25-27.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-27.1
libGraphicsMagick++-Q16-12-1.3.25-27.1
GraphicsMagick-debuginfo-1.3.25-27.1
libGraphicsMagick3-config-1.3.25-27.1
GraphicsMagick-debugsource-1.3.25-27.1

i586

libGraphicsMagick-Q16-3-1.3.25-27.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-27.1
perl-GraphicsMagick-1.3.25-27.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-27.1
libGraphicsMagickWand-Q16-2-1.3.25-27.1
libGraphicsMagick++-devel-1.3.25-27.1
perl-GraphicsMagick-debuginfo-1.3.25-27.1
GraphicsMagick-1.3.25-27.1
GraphicsMagick-devel-1.3.25-27.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-27.1
libGraphicsMagick++-Q16-12-1.3.25-27.1
GraphicsMagick-debuginfo-1.3.25-27.1
libGraphicsMagick3-config-1.3.25-27.1
GraphicsMagick-debugsource-1.3.25-27.1

145997 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2730-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15191, CVE-2017-15192, CVE-2017-15193

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2730-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00045.html>

SuSE Linux 42.2

x86_64

wireshark-devel-2.2.10-14.16.1
wireshark-debuginfo-2.2.10-14.16.1
wireshark-2.2.10-14.16.1
wireshark-debugsource-2.2.10-14.16.1
wireshark-ui-qt-debuginfo-2.2.10-14.16.1
wireshark-ui-gtk-debuginfo-2.2.10-14.16.1
wireshark-ui-gtk-2.2.10-14.16.1
wireshark-ui-qt-2.2.10-14.16.1

SuSE Linux 42.3

x86_64
wireshark-ui-qt-2.2.10-24.1
wireshark-2.2.10-24.1
wireshark-ui-gtk-debuginfo-2.2.10-24.1
wireshark-debugsource-2.2.10-24.1
wireshark-ui-gtk-2.2.10-24.1
wireshark-ui-qt-debuginfo-2.2.10-24.1
wireshark-debuginfo-2.2.10-24.1
wireshark-devel-2.2.10-24.1

145998 - SuSE SLES 11 SP4 SUSE-SU-2017:2715-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12150, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2715-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-October/003292.html>

SuSE SLES 11 SP4
noarch
samba-doc-3.6.3-94.5.1

i586
ldapsmb-1.34b-94.5.1
libldb1-3.6.3-94.5.1
libwbclient0-3.6.3-94.5.1
libsmbclient0-3.6.3-94.5.1
libtdb1-3.6.3-94.5.1
libtalloc2-3.6.3-94.5.1
libtevent0-3.6.3-94.5.1
samba-client-3.6.3-94.5.1
samba-winbind-3.6.3-94.5.1
samba-krb-printing-3.6.3-94.5.1
samba-3.6.3-94.5.1

x86_64
samba-client-3.6.3-94.5.1
libtalloc2-32bit-3.6.3-94.5.1
libtalloc2-3.6.3-94.5.1
libsmbclient0-3.6.3-94.5.1
libtevent0-32bit-3.6.3-94.5.1
samba-client-32bit-3.6.3-94.5.1
samba-krb-printing-3.6.3-94.5.1
libtevent0-3.6.3-94.5.1
libtdb1-32bit-3.6.3-94.5.1
libwbclient0-3.6.3-94.5.1
samba-32bit-3.6.3-94.5.1
samba-3.6.3-94.5.1
libwbclient0-32bit-3.6.3-94.5.1
libsmbclient0-32bit-3.6.3-94.5.1

samba-winbind-32bit-3.6.3-94.5.1
samba-winbind-3.6.3-94.5.1
libtdb1-3.6.3-94.5.1
ldapsmb-1.34b-94.5.1
libldb1-3.6.3-94.5.1

160311 - CentOS 6, 7 CESA-2017-2885 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2885

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-October/022567.html>

<http://lists.centos.org/pipermail/centos-announce/2017-October/022566.html>

CentOS 7
x86_64
thunderbird-52.4.0-2.el7.centos

CentOS 6
x86_64
thunderbird-52.4.0-2.el6.centos

i686
thunderbird-52.4.0-2.el6.centos

160312 - CentOS 7 CESA-2017-2907 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2907

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-October/022569.html>

CentOS 7
x86_64
wpa_supplicant-2.6-5.el7_4.1

163478 - Oracle Enterprise Linux ELSA-2017-2885 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7793, CVE-2017-7810, CVE-2017-7814, CVE-2017-7818, CVE-2017-7819, CVE-2017-7823, CVE-2017-7824

Description

The scan detected that the host is missing the following update:
ELSA-2017-2885

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-October/007265.html>

<http://oss.oracle.com/pipermail/el-errata/2017-October/007264.html>

OEL7

x86_64

thunderbird-52.4.0-2.0.1.el7_4

OEL6

x86_64

thunderbird-52.4.0-2.0.1.el6_9

i386

thunderbird-52.4.0-2.0.1.el6_9

170886 - Amazon Linux AMI ALAS-2017-911 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7805

Description

The scan detected that the host is missing the following update:
ALAS-2017-911

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-911.html>

Amazon Linux AMI

x86_64

nss-sysinit-3.28.4-12.80.amzn1

nss-devel-3.28.4-12.80.amzn1

nss-3.28.4-12.80.amzn1

nss-tools-3.28.4-12.80.amzn1

nss-pkcs11-devel-3.28.4-12.80.amzn1

nss-debuginfo-3.28.4-12.80.amzn1

i686

nss-sysinit-3.28.4-12.80.amzn1

nss-devel-3.28.4-12.80.amzn1

nss-3.28.4-12.80.amzn1

nss-tools-3.28.4-12.80.amzn1

nss-pkcs11-devel-3.28.4-12.80.amzn1
nss-debuginfo-3.28.4-12.80.amzn1

175273 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86_64 (1710-10309)

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

Risk Level: High

CVE: CVE-2017-7793, CVE-2017-7810, CVE-2017-7814, CVE-2017-7818, CVE-2017-7819, CVE-2017-7823, CVE-2017-7824

Description

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

Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86_64 (1710-10309)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1710&L=scientific-linux-errata&F=&S=&P=10309>

SL7

x86_64

thunderbird-debuginfo-52.4.0-2.el7_4

thunderbird-52.4.0-2.el7_4

SL6

x86_64

thunderbird-debuginfo-52.4.0-2.el6_9

thunderbird-52.4.0-2.el6_9

i386

thunderbird-debuginfo-52.4.0-2.el6_9

thunderbird-52.4.0-2.el6_9

178525 - Gentoo Linux GLSA-201710-17 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

GLSA-201710-17

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201710-17>

Affected packages:

app-emulation/xen < 4.7.3

app-emulation/xen-pvgrub < 4.7.3

app-emulation/xen-tools < 4.7.3

182481 - FreeBSD Python 2.7 Multiple Vulnerabilities (9164f51e-ae20-11e7-a633-009c02a2ab30)

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

Risk Level: High

CVE: CVE-2012-0876, CVE-2016-0718, CVE-2016-4472, CVE-2016-5300, CVE-2016-9063, CVE-2017-9233

Description

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

Python 2.7 -- multiple vulnerabilities (9164f51e-ae20-11e7-a633-009c02a2ab30)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/9164f51e-ae20-11e7-a633-009c02a2ab30.html>

Affected packages:

python27 < 2.7.14

182487 - FreeBSD mercurial Multiple Issues (b0628e53-092a-4037-938b-29805a7cd31b)

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

Risk Level: High

CVE: CVE-2017-1000115, CVE-2017-1000116

Description

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

mercurial -- multiple issues (b0628e53-092a-4037-938b-29805a7cd31b)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/b0628e53-092a-4037-938b-29805a7cd31b.html>

Affected packages:

mercurial < 4.3

182490 - FreeBSD FFmpeg Multiple Vulnerabilities (ed73829d-af6d-11e7-a633-009c02a2ab30)

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

Risk Level: High

CVE: CVE-2017-14054, CVE-2017-14055, CVE-2017-14056, CVE-2017-14057, CVE-2017-14058, CVE-2017-14059, CVE-2017-14169, CVE-2017-14170, CVE-2017-14171, CVE-2017-14222, CVE-2017-14223, CVE-2017-14225, CVE-2017-14767

Description

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

FFmpeg -- multiple vulnerabilities (ed73829d-af6d-11e7-a633-009c02a2ab30)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/ed73829d-af6d-11e7-a633-009c02a2ab30.html>

Affected packages:

ffmpeg < 3.3.4

185922 - Ubuntu Linux 16.04, 17.04 USN-3450-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9214, CVE-2017-9263, CVE-2017-9264, CVE-2017-9265

Description

The scan detected that the host is missing the following update:
USN-3450-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004089.html>

Ubuntu 17.04

openvswitch-common_2.6.1-0ubuntu5.1

Ubuntu 16.04

openvswitch-common_2.5.2-0ubuntu0.16.04.2

185925 - Ubuntu Linux 14.04 USN-3449-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3241, CVE-2015-3280, CVE-2015-5162, CVE-2015-7548, CVE-2015-7713, CVE-2015-8749, CVE-2016-2140

Description

The scan detected that the host is missing the following update:
USN-3449-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004092.html>

Ubuntu 14.04

python-nova_2014.1.5-0ubuntu1.7

192775 - Fedora Linux 27 FEDORA-2017-8489b17872 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6307, CVE-2017-6308, CVE-2017-6309, CVE-2017-6310, CVE-2017-8911

Description

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

FEDORA-2017-8489b17872

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 27

tnef-1.4.15-1.fc27

192776 - Fedora Linux 26 FEDORA-2017-45625fecca Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14970, CVE-2017-9263, CVE-2017-9265

Description

The scan detected that the host is missing the following update:
FEDORA-2017-45625fecca

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=2>

Fedora Core 26

openvswitch-2.7.3-2.fc26

145987 - SuSE Linux 42.3 openSUSE-SU-2017:2741-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000252, CVE-2017-12153, CVE-2017-12154, CVE-2017-14489

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2741-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00052.html>

SuSE Linux 42.3

x86_64

kernel-default-debugsource-4.4.90-28.1

kernel-vanilla-base-4.4.90-28.1

kernel-debug-4.4.90-28.1

kernel-default-4.4.90-28.1

kernel-syms-4.4.90-28.1

kernel-debug-devel-4.4.90-28.1
kernel-vanilla-4.4.90-28.1
kernel-obs-build-debugsource-4.4.90-28.1
kernel-debug-debuginfo-4.4.90-28.1
kernel-vanilla-debuginfo-4.4.90-28.1
kernel-default-base-4.4.90-28.1
kernel-vanilla-devel-4.4.90-28.1
kernel-default-base-debuginfo-4.4.90-28.1
kernel-debug-devel-debuginfo-4.4.90-28.1
kernel-default-debuginfo-4.4.90-28.1
kernel-debug-base-debuginfo-4.4.90-28.1
kernel-vanilla-debugsource-4.4.90-28.1
kernel-obs-qa-4.4.90-28.1
kernel-debug-base-4.4.90-28.1
kernel-debug-debugsource-4.4.90-28.1
kernel-default-devel-4.4.90-28.1
kernel-obs-build-4.4.90-28.1
kernel-vanilla-base-debuginfo-4.4.90-28.1

noarch

kernel-docs-4.4.90-28.2
kernel-docs-html-4.4.90-28.2
kernel-docs-pdf-4.4.90-28.2
kernel-source-vanilla-4.4.90-28.1
kernel-devel-4.4.90-28.1
kernel-macros-4.4.90-28.1
kernel-source-4.4.90-28.1

145995 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2736-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14032

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2736-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00050.html>

SuSE Linux 42.2

x86_64

mbbedtls-devel-1.3.19-16.1
libmbedtls9-32bit-1.3.19-16.1
libmbedtls9-1.3.19-16.1
mbbedtls-debugsource-1.3.19-16.1
libmbedtls9-debuginfo-1.3.19-16.1
libmbedtls9-debuginfo-32bit-1.3.19-16.1

i586

mbbedtls-devel-1.3.19-16.1
libmbedtls9-1.3.19-16.1
mbbedtls-debugsource-1.3.19-16.1
libmbedtls9-debuginfo-1.3.19-16.1

SuSE Linux 42.3
x86_64
mbedtls-debugsource-1.3.19-18.1
libmbedtls9-1.3.19-18.1
libmbedtls9-debuginfo-1.3.19-18.1
libmbedtls9-debuginfo-32bit-1.3.19-18.1
mbedtls-devel-1.3.19-18.1
libmbedtls9-32bit-1.3.19-18.1

i586
mbedtls-devel-1.3.19-18.1
libmbedtls9-1.3.19-18.1
mbedtls-debugsource-1.3.19-18.1
libmbedtls9-debuginfo-1.3.19-18.1

145999 - SuSE Linux 42.2 openSUSE-SU-2017:2739-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000252, CVE-2017-12153, CVE-2017-12154, CVE-2017-14489

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2739-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-10/msg00051.html>

SuSE Linux 42.2
x86_64
kernel-default-debuginfo-4.4.90-18.32.1
kernel-debug-devel-4.4.90-18.32.1
kernel-obs-build-4.4.90-18.32.1
kernel-debug-debuginfo-4.4.90-18.32.1
kernel-vanilla-debugsource-4.4.90-18.32.1
kernel-debug-devel-debuginfo-4.4.90-18.32.1
kernel-default-devel-4.4.90-18.32.1
kernel-vanilla-devel-4.4.90-18.32.1
kernel-default-debugsource-4.4.90-18.32.1
kernel-vanilla-4.4.90-18.32.1
kernel-obs-build-debugsource-4.4.90-18.32.1
kernel-debug-debugsource-4.4.90-18.32.1
kernel-debug-4.4.90-18.32.1
kernel-vanilla-base-debuginfo-4.4.90-18.32.1
kernel-obs-qa-4.4.90-18.32.1
kernel-default-base-debuginfo-4.4.90-18.32.1
kernel-syms-4.4.90-18.32.1
kernel-vanilla-base-4.4.90-18.32.1
kernel-vanilla-debuginfo-4.4.90-18.32.1
kernel-default-base-4.4.90-18.32.1
kernel-debug-base-4.4.90-18.32.1
kernel-default-4.4.90-18.32.1
kernel-debug-base-debuginfo-4.4.90-18.32.1

noarch

kernel-docs-pdf-4.4.90-18.32.2
kernel-devel-4.4.90-18.32.1
kernel-source-4.4.90-18.32.1
kernel-docs-4.4.90-18.32.2
kernel-docs-html-4.4.90-18.32.2
kernel-source-vanilla-4.4.90-18.32.1
kernel-macros-4.4.90-18.32.1

170888 - Amazon Linux AMI ALAS-2017-912 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
ALAS-2017-912

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-912.html>

Amazon Linux AMI

i686

emacs-common-24.3-20.22.amzn1

emacs-debuginfo-24.3-20.22.amzn1

emacs-24.3-20.22.amzn1

noarch

emacs-el-24.3-20.22.amzn1

x86_64

emacs-common-24.3-20.22.amzn1

emacs-debuginfo-24.3-20.22.amzn1

emacs-24.3-20.22.amzn1

182479 - FreeBSD xorg-server Multiple Issues (ab881a74-c016-4e6d-9f7d-68c8e7cedafb)

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

Risk Level: Medium

CVE: CVE-2017-10971, CVE-2017-10972

Description

The scan detected that the host is missing the following update:
xorg-server -- Multiple Issues (ab881a74-c016-4e6d-9f7d-68c8e7cedafb)

Observation

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

<http://www.vuxml.org/freebsd/ab881a74-c016-4e6d-9f7d-68c8e7cedafb.html>

Affected packages:

xorg-server <= 1.19.3

185917 - Ubuntu Linux 14.04 USN-3446-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5251, CVE-2015-5286, CVE-2016-0757

Description

The scan detected that the host is missing the following update:
USN-3446-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004088.html>

Ubuntu 14.04

glance-common_2014.1.5-0ubuntu1.1

185918 - Ubuntu Linux 12.04 USN-3445-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8633, CVE-2017-14106

Description

The scan detected that the host is missing the following update:
USN-3445-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004086.html>

Ubuntu 12.04

linux-image-3.2.0-131-omap_3.2.0-131.177
linux-image-generic-pae_3.2.0.131.145
linux-image-3.2.0-131-virtual_3.2.0-131.177
linux-image-powerpc64-smp_3.2.0.131.145
linux-image-3.2.0-131-powerpc-smp_3.2.0-131.177
linux-image-3.2.0-131-powerpc64-smp_3.2.0-131.177
linux-image-generic_3.2.0.131.145
linux-image-powerpc-smp_3.2.0.131.145
linux-image-3.2.0-131-highbank_3.2.0-131.177
linux-image-3.2.0-131-generic-pae_3.2.0-131.177
linux-image-omap_3.2.0.131.145
linux-image-highbank_3.2.0.131.145
linux-image-3.2.0-131-generic_3.2.0-131.177

185919 - Ubuntu Linux 14.04 USN-3454-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000376

Description

The scan detected that the host is missing the following update:
USN-3454-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004096.html>

Ubuntu 14.04

libffi6_3.1~rc1+r3.0.13-12ubuntu0.2

192767 - Fedora Linux 25 FEDORA-2017-ccb10391ad Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14520

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ccb10391ad

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 25

mingw-poppler-0.45.0-4.fc25

192782 - Fedora Linux 26 FEDORA-2017-9d9d8173df Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14520

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9d9d8173df

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 26

mingw-poppler-0.52.0-4.fc26

192783 - Fedora Linux 27 FEDORA-2017-d05a50dce6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14520

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d05a50dce6

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=4>

Fedora Core 27

mingw-poppler-0.57.0-2.fc27

192796 - Fedora Linux 25 FEDORA-2017-2008fdd7e2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12837, CVE-2017-12883

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2008fdd7e2

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 25

perl-5.24.3-389.fc25

22605 - (JSA10808) Juniper ScreenOS SSL Death Alert Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-8610

Description

A vulnerability is present in some versions of Juniper ScreenOS.

Observation

Juniper ScreenOS is a popular firewall and VPN operating system.

A vulnerability is present in some versions of Juniper ScreenOS. The flaw lies in the way the TLS/SSL protocol specifies processing of ALERT packets. Successful exploitation could allow an attacker to cause a denial of service condition.

130904 - Debian Linux 8.0, 9.0 DSA-3999-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088

Description

The scan detected that the host is missing the following update:
DSA-3999-1

Observation

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

<http://www.debian.org/security/2017/dsa-3999>

Debian 8.0

all
wpasupplicant_2.3-1+deb8u5
wpasupplicant-udeb_2.3-1+deb8u5
wpaui_2.3-1+deb8u5
hostapd_2.3-1+deb8u5

Debian 9.0

all
wpaui_2:2.4-1+deb9u1
hostapd_2:2.4-1+deb9u1
wpasupplicant_2:2.4-1+deb9u1
wpasupplicant-udeb_2:2.4-1+deb9u1

141744 - Red Hat Enterprise Linux RHSA-2017-2882 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
RHSA-2017-2882

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-October/msg00010.html>

RHEL7D

x86_64
httpd-2.4.6-67.el7_4.5
httpd-devel-2.4.6-67.el7_4.5
httpd-tools-2.4.6-67.el7_4.5

mod_proxy_html-2.4.6-67.el7_4.5
mod_ssl-2.4.6-67.el7_4.5
mod_ldap-2.4.6-67.el7_4.5
mod_session-2.4.6-67.el7_4.5
httpd-debuginfo-2.4.6-67.el7_4.5

noarch
httpd-manual-2.4.6-67.el7_4.5

RHEL7S
noarch
httpd-manual-2.4.6-67.el7_4.5

x86_64
httpd-2.4.6-67.el7_4.5
httpd-devel-2.4.6-67.el7_4.5
mod_ldap-2.4.6-67.el7_4.5
httpd-tools-2.4.6-67.el7_4.5
mod_proxy_html-2.4.6-67.el7_4.5
mod_ssl-2.4.6-67.el7_4.5
mod_session-2.4.6-67.el7_4.5
httpd-debuginfo-2.4.6-67.el7_4.5

RHEL7WS
x86_64
httpd-2.4.6-67.el7_4.5
httpd-devel-2.4.6-67.el7_4.5
mod_ldap-2.4.6-67.el7_4.5
httpd-tools-2.4.6-67.el7_4.5
mod_proxy_html-2.4.6-67.el7_4.5
mod_ssl-2.4.6-67.el7_4.5
mod_session-2.4.6-67.el7_4.5
httpd-debuginfo-2.4.6-67.el7_4.5

noarch
httpd-manual-2.4.6-67.el7_4.5

141747 - Red Hat Enterprise Linux RHSA-2017-2907 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088

Description

The scan detected that the host is missing the following update:
RHSA-2017-2907

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-October/msg00019.html>

RHEL7D
x86_64
wpa_supplicant-debuginfo-2.6-5.el7_4.1
wpa_supplicant-2.6-5.el7_4.1

RHEL7S
x86_64
wpa_supplicant-debuginfo-2.6-5.el7_4.1
wpa_supplicant-2.6-5.el7_4.1

RHEL7WS
x86_64
wpa_supplicant-debuginfo-2.6-5.el7_4.1
wpa_supplicant-2.6-5.el7_4.1

160313 - CentOS 7 CESA-2017-2882 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2882

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-October/022565.html>

CentOS 7
x86_64
mod_ldap-2.4.6-67.el7.centos.5
httpd-devel-2.4.6-67.el7.centos.5
mod_proxy_html-2.4.6-67.el7.centos.5
mod_ssl-2.4.6-67.el7.centos.5
httpd-2.4.6-67.el7.centos.5
mod_session-2.4.6-67.el7.centos.5
httpd-tools-2.4.6-67.el7.centos.5

noarch
httpd-manual-2.4.6-67.el7.centos.5

163476 - Oracle Enterprise Linux ELSA-2017-2907 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088

Description

The scan detected that the host is missing the following update:
ELSA-2017-2907

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-October/007266.html>

OEL7
x86_64
wpa_supplicant-2.6-5.el7_4.1

163477 - Oracle Enterprise Linux ELSA-2017-2882 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
ELSA-2017-2882

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-October/007263.html>

OEL7
x86_64
mod_ldap-2.4.6-67.0.1.el7_4.5
mod_proxy_html-2.4.6-67.0.1.el7_4.5
mod_session-2.4.6-67.0.1.el7_4.5
httpd-devel-2.4.6-67.0.1.el7_4.5
mod_ssl-2.4.6-67.0.1.el7_4.5
httpd-2.4.6-67.0.1.el7_4.5
httpd-tools-2.4.6-67.0.1.el7_4.5
httpd-manual-2.4.6-67.0.1.el7_4.5

170887 - Amazon Linux AMI ALAS-2017-910 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
ALAS-2017-910

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-910.html>

Amazon Linux AMI
i686
git-debuginfo-2.13.6-1.55.amzn1
git-2.13.6-1.55.amzn1
git-svn-2.13.6-1.55.amzn1
git-daemon-2.13.6-1.55.amzn1

noarch

git-all-2.13.6-1.55.amzn1
perl-Git-2.13.6-1.55.amzn1
emacs-git-2.13.6-1.55.amzn1
git-email-2.13.6-1.55.amzn1
git-p4-2.13.6-1.55.amzn1
git-hg-2.13.6-1.55.amzn1
emacs-git-el-2.13.6-1.55.amzn1
perl-Git-SVN-2.13.6-1.55.amzn1
git-cvs-2.13.6-1.55.amzn1
gitweb-2.13.6-1.55.amzn1
git-bzr-2.13.6-1.55.amzn1

x86_64
git-debuginfo-2.13.6-1.55.amzn1
git-2.13.6-1.55.amzn1
git-svn-2.13.6-1.55.amzn1
git-daemon-2.13.6-1.55.amzn1

170889 - Amazon Linux AMI ALAS-2017-909 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12150, CVE-2017-12151, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
ALAS-2017-909

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-909.html>

Amazon Linux AMI

i686
samba-devel-4.6.2-11.36.amzn1
samba-client-libs-4.6.2-11.36.amzn1
ctdb-tests-4.6.2-11.36.amzn1
samba-test-libs-4.6.2-11.36.amzn1
samba-4.6.2-11.36.amzn1
samba-winbind-krb5-locator-4.6.2-11.36.amzn1
samba-winbind-4.6.2-11.36.amzn1
libsmbclient-devel-4.6.2-11.36.amzn1
samba-test-4.6.2-11.36.amzn1
samba-libs-4.6.2-11.36.amzn1
libwbclient-devel-4.6.2-11.36.amzn1
samba-krb5-printing-4.6.2-11.36.amzn1
samba-common-libs-4.6.2-11.36.amzn1
samba-python-4.6.2-11.36.amzn1
libwbclient-4.6.2-11.36.amzn1
samba-common-tools-4.6.2-11.36.amzn1
samba-client-4.6.2-11.36.amzn1
samba-debuginfo-4.6.2-11.36.amzn1
libsmbclient-4.6.2-11.36.amzn1
samba-winbind-modules-4.6.2-11.36.amzn1
ctdb-4.6.2-11.36.amzn1
samba-winbind-clients-4.6.2-11.36.amzn1

noarch
samba-common-4.6.2-11.36.amzn1
samba-pidl-4.6.2-11.36.amzn1

x86_64
samba-devel-4.6.2-11.36.amzn1
samba-client-libs-4.6.2-11.36.amzn1
ctdb-tests-4.6.2-11.36.amzn1
samba-libs-4.6.2-11.36.amzn1
samba-client-4.6.2-11.36.amzn1
samba-winbind-krb5-locator-4.6.2-11.36.amzn1
samba-winbind-4.6.2-11.36.amzn1
libsmbclient-devel-4.6.2-11.36.amzn1
samba-test-4.6.2-11.36.amzn1
samba-test-libs-4.6.2-11.36.amzn1
libwbclient-devel-4.6.2-11.36.amzn1
samba-krb5-printing-4.6.2-11.36.amzn1
samba-common-libs-4.6.2-11.36.amzn1
samba-python-4.6.2-11.36.amzn1
libwbclient-4.6.2-11.36.amzn1
samba-common-tools-4.6.2-11.36.amzn1
samba-debuginfo-4.6.2-11.36.amzn1
libsmbclient-4.6.2-11.36.amzn1
samba-4.6.2-11.36.amzn1
samba-winbind-modules-4.6.2-11.36.amzn1
ctdb-4.6.2-11.36.amzn1
samba-winbind-clients-4.6.2-11.36.amzn1

175274 - Scientific Linux Security ERRATA Moderate: httpd on SL7.x x86_64 (1710-9988)

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

Risk Level: Medium

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: httpd on SL7.x x86_64 (1710-9988)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1710&L=scientific-linux-errata&F=&S=&P=9988>

SL7
x86_64
httpd-2.4.6-67.el7_4.5
httpd-devel-2.4.6-67.el7_4.5
httpd-tools-2.4.6-67.el7_4.5
mod_proxy_html-2.4.6-67.el7_4.5
mod_ssl-2.4.6-67.el7_4.5
mod_ldap-2.4.6-67.el7_4.5
mod_session-2.4.6-67.el7_4.5
httpd-debuginfo-2.4.6-67.el7_4.5

noarch
httpd-manual-2.4.6-67.el7_4.5

178522 - Gentoo Linux GLSA-201710-16 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201710-16

Observation

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

<https://security.gentoo.org/glsa/201710-16>

Affected packages:
sys-apps/shadow < 4.5

178523 - Gentoo Linux GLSA-201710-20 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201710-20

Observation

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

<https://security.gentoo.org/glsa/201710-20>

Affected packages:
net-analyzer/nagios-core < 4.3.3

178526 - Gentoo Linux GLSA-201710-11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201710-11

Observation

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

<https://security.gentoo.org/glsa/201710-11>

Affected packages:
dev-libs/libtasn1 < 4.12-r1

178527 - Gentoo Linux GLSA-201710-13 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201710-13

Observation

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

<https://security.gentoo.org/glsa/201710-13>

Affected packages:
media-gfx/graphite2 < 1.3.10

178528 - Gentoo Linux GLSA-201710-10 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201710-10

Observation

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

<https://security.gentoo.org/glsa/201710-10>

Affected packages:
dev-libs/elfutils < 0.169-r1

178529 - Gentoo Linux GLSA-201710-12 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201710-12

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201710-12>

Affected packages:

app-admin/puppet-agent < 1.7.1

178530 - Gentoo Linux GLSA-201710-18 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

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

GLSA-201710-18

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201710-18>

Affected packages:

dev-lang/ruby < 2.2.8

178531 - Gentoo Linux GLSA-201710-15 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

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

GLSA-201710-15

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201710-15>

Affected packages:

net-libs/gnutls < 3.5.13

178532 - Gentoo Linux GLSA-201710-19 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

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

GLSA-201710-19

Observation

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

<https://security.gentoo.org/glsa/201710-19>

Affected packages:

app-arch/libarchive < 3.3.0

182484 - FreeBSD osip Improper Restriction Of Operations Within The Bounds Of A Memory Buffer (15a62f22-098a-443b-94e2-2d26c375b993)

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

Risk Level: Medium

CVE: CVE-2017-7853

Description

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

osip -- Improper Restriction of Operations within the Bounds of a Memory Buffer (15a62f22-098a-443b-94e2-2d26c375b993)

Observation

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

<http://www.vuxml.org/freebsd/15a62f22-098a-443b-94e2-2d26c375b993.html>

Affected packages:

libosip2 <= 5.0.0

182491 - FreeBSD WPA Packet Number Reuse With Replayed Messages And Key Reinstallation (d670a953-b2a1-11e7-a633-009c02a2ab30)

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

Risk Level: Medium

CVE: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088

Description

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

WPA packet number reuse with replayed messages and key reinstallation (d670a953-b2a1-11e7-a633-009c02a2ab30)

Observation

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

<http://www.vuxml.org/freebsd/d670a953-b2a1-11e7-a633-009c02a2ab30.html>

Affected packages:

wpa_supplicant <= 2.6_1

hostapd <= 2.6

185913 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3455-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4476, CVE-2016-4477, CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088

Description

The scan detected that the host is missing the following update:
USN-3455-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004097.html>

Ubuntu 16.04

wpa_supplicant_2.4-0ubuntu6.2
hostapd_2.4-0ubuntu6.2

Ubuntu 14.04

wpa_supplicant_2.1-0ubuntu1.5
hostapd_2.1-0ubuntu1.5

Ubuntu 17.04

hostapd_2.4-0ubuntu9.1
wpa_supplicant_2.4-0ubuntu9.1

185920 - Ubuntu Linux 14.04 USN-3451-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5223, CVE-2016-0737, CVE-2016-0738

Description

The scan detected that the host is missing the following update:
USN-3451-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004091.html>

Ubuntu 14.04

python-swift_1.13.1-0ubuntu1.5
swift_1.13.1-0ubuntu1.5

192781 - Fedora Linux 27 FEDORA-2017-f45e844a85 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-

13087, CVE-2017-13088

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f45e844a85

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 27

wpa_supplicant-2.6-11.fc27

192789 - Fedora Linux 27 FEDORA-2017-0d225819cf Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14970

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0d225819cf

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 27

openvswitch-2.8.1-1.fc27

192793 - Fedora Linux 26 FEDORA-2017-60bfb576b7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13087, CVE-2017-13088

Description

The scan detected that the host is missing the following update:
FEDORA-2017-60bfb576b7

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=2>

Fedora Core 26

wpa_supPLICant-2.6-11.fc26

192794 - Fedora Linux 25 FEDORA-2017-12e76e8364 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13087, CVE-2017-13088

Description

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

FEDORA-2017-12e76e8364

Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 25

wpa_supPLICant-2.6-3.fc25.1

145989 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2751-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5526

Description

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

SUSE-SU-2017:2751-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-October/003303.html>

SuSE SLED 12 SP3

x86_64

xen-4.9.0_14-3.18.1

xen-debugsource-4.9.0_14-3.18.1

xen-libs-32bit-4.9.0_14-3.18.1

xen-libs-debuginfo-32bit-4.9.0_14-3.18.1

xen-libs-debuginfo-4.9.0_14-3.18.1

xen-libs-4.9.0_14-3.18.1

SuSE SLES 12 SP3

x86_64

xen-4.9.0_14-3.18.1

xen-debugsource-4.9.0_14-3.18.1

xen-libs-32bit-4.9.0_14-3.18.1

xen-tools-4.9.0_14-3.18.1

xen-tools-domU-4.9.0_14-3.18.1

xen-libs-debuginfo-32bit-4.9.0_14-3.18.1

xen-libs-debuginfo-4.9.0_14-3.18.1
xen-tools-debuginfo-4.9.0_14-3.18.1
xen-libs-4.9.0_14-3.18.1
xen-doc-html-4.9.0_14-3.18.1
xen-tools-domU-debuginfo-4.9.0_14-3.18.1

182486 - FreeBSD ncurses Multiple Issues (b84dbd94-e894-4c91-b8cd-d328537b1b2b)

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

Risk Level: Medium

CVE: CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734

Description

The scan detected that the host is missing the following update:
ncurses -- multiple issues (b84dbd94-e894-4c91-b8cd-d328537b1b2b)

Observation

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

<http://www.vuxml.org/freebsd/b84dbd94-e894-4c91-b8cd-d328537b1b2b.html>

Affected packages:
ncurses <= 6.0

185921 - Ubuntu Linux 14.04 USN-3452-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5009, CVE-2016-7031, CVE-2016-8626, CVE-2016-9579

Description

The scan detected that the host is missing the following update:
USN-3452-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004094.html>

Ubuntu 14.04

ceph_0.80.11-0ubuntu1.14.04.3
ceph-common_0.80.11-0ubuntu1.14.04.3

185924 - Ubuntu Linux 16.04 USN-3443-3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14106

Description

The scan detected that the host is missing the following update:
USN-3443-3

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004085.html>

Ubuntu 16.04

linux-image-4.10.0-1007-gcp_4.10.0-1007.7

linux-image-gcp_4.10.0.1007.9

192778 - Fedora Linux 27 FEDORA-2017-79b7fd1b4d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1495, CVE-2017-14955

Description

The scan detected that the host is missing the following update:
FEDORA-2017-79b7fd1b4d

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=4>

Fedora Core 27

check-mk-1.2.8p26-1.fc27

192784 - Fedora Linux 26 FEDORA-2017-1179268a20 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0380

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1179268a20

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 26

tor-0.3.1.7-1.fc26

192785 - Fedora Linux 25 FEDORA-2017-66d9113c7a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13768

Description

The scan detected that the host is missing the following update:
FEDORA-2017-66d9113c7a

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=4>

Fedora Core 25

rubygem-rmagick-2.16.0-7.fc25

ImageMagick-6.9.9.15-1.fc25

192797 - Fedora Linux 25 FEDORA-2017-238961d86d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0380

Description

The scan detected that the host is missing the following update:
FEDORA-2017-238961d86d

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=4>

Fedora Core 25

tor-0.2.9.12-1.fc25

130905 - Debian Linux 8.0, 9.0 DSA-3995-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13720, CVE-2017-13722

Description

The scan detected that the host is missing the following update:
DSA-3995-1

Observation

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

<http://www.debian.org/security/2017/dsa-3995>

Debian 8.0

all

libxfont1-dbg_1:1.5.1-1+deb8u1

libxfont-dev_1:1.5.1-1+deb8u1

libxfont1_1:1.5.1-1+deb8u1

libxfont1-udeb_1:1.5.1-1+deb8u1

Debian 9.0

all

libxfont-dev_1:2.0.1-3+deb9u1

libxfont2_1:2.0.1-3+deb9u1

libxfont2-udeb_1:2.0.1-3+deb9u1

130906 - Debian Linux 8.0, 9.0 DSA-3998-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7805

Description

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

DSA-3998-1

Observation

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

For more information see:

<http://www.debian.org/security/2017/dsa-3998>

Debian 8.0

all

libnss3-1d_2:3.26-1+debu8u3

libnss3-tools_2:3.26-1+debu8u3

libnss3-dev_2:3.26-1+debu8u3

libnss3-dbg_2:3.26-1+debu8u3

libnss3_2:3.26-1+debu8u3

Debian 9.0

all

libnss3-dev_2:3.26.2-1.1+deb9u1

libnss3-tools_2:3.26.2-1.1+deb9u1

libnss3_2:3.26.2-1.1+deb9u1

libnss3-dbg_2:3.26.2-1.1+deb9u1

130907 - Debian Linux 8.0, 9.0 DSA-4000-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12176, CVE-2017-12177, CVE-2017-12178, CVE-2017-12179, CVE-2017-12180, CVE-2017-12181, CVE-2017-12182, CVE-2017-12183, CVE-2017-12184, CVE-2017-12185, CVE-2017-12186, CVE-2017-12187, CVE-2017-13721, CVE-2017-13723

Description

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

DSA-4000-1

Observation

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

<http://www.debian.org/security/2017/dsa-4000>

Debian 8.0

all

xserver-common_2:1.16.4-1+deb8u2
xdmx_2:1.16.4-1+deb8u2
xserver-xorg-dev_2:1.16.4-1+deb8u2
xserver-xorg-core_2:1.16.4-1+deb8u2
xorg-server-source_2:1.16.4-1+deb8u2
xserver-xephyr_2:1.16.4-1+deb8u2
xdmx-tools_2:1.16.4-1+deb8u2
xnest_2:1.16.4-1+deb8u2
xvfb_2:1.16.4-1+deb8u2
xserver-xorg-core-dbg_2:1.16.4-1+deb8u2
xserver-xorg-core-udeb_2:1.16.4-1+deb8u2
xwayland_2:1.16.4-1+deb8u2

Debian 9.0

all

xserver-xorg-legacy_2:1.19.2-1+deb9u2
xvfb_2:1.19.2-1+deb9u2
xnest_2:1.19.2-1+deb9u2
xserver-xephyr_2:1.19.2-1+deb9u2
xorg-server-source_2:1.19.2-1+deb9u2
xserver-common_2:1.19.2-1+deb9u2
xwayland_2:1.19.2-1+deb9u2
xserver-xorg-core_2:1.19.2-1+deb9u2
xserver-xorg-core-udeb_2:1.19.2-1+deb9u2
xdmx-tools_2:1.19.2-1+deb9u2
xdmx_2:1.19.2-1+deb9u2
xserver-xorg-dev_2:1.19.2-1+deb9u2

182478 - FreeBSD Multiple Exploitable Heap-based Buffer Overflow Vulnerabilities Exists In FreeXL 1.0.3 (555cd806-b031-11e7-a369-14dae9d)

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

Risk Level: Low

CVE: CVE-2017-2923, CVE-2017-2924

Description

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

Multiple exploitable heap-based buffer overflow vulnerabilities exists in FreeXL 1.0.3 (555cd806-b031-11e7-a369-14dae9d59f67)

Observation

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

<http://www.vuxml.org/freebsd/555cd806-b031-11e7-a369-14dae9d59f67.html>

Affected packages:

freexl < 1.0.4

182480 - FreeBSD nss Use-after-free In TLS 1.2 Generating Handshake Hashes (e71fd9d3-af47-11e7-a633-009c02a2ab30)

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

Risk Level: Low

CVE: CVE-2017-7805

Description

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

nss -- Use-after-free in TLS 1.2 generating handshake hashes (e71fd9d3-af47-11e7-a633-009c02a2ab30)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/e71fd9d3-af47-11e7-a633-009c02a2ab30.html>

Affected packages:

3.32 <= nss < 3.32.1

3.32 <= linux-c6-nss < 3.32.1

3.32 <= linux-c7-nss < 3.32.1

3.28 <= nss < 3.28.6

3.28 <= linux-c6-nss < 3.28.6

3.28 <= linux-c7-nss < 3.28.6

182482 - FreeBSD Flash Player Remote Code Execution (a73518da-b2fa-11e7-98ef-d43d7ef03aa6)

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

Risk Level: Low

CVE: CVE-2017-11292

Description

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

Flash Player -- Remote code execution (a73518da-b2fa-11e7-98ef-d43d7ef03aa6)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/a73518da-b2fa-11e7-98ef-d43d7ef03aa6.html>

Affected packages:

linux-flashplayer < 27.0.0.170

182483 - FreeBSD xorg-server Multiple Vulnerabilities (7274e0cc-575f-41bc-8619-14a41b3c2ad0)

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

Risk Level: Low

CVE: CVE-2017-12176, CVE-2017-12177, CVE-2017-12178, CVE-2017-12179, CVE-2017-12180, CVE-2017-12181, CVE-2017-12182, CVE-2017-12183, CVE-2017-12184, CVE-2017-12185, CVE-2017-12186, CVE-2017-12187

Description

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

xorg-server -- multiple vulnerabilities (7274e0cc-575f-41bc-8619-14a41b3c2ad0)

Observation

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

<http://www.vuxml.org/freebsd/7274e0cc-575f-41bc-8619-14a41b3c2ad0.html>

Affected packages:

xephyr < 1.18.4_5,1
xorg-dmx < 1.18.4_5,1
xorg-nestserver < 1.19.1_2,2
xorg-server < 1.18.4_5,1
xorg-vfbserver < 1.19.1_2,1
xwayland < 1.19.1_2

182485 - FreeBSD xen-kernel Multiple Vulnerabilities (da70d472-af59-11e7-ace2-f8b156b439c5)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
xen-kernel -- multiple vulnerabilities (da70d472-af59-11e7-ace2-f8b156b439c5)

Observation

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

<http://www.vuxml.org/freebsd/da70d472-af59-11e7-ace2-f8b156b439c5.html>

Affected packages:

xen-kernel < 4.7.2_6

182488 - FreeBSD jenkins Multiple Issues (6dc3c61c-e866-4c27-93f7-ae50908594fd)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
jenkins -- multiple issues (6dc3c61c-e866-4c27-93f7-ae50908594fd)

Observation

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

<http://www.vuxml.org/freebsd/6dc3c61c-e866-4c27-93f7-ae50908594fd.html>

Affected packages:

jenkins <= 2.83
jenkins-lts <= 2.73.1

182489 - FreeBSD solr Code Execution Via Entity Expansion (e837390d-0ceb-46b8-9b32-29c1195f5dc7)

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

Risk Level: Low

CVE: CVE-2017-12629

Description

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

solr -- Code execution via entity expansion (e837390d-0ceb-46b8-9b32-29c1195f5dc7)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/e837390d-0ceb-46b8-9b32-29c1195f5dc7.html>

Affected packages:

5.1 <= apache-solr <= 6.6.1

7.0.0 <= apache-solr < 7.1

185914 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3453-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13721, CVE-2017-13723

Description

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

USN-3453-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004095.html>

Ubuntu 16.04

xserver-xorg-core_1.18.4-0ubuntu0.6

xserver-xorg-core-hwe-16.04_1.19.3-1ubuntu1~16.04.3

Ubuntu 14.04

xserver-xorg-core_1.15.1-0ubuntu2.10

xserver-xorg-core-lts-xenial_1.18.3-1ubuntu2.3~trusty3

Ubuntu 17.04

xserver-xorg-core_1.19.3-1ubuntu1.2

185915 - Ubuntu Linux 16.04 USN-3448-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2673

Description

The scan detected that the host is missing the following update:
USN-3448-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004093.html>

Ubuntu 16.04

python-keystone_9.3.0-0ubuntu3.1
keystone_9.3.0-0ubuntu3.1

185916 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3456-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12176, CVE-2017-12177, CVE-2017-12178, CVE-2017-12179, CVE-2017-12180, CVE-2017-12181, CVE-2017-12182, CVE-2017-12183, CVE-2017-12184, CVE-2017-12185, CVE-2017-12186, CVE-2017-12187

Description

The scan detected that the host is missing the following update:
USN-3456-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004098.html>

Ubuntu 16.04

xserver-xorg-core-hwe-16.04_1.19.3-1ubuntu1~16.04.4
xserver-xorg-core_1.18.4-0ubuntu0.7

Ubuntu 14.04

xserver-xorg-core-lts-xenial_1.18.3-1ubuntu2.3~trusty4
xserver-xorg-core_1.15.1-0ubuntu2.11

Ubuntu 17.04

xserver-xorg-core_1.19.3-1ubuntu1.3

185923 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3436-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7793, CVE-2017-7805, CVE-2017-7810, CVE-2017-7814, CVE-2017-7818, CVE-2017-7819, CVE-2017-7823, CVE-2017-7824

Description

The scan detected that the host is missing the following update:
USN-3436-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004087.html>

Ubuntu 16.04

thunderbird_52.4.0+build1-0ubuntu0.16.04.2

Ubuntu 14.04

thunderbird_52.4.0+build1-0ubuntu0.14.04.2

Ubuntu 17.04

thunderbird_52.4.0+build1-0ubuntu0.17.04.2

185926 - Ubuntu Linux 14.04 USN-3447-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4428

Description

The scan detected that the host is missing the following update:
USN-3447-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004090.html>

Ubuntu 14.04

openstack-dashboard_2014.1.5-0ubuntu2.1

192768 - Fedora Linux 26 FEDORA-2017-88b6a06bce 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-2017-88b6a06bce

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 26

selinux-policy-3.13.1-260.13.fc26

192769 - Fedora Linux 25 FEDORA-2017-89efe409a2 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-2017-89efe409a2

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 25

weechat-1.9.1-1.fc25

192770 - Fedora Linux 27 FEDORA-2017-ff17e19bae 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-2017-ff17e19bae

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=2>

Fedora Core 27

weechat-1.9.1-1.fc27

192771 - Fedora Linux 26 FEDORA-2017-5c2a294fba 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-2017-5c2a294fba

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 26

weechat-1.9.1-1.fc26

192772 - Fedora Linux 26 FEDORA-2017-601b4c20a4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000254

Description

The scan detected that the host is missing the following update:
FEDORA-2017-601b4c20a4

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=2>

Fedora Core 26

curl-7.53.1-11.fc26

192773 - Fedora Linux 27 FEDORA-2017-097791759e 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-2017-097791759e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 27

ImageMagick-6.9.9.19-1.fc27
rubygem-rmagick-2.16.0-8.fc27

192774 - Fedora Linux 27 FEDORA-2017-33506d3f26 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-2017-33506d3f26

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 27

xorg-x11-server-1.19.5-1.fc27

192777 - Fedora Linux 26 FEDORA-2017-f244168d7f 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-2017-f244168d7f

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 26

recode-3.6-44.fc26

192779 - Fedora Linux 27 FEDORA-2017-89e2655938 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15056

Description

The scan detected that the host is missing the following update:
FEDORA-2017-89e2655938

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 27

upx-3.94-1.fc27

192780 - Fedora Linux 27 FEDORA-2017-2c58422bc0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2887

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2c58422bc0

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 27

SDL2_image-2.0.1-8.fc27

192786 - Fedora Linux 25 FEDORA-2017-66aa5d1d33 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-2017-66aa5d1d33

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=4>

Fedora Core 25

git-2.9.5-2.fc25

192787 - Fedora Linux 25 FEDORA-2017-4dfebebd39 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-2017-4dfebebd39

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 25

recode-3.6-43.fc25

192788 - Fedora Linux 27 FEDORA-2017-f3e5d31524 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13720, CVE-2017-13722

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f3e5d31524

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 27

libXfont-1.5.2-5.fc27

192790 - Fedora Linux 26 FEDORA-2017-6f1b90dbb7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15041, CVE-2017-15042

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6f1b90dbb7

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 26

golang-1.8.4-1.fc26

192791 - Fedora Linux 26 FEDORA-2017-efeb59171d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120, CVE-2017-5121, CVE-2017-5122

Description

The scan detected that the host is missing the following update:
FEDORA-2017-efeb59171d

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=3>

Fedora Core 26

chromium-61.0.3163.100-1.fc26

192792 - Fedora Linux 27 FEDORA-2017-75cf2c921a 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-2017-75cf2c921a

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=1>

Fedora Core 27

procmail-3.22-44.fc27

192795 - Fedora Linux 27 FEDORA-2017-f4fc897e8f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15041, CVE-2017-15042

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f4fc897e8f

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/10/?count=200&page=4>

Fedora Core 27

golang-1.9.1-1.fc27

22611 - Wireshark Multiple Vulnerabilities Prior To 2.4.2

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

Risk Level: Low

CVE: CVE-2017-15189, CVE-2017-15190, CVE-2017-15191, CVE-2017-15192, CVE-2017-15193

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

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.

33312 - Oracle Solaris 152078-71 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

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

33313 - Oracle Solaris 152076-71 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

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

33314 - Oracle Solaris 152079-71 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

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

33315 - Oracle Solaris 152077-71 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

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

33106 - Oracle Solaris 148562-12 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2004-0452, CVE-2005-0156, CVE-2005-0448, CVE-2005-4278, CVE-2010-1158, CVE-2010-1168, CVE-2010-2761, CVE-2010-4411, CVE-2011-2939, CVE-2012-5195, CVE-2012-5526, CVE-2012-6329, CVE-2013-1667

Update Details

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

33107 - Oracle Solaris 148561-12 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2004-0452, CVE-2005-0156, CVE-2005-0448, CVE-2005-4278, CVE-2010-1158, CVE-2010-1168, CVE-2010-2761, CVE-2010-4411, CVE-2011-2939, CVE-2012-5195, CVE-2012-5526, CVE-2012-6329, CVE-2013-1667

Update Details

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

32622 - Oracle Solaris 143725-11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-3563, CVE-2013-5211, CVE-2014-9295, CVE-2014-9296

Update Details

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

32623 - Oracle Solaris 143726-11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-3563, CVE-2013-5211, CVE-2014-9295, CVE-2014-9296

Update Details

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

33326 - Oracle Solaris 152260-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0535, CVE-2017-10003

Update Details

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

33327 - Oracle Solaris 152261-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0535, CVE-2017-10003

Update Details

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

33336 - Oracle Solaris 152099-61 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

33339 - Oracle Solaris 152097-61 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

33340 - Oracle Solaris 152098-61 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

33341 - Oracle Solaris 152096-61 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

33349 - Oracle Solaris 152101-52 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

33350 - Oracle Solaris 152100-52 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

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

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 2017 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates