2017-OCT-12
FSL version 7.5.966

MCAFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

145976 - SuSE SLES 11 SP4 SUSE-SU-2017:2694-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000112, CVE-2017-1000251, CVE-2017-10661, CVE-2017-12762, CVE-2017-14051, CVE-2017-14140, CVE-2017-14340, CVE-2017-8831

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2694-1

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/003284.html

SuSE SLES 11 SP4
x86_64
kernel-rt_trace-base-3.0.101.rt130-69.8.1
kernel-rt_trace-devel-3.0.101.rt130-69.8.1
kernel-rt-devel-3.0.101.rt130-69.8.1
kernel-rt-base-3.0.101.rt130-69.8.1
kernel-rt-3.0.101.rt130-69.8.1
kernel-source-rt-3.0.101.rt130-69.8.1
kernel-rt_trace-3.0.101.rt130-69.8.1
kernel-syms-rt-3.0.101.rt130-69.8.1

163473 - Oracle Enterprise Linux ELSA-2017-2801 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253, CVE-2017-7895

Description

The scan detected that the host is missing the following update:
ELSA-2017-2801

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/007255.html

OEL5
x86_64
kernel-headers-2.6.18-419.0.0.0.4.el5
kernel-devel-2.6.18-419.0.0.0.4.el5
kernel-2.6.18-419.0.0.0.4.el5
kernel-xen-2.6.18-419.0.0.0.4.el5
kernel-xen-devel-2.6.18-419.0.0.0.4.el5

kernel-doc-2.6.18-419.0.0.0.4.el5
kernel-debug-2.6.18-419.0.0.0.4.el5
kernel-debug-devel-2.6.18-419.0.0.0.4.el5

i386
kernel-PAE-2.6.18-419.0.0.0.4.el5
kernel-headers-2.6.18-419.0.0.0.4.el5
kernel-PAE-devel-2.6.18-419.0.0.0.4.el5
kernel-devel-2.6.18-419.0.0.0.4.el5
kernel-2.6.18-419.0.0.0.4.el5
kernel-xen-2.6.18-419.0.0.0.4.el5
kernel-xen-devel-2.6.18-419.0.0.0.4.el5
kernel-doc-2.6.18-419.0.0.0.4.el5
kernel-debug-2.6.18-419.0.0.0.4.el5
kernel-debug-devel-2.6.18-419.0.0.0.4.el5

22586 - (HPESBHF03769) HPE Integrated Lights-Out Remote Vulnerability

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

Risk Level: High

CVE: CVE-2017-12542

Description

A vulnerability is present in some versions of HPE Integrated Lights-Out.

Observation

HPE Integrated Lights-Out is a Hewlett-Packard proprietary embedded server management technology.

A vulnerability is present in some versions of HPE Integrated Lights-Out. The flaw lies in an unknown component. Successful exploitation could allow a remote attacker to execute arbitrary code or bypass authentication security measure.

22582 - Apache Tomcat Vulnerability Prior To 8.5.23

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

Risk Level: High

CVE: CVE-2017-12617

Description

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

Observation

Apache Tomcat is a container for the Java Servlet and Java Server Pages Web applications.

A remote code vulnerability is present in some versions of Apache Tomcat. The flaw is due to insufficient validation of user input. Successful exploitation could allow an attacker to execute remote code on the target system.

163474 - Oracle Enterprise Linux ELSA-2017-2863 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-1000253, CVE-2017-7541

Description

The scan detected that the host is missing the following update:
ELSA-2017-2863

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/007253.html

OEL6
x86_64
kernel-abi-whitelists-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
kernel-firmware-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6
kernel-doc-2.6.32-696.13.2.el6

i386
kernel-abi-whitelists-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
kernel-firmware-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6
kernel-doc-2.6.32-696.13.2.el6

22480 - (APSB17-25) Vulnerabilities In RoboHelp

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

Risk Level: High

CVE: CVE-2017-3104, CVE-2017-3105

Description

Multiple vulnerabilities are present in Adobe RoboHelp.

Observation

Adobe RoboHelp is a tool used to create help document.

Multiple vulnerabilities are present in Adobe RoboHelp. The flaws exist in multiple components. Successful exploitation could allow an attacker to launch cross-site scripting attacks or phishing attacks.

22497 - NVIDIA Windows Drivers Multiple Vulnerabilities 09-2017

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

Risk Level: High

CVE: CVE-2017-6266, CVE-2017-6267, CVE-2017-6268, CVE-2017-6269, CVE-2017-6270, CVE-2017-6271, CVE-2017-6272, CVE-2017-6277

Description

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers.

Observation

NVIDIA is a technology company which manufactures graphics processing units.

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers. The flaws occur within the kernel mode layer. Successful exploitation could allow an attacker to escalate privileges or cause a denial of service condition.

22565 - (HT208102) Apple macOS Server Multiple Vulnerabilities Prior to 5.4

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10979

Description

Multiple vulnerabilities are present in some versions of Apple macOS Server.

Observation

Apple macOS Server provides easy to use interface to configure enterprise services for Apple devices.

Multiple vulnerabilities are present in some versions of Apple macOS Server. The flaws lie in the FreeRADIUS component. Successful exploitation could allow an attacker to cause denial-of-service or to possibly execute arbitrary code.

22581 - (CTX227928) Citrix NetScaler Gateway Authentication Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-14602

Description

A vulnerability is present in some versions of Citrix NetScaler Gateway.

Observation

Citrix NetScaler Gateway is a secure network access gateway.

A vulnerability is present in some versions of Citrix NetScaler Gateway. The flaw is in the management interface. Successful exploitation could allow an attacker to gain administrative access to system.

22592 - Cisco IOS Industrial Ethernet Switches PROFINET Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-12235

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw lies in the implementation of the PROFINET Discovery and Configuration Protocol component. Successful exploitation could allow an attacker to cause a denial-of-service condition.

141741 - Red Hat Enterprise Linux RHSA-2017-2860 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546

Description

The scan detected that the host is missing the following update:
RHSA-2017-2860

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/msg00007.html

RHEL6D
x86_64
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-debuginfo-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

i386
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-debuginfo-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

RHEL6S
i386
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-debuginfo-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

x86_64
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-debuginfo-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

RHEL6WS
x86_64
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9

postgresql-plperl-8.4.20-8.el6_9
postgresql-debuginfo-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

i386
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-debuginfo-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

141742 - Red Hat Enterprise Linux RHSA-2017-2863 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7541

Description

The scan detected that the host is missing the following update:
RHSA-2017-2863

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/msg00008.html

RHEL6D
i386
kernel-debug-debuginfo-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-debuginfo-common-i686-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-debuginfo-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6
perf-debuginfo-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6
python-perf-debuginfo-2.6.32-696.13.2.el6

noarch
kernel-firmware-2.6.32-696.13.2.el6
kernel-doc-2.6.32-696.13.2.el6
kernel-abi-whitelists-2.6.32-696.13.2.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-696.13.2.el6
kernel-debuginfo-common-x86_64-2.6.32-696.13.2.el6
python-perf-debuginfo-2.6.32-696.13.2.el6
perf-debuginfo-2.6.32-696.13.2.el6
kernel-debuginfo-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-debuginfo-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6

python-perf-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6

RHEL6S
i386
kernel-debug-debuginfo-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-debuginfo-common-i686-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-debuginfo-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6
perf-debuginfo-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6
python-perf-debuginfo-2.6.32-696.13.2.el6

noarch
kernel-firmware-2.6.32-696.13.2.el6
kernel-doc-2.6.32-696.13.2.el6
kernel-abi-whitelists-2.6.32-696.13.2.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-696.13.2.el6
kernel-debuginfo-common-x86_64-2.6.32-696.13.2.el6
python-perf-debuginfo-2.6.32-696.13.2.el6
perf-debuginfo-2.6.32-696.13.2.el6
kernel-debuginfo-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-debuginfo-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6

RHEL6WS
i386
kernel-debug-debuginfo-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-debuginfo-common-i686-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-debuginfo-2.6.32-696.13.2.el6
perf-debuginfo-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6
python-perf-debuginfo-2.6.32-696.13.2.el6

noarch
kernel-firmware-2.6.32-696.13.2.el6
kernel-doc-2.6.32-696.13.2.el6
kernel-abi-whitelists-2.6.32-696.13.2.el6

x86_64
kernel-debug-debuginfo-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-debuginfo-common-i686-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-debuginfo-2.6.32-696.13.2.el6
perf-debuginfo-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6

kernel-debug-2.6.32-696.13.2.el6
python-perf-debuginfo-2.6.32-696.13.2.el6
kernel-debuginfo-common-x86_64-2.6.32-696.13.2.el6

145970 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2688-1 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:
SUSE-SU-2017:2688-1

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/003282.html

SuSE SLES 12 SP2
x86_64
libfreebl3-hmac-32bit-3.29.5-58.3.1
mozilla-nss-certs-32bit-3.29.5-58.3.1
mozilla-nss-sysinit-3.29.5-58.3.1
mozilla-nss-sysinit-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-tools-debuginfo-3.29.5-58.3.1
libsoftokn3-hmac-3.29.5-58.3.1
libsoftokn3-3.29.5-58.3.1
libsoftokn3-debuginfo-32bit-3.29.5-58.3.1
libsoftokn3-32bit-3.29.5-58.3.1
libfreebl3-hmac-3.29.5-58.3.1
mozilla-nss-sysinit-debuginfo-3.29.5-58.3.1
mozilla-nss-sysinit-32bit-3.29.5-58.3.1
mozilla-nss-certs-debuginfo-3.29.5-58.3.1
libfreebl3-32bit-3.29.5-58.3.1
libfreebl3-3.29.5-58.3.1
mozilla-nss-debugsource-3.29.5-58.3.1
mozilla-nss-3.29.5-58.3.1
MozillaFirefox-52.4.0esr-109.6.2
MozillaFirefox-debugsource-52.4.0esr-109.6.2
libfreebl3-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-tools-3.29.5-58.3.1
libsoftokn3-hmac-32bit-3.29.5-58.3.1
mozilla-nss-debuginfo-3.29.5-58.3.1
libsoftokn3-debuginfo-3.29.5-58.3.1
mozilla-nss-certs-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-debuginfo-32bit-3.29.5-58.3.1
MozillaFirefox-translations-52.4.0esr-109.6.2
libfreebl3-debuginfo-3.29.5-58.3.1
mozilla-nss-certs-3.29.5-58.3.1
mozilla-nss-32bit-3.29.5-58.3.1
MozillaFirefox-debuginfo-52.4.0esr-109.6.2

SuSE SLED 12 SP3
x86_64
mozilla-nss-certs-32bit-3.29.5-58.3.1
mozilla-nss-sysinit-3.29.5-58.3.1
mozilla-nss-tools-debuginfo-3.29.5-58.3.1
libsoftokn3-3.29.5-58.3.1
libsoftokn3-debuginfo-32bit-3.29.5-58.3.1
libsoftokn3-32bit-3.29.5-58.3.1
mozilla-nss-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-sysinit-debuginfo-3.29.5-58.3.1

mozilla-nss-sysinit-32bit-3.29.5-58.3.1
mozilla-nss-certs-debuginfo-3.29.5-58.3.1
libfreebl3-32bit-3.29.5-58.3.1
libfreebl3-3.29.5-58.3.1
mozilla-nss-debugsource-3.29.5-58.3.1
mozilla-nss-3.29.5-58.3.1
MozillaFirefox-52.4.0esr-109.6.2
MozillaFirefox-debugsource-52.4.0esr-109.6.2
libfreebl3-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-tools-3.29.5-58.3.1
mozilla-nss-sysinit-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-debuginfo-3.29.5-58.3.1
libsoftokn3-debuginfo-3.29.5-58.3.1
mozilla-nss-certs-debuginfo-32bit-3.29.5-58.3.1
MozillaFirefox-translations-52.4.0esr-109.6.2
libfreebl3-debuginfo-3.29.5-58.3.1
mozilla-nss-certs-3.29.5-58.3.1
mozilla-nss-32bit-3.29.5-58.3.1
MozillaFirefox-debuginfo-52.4.0esr-109.6.2

SuSE SLED 12 SP2
x86_64
mozilla-nss-certs-32bit-3.29.5-58.3.1
mozilla-nss-sysinit-3.29.5-58.3.1
mozilla-nss-tools-debuginfo-3.29.5-58.3.1
libsoftokn3-3.29.5-58.3.1
libsoftokn3-debuginfo-32bit-3.29.5-58.3.1
libsoftokn3-32bit-3.29.5-58.3.1
mozilla-nss-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-sysinit-debuginfo-3.29.5-58.3.1
mozilla-nss-sysinit-32bit-3.29.5-58.3.1
mozilla-nss-certs-debuginfo-3.29.5-58.3.1
libfreebl3-32bit-3.29.5-58.3.1
libfreebl3-3.29.5-58.3.1
mozilla-nss-debugsource-3.29.5-58.3.1
mozilla-nss-3.29.5-58.3.1
MozillaFirefox-52.4.0esr-109.6.2
MozillaFirefox-debugsource-52.4.0esr-109.6.2
libfreebl3-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-tools-3.29.5-58.3.1
mozilla-nss-sysinit-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-debuginfo-3.29.5-58.3.1
libsoftokn3-debuginfo-3.29.5-58.3.1
mozilla-nss-certs-debuginfo-32bit-3.29.5-58.3.1
MozillaFirefox-translations-52.4.0esr-109.6.2
libfreebl3-debuginfo-3.29.5-58.3.1
mozilla-nss-certs-3.29.5-58.3.1
mozilla-nss-32bit-3.29.5-58.3.1
MozillaFirefox-debuginfo-52.4.0esr-109.6.2

SuSE SLES 12 SP3
x86_64
libfreebl3-hmac-32bit-3.29.5-58.3.1
mozilla-nss-certs-32bit-3.29.5-58.3.1
mozilla-nss-sysinit-3.29.5-58.3.1
mozilla-nss-sysinit-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-tools-debuginfo-3.29.5-58.3.1
libsoftokn3-hmac-3.29.5-58.3.1
libsoftokn3-3.29.5-58.3.1
libsoftokn3-debuginfo-32bit-3.29.5-58.3.1
libsoftokn3-32bit-3.29.5-58.3.1
libfreebl3-hmac-3.29.5-58.3.1
mozilla-nss-sysinit-debuginfo-3.29.5-58.3.1
mozilla-nss-sysinit-32bit-3.29.5-58.3.1
mozilla-nss-certs-debuginfo-3.29.5-58.3.1
libfreebl3-32bit-3.29.5-58.3.1
libfreebl3-3.29.5-58.3.1
mozilla-nss-debugsource-3.29.5-58.3.1

mozilla-nss-3.29.5-58.3.1
MozillaFirefox-52.4.0esr-109.6.2
MozillaFirefox-debugsource-52.4.0esr-109.6.2
libfreebl3-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-tools-3.29.5-58.3.1
libsoftokn3-hmac-32bit-3.29.5-58.3.1
mozilla-nss-debuginfo-3.29.5-58.3.1
libsoftokn3-debuginfo-3.29.5-58.3.1
mozilla-nss-certs-debuginfo-32bit-3.29.5-58.3.1
mozilla-nss-debuginfo-32bit-3.29.5-58.3.1
MozillaFirefox-translations-52.4.0esr-109.6.2
libfreebl3-debuginfo-3.29.5-58.3.1
mozilla-nss-certs-3.29.5-58.3.1
mozilla-nss-32bit-3.29.5-58.3.1
MozillaFirefox-debuginfo-52.4.0esr-109.6.2

145972 - SuSE SLES 11 SP4 SUSE-SU-2017:2660-1 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-2017:2660-1

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/003278.html

SuSE SLES 11 SP4
i586
libvirt-client-1.2.5-23.3.1
libvirt-1.2.5-23.3.1
libvirt-doc-1.2.5-23.3.1
libvirt-lock-sanlock-1.2.5-23.3.1

x86_64
libvirt-client-32bit-1.2.5-23.3.1
libvirt-client-1.2.5-23.3.1
libvirt-1.2.5-23.3.1
libvirt-doc-1.2.5-23.3.1
libvirt-lock-sanlock-1.2.5-23.3.1

145975 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2659-1 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:
SUSE-SU-2017:2659-1

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/003277.html

SuSE SLES 12 SP2
x86_64
krb5-server-debuginfo-1.12.5-40.13.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-40.13.1
krb5-debuginfo-32bit-1.12.5-40.13.1
krb5-debuginfo-1.12.5-40.13.1
krb5-32bit-1.12.5-40.13.1
krb5-plugin-preauth-otp-1.12.5-40.13.1
krb5-plugin-kdb-ldap-1.12.5-40.13.1
krb5-debugsource-1.12.5-40.13.1
krb5-doc-1.12.5-40.13.1
krb5-server-1.12.5-40.13.1
krb5-1.12.5-40.13.1
krb5-plugin-preauth-pkinit-1.12.5-40.13.1
krb5-client-debuginfo-1.12.5-40.13.1
krb5-client-1.12.5-40.13.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-40.13.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-40.13.1

SuSE SLED 12 SP3
x86_64
krb5-32bit-1.12.5-40.13.1
krb5-client-1.12.5-40.13.1
krb5-debuginfo-32bit-1.12.5-40.13.1
krb5-debuginfo-1.12.5-40.13.1
krb5-client-debuginfo-1.12.5-40.13.1
krb5-debugsource-1.12.5-40.13.1
krb5-1.12.5-40.13.1

SuSE SLED 12 SP2
x86_64
krb5-32bit-1.12.5-40.13.1
krb5-client-1.12.5-40.13.1
krb5-debuginfo-32bit-1.12.5-40.13.1
krb5-debuginfo-1.12.5-40.13.1
krb5-client-debuginfo-1.12.5-40.13.1
krb5-debugsource-1.12.5-40.13.1
krb5-1.12.5-40.13.1

SuSE SLES 12 SP3
x86_64
krb5-server-debuginfo-1.12.5-40.13.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-40.13.1
krb5-debuginfo-32bit-1.12.5-40.13.1
krb5-debuginfo-1.12.5-40.13.1
krb5-32bit-1.12.5-40.13.1
krb5-plugin-preauth-otp-1.12.5-40.13.1
krb5-plugin-kdb-ldap-1.12.5-40.13.1
krb5-debugsource-1.12.5-40.13.1
krb5-doc-1.12.5-40.13.1
krb5-server-1.12.5-40.13.1
krb5-1.12.5-40.13.1
krb5-plugin-preauth-pkinit-1.12.5-40.13.1
krb5-client-debuginfo-1.12.5-40.13.1
krb5-client-1.12.5-40.13.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-40.13.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-40.13.1

145977 - SuSE Linux 42.3 openSUSE-SU-2017:2653-1 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-2017:2653-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00018.html

SuSE Linux 42.3
x86_64
libvirt-daemon-driver-storage-mpath-3.3.0-6.1
libvirt-daemon-driver-interface-3.3.0-6.1
libvirt-daemon-driver-nodedev-3.3.0-6.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-6.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-6.1
libvirt-lock-sanlock-debuginfo-3.3.0-6.1
libvirt-client-debuginfo-32bit-3.3.0-6.1
libvirt-admin-3.3.0-6.1
libvirt-devel-32bit-3.3.0-6.1
libvirt-client-debuginfo-3.3.0-6.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-6.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-6.1
libvirt-daemon-driver-storage-logical-3.3.0-6.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-6.1
libvirt-3.3.0-6.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-6.1
libvirt-client-3.3.0-6.1
libvirt-daemon-vbox-3.3.0-6.1
libvirt-devel-3.3.0-6.1
libvirt-daemon-driver-storage-core-3.3.0-6.1
libvirt-lock-sanlock-3.3.0-6.1
libvirt-daemon-qemu-3.3.0-6.1
libvirt-daemon-driver-storage-scsi-3.3.0-6.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-6.1
libvirt-daemon-driver-nwfilter-3.3.0-6.1
libvirt-daemon-config-network-3.3.0-6.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-6.1
libvirt-daemon-driver-storage-3.3.0-6.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-6.1
libvirt-daemon-xen-3.3.0-6.1
libvirt-daemon-lxc-3.3.0-6.1
libvirt-daemon-3.3.0-6.1
libvirt-daemon-driver-vbox-3.3.0-6.1
libvirt-daemon-driver-libxl-3.3.0-6.1
libvirt-daemon-driver-storage-iscsi-3.3.0-6.1
libvirt-nss-debuginfo-3.3.0-6.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-6.1
libvirt-daemon-driver-qemu-3.3.0-6.1
libvirt-doc-3.3.0-6.1
libvirt-daemon-driver-uml-3.3.0-6.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-6.1
libvirt-daemon-driver-lxc-3.3.0-6.1
libvirt-nss-3.3.0-6.1
libvirt-daemon-driver-network-3.3.0-6.1
libvirt-daemon-driver-uml-debuginfo-3.3.0-6.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-6.1
libvirt-daemon-uml-3.3.0-6.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-6.1
libvirt-debugsource-3.3.0-6.1
libvirt-daemon-driver-storage-rbd-3.3.0-6.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-6.1
libvirt-libs-debuginfo-3.3.0-6.1
libvirt-daemon-debuginfo-3.3.0-6.1
libvirt-libs-3.3.0-6.1
libvirt-admin-debuginfo-3.3.0-6.1
libvirt-daemon-driver-storage-disk-3.3.0-6.1
libvirt-daemon-driver-network-debuginfo-3.3.0-6.1

libvirt-daemon-config-nwfilter-3.3.0-6.1
libvirt-daemon-driver-secret-3.3.0-6.1
libvirt-daemon-driver-vbox-debuginfo-3.3.0-6.1

i586
libvirt-daemon-driver-storage-mpath-3.3.0-6.1
libvirt-daemon-driver-interface-3.3.0-6.1
libvirt-daemon-driver-nodedev-3.3.0-6.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-6.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-6.1
libvirt-lock-sanlock-debuginfo-3.3.0-6.1
libvirt-admin-3.3.0-6.1
libvirt-client-debuginfo-3.3.0-6.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-6.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-6.1
libvirt-daemon-driver-storage-logical-3.3.0-6.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-6.1
libvirt-3.3.0-6.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-6.1
libvirt-client-3.3.0-6.1
libvirt-daemon-vbox-3.3.0-6.1
libvirt-devel-3.3.0-6.1
libvirt-daemon-driver-storage-core-3.3.0-6.1
libvirt-lock-sanlock-3.3.0-6.1
libvirt-daemon-qemu-3.3.0-6.1
libvirt-daemon-driver-storage-scsi-3.3.0-6.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-6.1
libvirt-daemon-driver-nwfilter-3.3.0-6.1
libvirt-daemon-config-network-3.3.0-6.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-6.1
libvirt-daemon-driver-storage-3.3.0-6.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-6.1
libvirt-daemon-lxc-3.3.0-6.1
libvirt-daemon-3.3.0-6.1
libvirt-daemon-driver-vbox-3.3.0-6.1
libvirt-daemon-driver-storage-iscsi-3.3.0-6.1
libvirt-nss-debuginfo-3.3.0-6.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-6.1
libvirt-daemon-driver-qemu-3.3.0-6.1
libvirt-doc-3.3.0-6.1
libvirt-daemon-driver-uml-3.3.0-6.1
libvirt-daemon-driver-lxc-3.3.0-6.1
libvirt-nss-3.3.0-6.1
libvirt-daemon-driver-network-3.3.0-6.1
libvirt-daemon-driver-uml-debuginfo-3.3.0-6.1
libvirt-daemon-uml-3.3.0-6.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-6.1
libvirt-debugsource-3.3.0-6.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-6.1
libvirt-libs-debuginfo-3.3.0-6.1
libvirt-daemon-debuginfo-3.3.0-6.1
libvirt-libs-3.3.0-6.1
libvirt-admin-debuginfo-3.3.0-6.1
libvirt-daemon-driver-storage-disk-3.3.0-6.1
libvirt-daemon-driver-network-debuginfo-3.3.0-6.1
libvirt-daemon-config-nwfilter-3.3.0-6.1
libvirt-daemon-driver-secret-3.3.0-6.1
libvirt-daemon-driver-vbox-debuginfo-3.3.0-6.1

145978 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2695-1 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:
SUSE-SU-2017:2695-1

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/003285.html

SuSE SLED 12 SP3
x86_64
libsmbldap0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-errors0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-errors0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
samba-libs-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-credentials0-4.6.7+git.51.327af8d0a11-3.12.1
libndr-nbt0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libnetapi0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-credentials0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libwbclient0-4.6.7+git.51.327af8d0a11-3.12.1
samba-libs-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libndr-krb5pac0-4.6.7+git.51.327af8d0a11-3.12.1
libndr-nbt0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-errors0-4.6.7+git.51.327af8d0a11-3.12.1
libndr-standard0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-client-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-hostconfig0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libndr-nbt0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libndr-standard0-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-passdb0-4.6.7+git.51.327af8d0a11-3.12.1
libndr0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libtevent-util0-4.6.7+git.51.327af8d0a11-3.12.1
libwbclient0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
samba-libs-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libndr0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc-binding0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-winbind-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsmbconf0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbclient0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-debugsource-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-passdb0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libwbclient0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc-binding0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libndr-krb5pac0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libnetapi0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libndr0-4.6.7+git.51.327af8d0a11-3.12.1
libsmbldap0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamdb0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-hostconfig0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbclient0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-util0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsmbconf0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-client-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-client-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-hostconfig0-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-hostconfig0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbconf0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc0-4.6.7+git.51.327af8d0a11-3.12.1
libtevent-util0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamdb0-4.6.7+git.51.327af8d0a11-3.12.1
libndr0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc-binding0-4.6.7+git.51.327af8d0a11-3.12.1
libndr-standard0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-passdb0-32bit-4.6.7+git.51.327af8d0a11-3.12.1

libsamba-util0-4.6.7+git.51.327af8d0a11-3.12.1
samba-winbind-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbconf0-4.6.7+git.51.327af8d0a11-3.12.1
libsmbclient0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libndr-krb5pac0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamdb0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-passdb0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc-binding0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-util0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-errors0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbclient0-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-credentials0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libndr-nbt0-4.6.7+git.51.327af8d0a11-3.12.1
samba-winbind-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libwbclient0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libtevent-util0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libndr-krb5pac0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libnetapi0-4.6.7+git.51.327af8d0a11-3.12.1
libnetapi0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-util0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
samba-winbind-4.6.7+git.51.327af8d0a11-3.12.1
libndr-standard0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libtevent-util0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-credentials0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbldap0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbldap0-4.6.7+git.51.327af8d0a11-3.12.1
samba-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
samba-client-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamdb0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-libs-4.6.7+git.51.327af8d0a11-3.12.1

noarch
samba-doc-4.6.7+git.51.327af8d0a11-3.12.1

SuSE SLES 12 SP3
noarch
samba-doc-4.6.7+git.51.327af8d0a11-3.12.1

x86_64
libsmbldap0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-passdb0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-errors0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-errors0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
samba-libs-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-credentials0-4.6.7+git.51.327af8d0a11-3.12.1
libsmbclient0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libndr-nbt0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libnetapi0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-credentials0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-libs-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libndr-krb5pac0-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-errors0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-errors0-4.6.7+git.51.327af8d0a11-3.12.1
libndr-standard0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-client-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-hostconfig0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libndr-nbt0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libndr-standard0-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-passdb0-4.6.7+git.51.327af8d0a11-3.12.1
libwbclient0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libndr0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc-binding0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbconf0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbclient0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
samba-debugsource-4.6.7+git.51.327af8d0a11-3.12.1

libndr0-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-util0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libwbclient0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libdcerpc-binding0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libndr-krb5pac0-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libnetapi0-debuginfo-32bit-4.6.7+git.51.327af8d0a11-3.12.1
libsmbldap0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamdb0-debuginfo-4.6.7+git.51.327af8d0a11-3.12.1
libsamba-hostconfig0-32bit-4.6.7+git.51.327af8d0a11-3.12.1

145979 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2697-1 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-2017:2697-1

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/003287.html

SuSE SLED 12 SP2
x86_64
libvirt-daemon-driver-network-2.0.0-27.20.1
libvirt-daemon-driver-storage-2.0.0-27.20.1
libvirt-debugsource-2.0.0-27.20.1
libvirt-client-32bit-2.0.0-27.20.1
libvirt-daemon-driver-interface-2.0.0-27.20.1
libvirt-daemon-qemu-2.0.0-27.20.1
libvirt-daemon-driver-secret-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-secret-2.0.0-27.20.1
libvirt-daemon-lxc-2.0.0-27.20.1
libvirt-daemon-driver-interface-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-lxc-2.0.0-27.20.1
libvirt-daemon-2.0.0-27.20.1
libvirt-daemon-config-network-2.0.0-27.20.1
libvirt-daemon-driver-nwfilter-2.0.0-27.20.1
libvirt-daemon-driver-qemu-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-lxc-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-nodedev-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-qemu-2.0.0-27.20.1
libvirt-2.0.0-27.20.1
libvirt-daemon-driver-libxl-debuginfo-2.0.0-27.20.1
libvirt-client-2.0.0-27.20.1
libvirt-daemon-driver-libxl-2.0.0-27.20.1
libvirt-daemon-driver-nwfilter-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-network-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-storage-debuginfo-2.0.0-27.20.1
libvirt-client-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-nodedev-2.0.0-27.20.1
libvirt-daemon-config-nwfilter-2.0.0-27.20.1
libvirt-daemon-xen-2.0.0-27.20.1
libvirt-daemon-debuginfo-2.0.0-27.20.1
libvirt-doc-2.0.0-27.20.1
libvirt-client-debuginfo-32bit-2.0.0-27.20.1

SuSE SLES 12 SP2
x86_64
libvirt-daemon-driver-network-2.0.0-27.20.1
libvirt-daemon-driver-storage-2.0.0-27.20.1

libvirt-debugsource-2.0.0-27.20.1
libvirt-daemon-driver-interface-2.0.0-27.20.1
libvirt-nss-2.0.0-27.20.1
libvirt-daemon-qemu-2.0.0-27.20.1
libvirt-daemon-driver-secret-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-secret-2.0.0-27.20.1
libvirt-daemon-lxc-2.0.0-27.20.1
libvirt-daemon-driver-interface-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-lxc-2.0.0-27.20.1
libvirt-daemon-2.0.0-27.20.1
libvirt-daemon-config-network-2.0.0-27.20.1
libvirt-daemon-driver-nwfilter-2.0.0-27.20.1
libvirt-daemon-driver-qemu-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-lxc-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-nodedev-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-qemu-2.0.0-27.20.1
libvirt-2.0.0-27.20.1
libvirt-daemon-driver-libxl-debuginfo-2.0.0-27.20.1
libvirt-client-2.0.0-27.20.1
libvirt-daemon-driver-libxl-2.0.0-27.20.1
libvirt-lock-sanlock-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-nwfilter-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-network-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-storage-debuginfo-2.0.0-27.20.1
libvirt-nss-debuginfo-2.0.0-27.20.1
libvirt-client-debuginfo-2.0.0-27.20.1
libvirt-daemon-driver-nodedev-2.0.0-27.20.1
libvirt-lock-sanlock-2.0.0-27.20.1
libvirt-daemon-config-nwfilter-2.0.0-27.20.1
libvirt-daemon-xen-2.0.0-27.20.1
libvirt-daemon-debuginfo-2.0.0-27.20.1
libvirt-doc-2.0.0-27.20.1

145980 - SuSE SLES 11 SP4 SUSE-SU-2017:2690-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-13011

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2690-1

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/003283.html

SuSE SLES 11 SP4
i586
tcpdump-3.9.8-1.30.5.1

x86_64
tcpdump-3.9.8-1.30.5.1

145981 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2650-1 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:
SUSE-SU-2017:2650-1

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/003275.html

SuSE SLED 12 SP2
x86_64
libsamba-credentials0-debuginfo-4.4.2-38.11.2
libsmbclient0-debuginfo-32bit-4.4.2-38.11.2
libnetapi0-debuginfo-32bit-4.4.2-38.11.2
libndr-krb5pac0-debuginfo-32bit-4.4.2-38.11.2
libndr0-debuginfo-4.4.2-38.11.2
libdcerpc0-4.4.2-38.11.2
libsamba-errors0-32bit-4.4.2-38.11.2
samba-client-debuginfo-4.4.2-38.11.2
libndr-krb5pac0-32bit-4.4.2-38.11.2
libnetapi0-debuginfo-4.4.2-38.11.2
samba-libs-debuginfo-32bit-4.4.2-38.11.2
libdcerpc-binding0-debuginfo-4.4.2-38.11.2
libtevent-util0-debuginfo-4.4.2-38.11.2
libsmbldap0-32bit-4.4.2-38.11.2
libsmbldap0-debuginfo-32bit-4.4.2-38.11.2
samba-winbind-debuginfo-4.4.2-38.11.2
libsamba-passdb0-4.4.2-38.11.2
samba-libs-32bit-4.4.2-38.11.2
libsamba-hostconfig0-32bit-4.4.2-38.11.2
libtevent-util0-debuginfo-32bit-4.4.2-38.11.2
libdcerpc-binding0-debuginfo-32bit-4.4.2-38.11.2
libdcerpc0-debuginfo-4.4.2-38.11.2
libdcerpc0-debuginfo-32bit-4.4.2-38.11.2
libsamdb0-debuginfo-32bit-4.4.2-38.11.2
samba-client-32bit-4.4.2-38.11.2
libsmbconf0-debuginfo-4.4.2-38.11.2
libnetapi0-4.4.2-38.11.2
libndr-nbt0-debuginfo-32bit-4.4.2-38.11.2
libndr-standard0-32bit-4.4.2-38.11.2
libnetapi0-32bit-4.4.2-38.11.2
samba-libs-debuginfo-4.4.2-38.11.2
samba-debugsource-4.4.2-38.11.2
libtevent-util0-4.4.2-38.11.2
samba-client-debuginfo-32bit-4.4.2-38.11.2
libsamba-errors0-debuginfo-32bit-4.4.2-38.11.2
libsmbconf0-4.4.2-38.11.2
libndr-krb5pac0-debuginfo-4.4.2-38.11.2
libwbclient0-32bit-4.4.2-38.11.2
libndr-krb5pac0-4.4.2-38.11.2
samba-winbind-4.4.2-38.11.2
libsamba-passdb0-32bit-4.4.2-38.11.2
libsmbclient0-debuginfo-4.4.2-38.11.2
samba-winbind-debuginfo-32bit-4.4.2-38.11.2
samba-winbind-32bit-4.4.2-38.11.2
libsamba-credentials0-debuginfo-32bit-4.4.2-38.11.2
libsamba-hostconfig0-debuginfo-32bit-4.4.2-38.11.2
libsamba-util0-debuginfo-32bit-4.4.2-38.11.2
libsamba-credentials0-4.4.2-38.11.2
libsamba-credentials0-32bit-4.4.2-38.11.2
libndr-standard0-4.4.2-38.11.2
libsamba-passdb0-debuginfo-32bit-4.4.2-38.11.2
libsamba-util0-32bit-4.4.2-38.11.2
libndr-nbt0-debuginfo-4.4.2-38.11.2
libndr0-32bit-4.4.2-38.11.2
libndr-standard0-debuginfo-32bit-4.4.2-38.11.2
libwbclient0-debuginfo-4.4.2-38.11.2

libsmbconf0-debuginfo-32bit-4.4.2-38.11.2
libsamba-util0-debuginfo-4.4.2-38.11.2
libndr-standard0-debuginfo-4.4.2-38.11.2
libsmbclient0-4.4.2-38.11.2
libndr0-4.4.2-38.11.2
libndr0-debuginfo-32bit-4.4.2-38.11.2
libsmbclient0-32bit-4.4.2-38.11.2
samba-libs-4.4.2-38.11.2
libdcerpc-binding0-4.4.2-38.11.2
libdcerpc0-32bit-4.4.2-38.11.2
libsamba-passdb0-debuginfo-4.4.2-38.11.2
libsamba-errors0-4.4.2-38.11.2
libdcerpc-binding0-32bit-4.4.2-38.11.2
libsamdb0-4.4.2-38.11.2
libsamdb0-32bit-4.4.2-38.11.2
libwbclient0-debuginfo-32bit-4.4.2-38.11.2
libsamba-hostconfig0-debuginfo-4.4.2-38.11.2
libsamba-errors0-debuginfo-4.4.2-38.11.2
libndr-nbt0-4.4.2-38.11.2
samba-4.4.2-38.11.2
libsmbldap0-debuginfo-4.4.2-38.11.2
libtevent-util0-32bit-4.4.2-38.11.2
samba-client-4.4.2-38.11.2
libsamba-hostconfig0-4.4.2-38.11.2
libsamdb0-debuginfo-4.4.2-38.11.2
libndr-nbt0-32bit-4.4.2-38.11.2
libwbclient0-4.4.2-38.11.2
samba-debuginfo-4.4.2-38.11.2
libsamba-util0-4.4.2-38.11.2
libsmbldap0-4.4.2-38.11.2
libsmbconf0-32bit-4.4.2-38.11.2

noarch
samba-doc-4.4.2-38.11.2

SuSE SLES 12 SP2
noarch
samba-doc-4.4.2-38.11.2

x86_64
libsamba-credentials0-debuginfo-4.4.2-38.11.2
libsmbclient0-debuginfo-32bit-4.4.2-38.11.2
libtevent-util0-4.4.2-38.11.2
libndr-krb5pac0-debuginfo-32bit-4.4.2-38.11.2
libndr0-debuginfo-4.4.2-38.11.2
libdcerpc0-4.4.2-38.11.2
libsamba-errors0-32bit-4.4.2-38.11.2
samba-client-debuginfo-4.4.2-38.11.2
libndr-krb5pac0-32bit-4.4.2-38.11.2
libnetapi0-debuginfo-4.4.2-38.11.2
libsamba-util0-debuginfo-32bit-4.4.2-38.11.2
libdcerpc-binding0-debuginfo-4.4.2-38.11.2
libtevent-util0-debuginfo-4.4.2-38.11.2
libsmbldap0-32bit-4.4.2-38.11.2
libsmbldap0-debuginfo-32bit-4.4.2-38.11.2
samba-winbind-debuginfo-4.4.2-38.11.2
libsamba-passdb0-4.4.2-38.11.2
samba-libs-32bit-4.4.2-38.11.2
libsamba-hostconfig0-32bit-4.4.2-38.11.2
libtevent-util0-debuginfo-32bit-4.4.2-38.11.2
libdcerpc-binding0-debuginfo-32bit-4.4.2-38.11.2
libdcerpc0-debuginfo-4.4.2-38.11.2
libdcerpc0-debuginfo-32bit-4.4.2-38.11.2
libsamdb0-debuginfo-32bit-4.4.2-38.11.2
samba-client-32bit-4.4.2-38.11.2
libsmbconf0-debuginfo-4.4.2-38.11.2
libnetapi0-4.4.2-38.11.2
libndr-nbt0-debuginfo-32bit-4.4.2-38.11.2

libnetapi0-32bit-4.4.2-38.11.2
samba-debugsource-4.4.2-38.11.2
samba-client-4.4.2-38.11.2
samba-client-debuginfo-32bit-4.4.2-38.11.2
libsamba-errors0-debuginfo-32bit-4.4.2-38.11.2
libndr-standard0-debuginfo-4.4.2-38.11.2
libsmbconf0-4.4.2-38.11.2
libndr-krb5pac0-debuginfo-4.4.2-38.11.2
libwbclient0-32bit-4.4.2-38.11.2
libndr-krb5pac0-4.4.2-38.11.2
samba-winbind-4.4.2-38.11.2
libsamba-passdb0-32bit-4.4.2-38.11.2
libsmbclient0-debuginfo-4.4.2-38.11.2
samba-winbind-debuginfo-32bit-4.4.2-38.11.2
samba-winbind-32bit-4.4.2-38.11.2
libnetapi0-debuginfo-32bit-4.4.2-38.11.2
libsamba-credentials0-debuginfo-32bit-4.4.2-38.11.2
libsamba-hostconfig0-debuginfo-32bit-4.4.2-38.11.2
libndr-standard0-32bit-4.4.2-38.11.2
libsamba-credentials0-4.4.2-38.11.2
libsamba-credentials0-32bit-4.4.2-38.11.2
libndr-standard0-4.4.2-38.11.2
libsamba-passdb0-debuginfo-32bit-4.4.2-38.11.2
libsamba-util0-32bit-4.4.2-38.11.2
libndr-nbt0-debuginfo-4.4.2-38.11.2
libndr0-32bit-4.4.2-38.11.2
libndr-standard0-debuginfo-32bit-4.4.2-38.11.2
libwbclient0-debuginfo-4.4.2-38.11.2
libsmbconf0-debuginfo-32bit-4.4.2-38.11.2
libsamba-util0-debuginfo-4.4.2-38.11.2
samba-libs-debuginfo-4.4.2-38.11.2
libsmbclient0-4.4.2-38.11.2
libndr0-4.4.2-38.11.2
libndr0-debuginfo-32bit-4.4.2-38.11.2
libsmbclient0-32bit-4.4.2-38.11.2
samba-libs-4.4.2-38.11.2
libdcerpc-binding0-4.4.2-38.11.2
libdcerpc0-32bit-4.4.2-38.11.2
libsamba-passdb0-debuginfo-4.4.2-38.11.2
libsamba-errors0-4.4.2-38.11.2
libdcerpc-binding0-32bit-4.4.2-38.11.2
libsamdb0-4.4.2-38.11.2
libsamdb0-32bit-4.4.2-38.11.2
libwbclient0-debuginfo-32bit-4.4.2-38.11.2
libsamba-hostconfig0-debuginfo-4.4.2-38.11.2
libsamba-errors0-debuginfo-4.4.2-38.11.2
libndr-nbt0-4.4.2-38.11.2
samba-4.4.2-38.11.2
samba-libs-debuginfo-32bit-4.4.2-38.11.2
libsmbldap0-debuginfo-4.4.2-38.11.2
libtevent-util0-32bit-4.4.2-38.11.2
libsamba-hostconfig0-4.4.2-38.11.2
libsamdb0-debuginfo-4.4.2-38.11.2
libndr-nbt0-32bit-4.4.2-38.11.2
libwbclient0-4.4.2-38.11.2
samba-debuginfo-4.4.2-38.11.2
libsamba-util0-4.4.2-38.11.2
libsmbldap0-4.4.2-38.11.2
libsmbconf0-32bit-4.4.2-38.11.2

163472 - Oracle Enterprise Linux ELSA-2017-3629 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7541

Description

The scan detected that the host is missing the following update:
ELSA-2017-3629

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/007260.html
http://oss.oracle.com/pipermail/el-errata/2017-October/007261.html

OEL7
x86_64
kernel-uek-4.1.12-103.7.3.el7uek
kernel-uek-debug-4.1.12-103.7.3.el7uek
kernel-uek-devel-4.1.12-103.7.3.el7uek
kernel-uek-debug-devel-4.1.12-103.7.3.el7uek
kernel-uek-firmware-4.1.12-103.7.3.el7uek
kernel-uek-doc-4.1.12-103.7.3.el7uek

OEL6
x86_64
kernel-uek-debug-4.1.12-103.7.3.el6uek
kernel-uek-debug-devel-4.1.12-103.7.3.el6uek
kernel-uek-4.1.12-103.7.3.el6uek
kernel-uek-firmware-4.1.12-103.7.3.el6uek
kernel-uek-devel-4.1.12-103.7.3.el6uek
kernel-uek-doc-4.1.12-103.7.3.el6uek

163475 - Oracle Enterprise Linux ELSA-2017-2860 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546

Description

The scan detected that the host is missing the following update:
ELSA-2017-2860

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/007252.html

OEL6
x86_64
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

i386
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9

postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

170885 - Amazon Linux AMI ALAS-2017-908 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547

Description

The scan detected that the host is missing the following update:
ALAS-2017-908

Observation

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

https://alas.aws.amazon.com/ALAS-2017-908.html

Amazon Linux AMI
x86_64
postgresql96-test-9.6.4-1.77.amzn1
postgresql96-devel-9.6.4-1.77.amzn1
postgresql96-plperl-9.6.4-1.77.amzn1
postgresql96-contrib-9.6.4-1.77.amzn1
postgresql96-static-9.6.4-1.77.amzn1
postgresql96-server-9.6.4-1.77.amzn1
postgresql96-docs-9.6.4-1.77.amzn1
postgresql96-debuginfo-9.6.4-1.77.amzn1
postgresql96-libs-9.6.4-1.77.amzn1
postgresql96-plpython27-9.6.4-1.77.amzn1
postgresql96-9.6.4-1.77.amzn1
postgresql96-plpython26-9.6.4-1.77.amzn1

i686
postgresql96-docs-9.6.4-1.77.amzn1
postgresql96-devel-9.6.4-1.77.amzn1
postgresql96-plperl-9.6.4-1.77.amzn1
postgresql96-contrib-9.6.4-1.77.amzn1
postgresql96-static-9.6.4-1.77.amzn1
postgresql96-test-9.6.4-1.77.amzn1
postgresql96-debuginfo-9.6.4-1.77.amzn1
postgresql96-plpython27-9.6.4-1.77.amzn1
postgresql96-libs-9.6.4-1.77.amzn1
postgresql96-server-9.6.4-1.77.amzn1
postgresql96-9.6.4-1.77.amzn1
postgresql96-plpython26-9.6.4-1.77.amzn1

175271 - Scientific Linux Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1710-6234)

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

Risk Level: High

CVE: CVE-2017-7541

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1710-6234)

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=6234

SL6
i386
kernel-debug-debuginfo-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-debuginfo-common-i686-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-debuginfo-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6
perf-debuginfo-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6
python-perf-debuginfo-2.6.32-696.13.2.el6

noarch
kernel-firmware-2.6.32-696.13.2.el6
kernel-doc-2.6.32-696.13.2.el6
kernel-abi-whitelists-2.6.32-696.13.2.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-696.13.2.el6
kernel-debuginfo-common-x86_64-2.6.32-696.13.2.el6
python-perf-debuginfo-2.6.32-696.13.2.el6
perf-debuginfo-2.6.32-696.13.2.el6
kernel-debuginfo-2.6.32-696.13.2.el6
kernel-headers-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-debuginfo-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6

175272 - Scientific Linux Security ERRATA Moderate: postgresql on SL6.x i386/x86_64 (1710-5899)

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

Risk Level: High

CVE: CVE-2017-7546

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: postgresql on SL6.x i386/x86_64 (1710-5899)

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=5899

SL6
x86_64
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9

postgresql-plperl-8.4.20-8.el6_9
postgresql-debuginfo-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

i386
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-debuginfo-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

178515 - Gentoo Linux GLSA-201710-07 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-201710-07

Observation

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

https://security.gentoo.org/glsa/201710-07

Affected packages:
dev-lang/ocaml < 4.04.2

178521 - Gentoo Linux GLSA-201710-04 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-201710-04

Observation

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

https://security.gentoo.org/glsa/201710-04

Affected packages:
app-admin/sudo < 1.8.20_p2

185905 - Ubuntu Linux 16.04 USN-3444-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12134, CVE-2017-14106, CVE-2017-14140

Description

The scan detected that the host is missing the following update:
USN-3444-1

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/004082.html

Ubuntu 16.04

linux-image-powerpc-smp_4.4.0.97.102
linux-image-4.4.0-1077-snapdragon_4.4.0-1077.82
linux-image-kvm_4.4.0.1008.8
linux-image-gke_4.4.0.1032.33
linux-image-raspi2_4.4.0.1075.75
linux-image-4.4.0-97-generic-lpae_4.4.0-97.120
linux-image-powerpc-e500mc_4.4.0.97.102
linux-image-4.4.0-1038-aws_4.4.0-1038.47
linux-image-4.4.0-97-generic_4.4.0-97.120
linux-image-generic_4.4.0.97.102
linux-image-4.4.0-97-powerpc64-smp_4.4.0-97.120
linux-image-generic-lpae_4.4.0.97.102
linux-image-4.4.0-1008-kvm_4.4.0-1008.13
linux-image-snapdragon_4.4.0.1077.69
linux-image-powerpc64-emb_4.4.0.97.102
linux-image-aws_4.4.0.1038.40
linux-image-4.4.0-97-powerpc-e500mc_4.4.0-97.120
linux-image-powerpc64-smp_4.4.0.97.102
linux-image-4.4.0-97-lowlatency_4.4.0-97.120
linux-image-4.4.0-1075-raspi2_4.4.0-1075.83
linux-image-4.4.0-97-powerpc-smp_4.4.0-97.120
linux-image-lowlatency_4.4.0.97.102
linux-image-4.4.0-1032-gke_4.4.0-1032.32
linux-image-4.4.0-97-powerpc64-emb_4.4.0-97.120

185910 - Ubuntu Linux 14.04 USN-3444-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12134, CVE-2017-14106, CVE-2017-14140

Description

The scan detected that the host is missing the following update:
USN-3444-2

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/004084.html

Ubuntu 14.04

linux-image-4.4.0-97-lowlatency_4.4.0-97.120~14.04.1
linux-image-powerpc-smp-lts-xenial_4.4.0.97.81
linux-image-4.4.0-97-powerpc64-smp_4.4.0-97.120~14.04.1
linux-image-powerpc64-emb-lts-xenial_4.4.0.97.81
linux-image-4.4.0-97-powerpc64-emb_4.4.0-97.120~14.04.1
linux-image-4.4.0-97-powerpc-smp_4.4.0-97.120~14.04.1
linux-image-4.4.0-97-generic-lpae_4.4.0-97.120~14.04.1
linux-image-4.4.0-97-generic_4.4.0-97.120~14.04.1

linux-image-lowlatency-lts-xenial_4.4.0.97.81
linux-image-powerpc64-smp-lts-xenial_4.4.0.97.81
linux-image-generic-lpae-lts-xenial_4.4.0.97.81
linux-image-generic-lts-xenial_4.4.0.97.81
linux-image-powerpc-e500mc-lts-xenial_4.4.0.97.81
linux-image-4.4.0-97-powerpc-e500mc_4.4.0-97.120~14.04.1

192756 - Fedora Linux 25 FEDORA-2017-7a3ddf2484 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14497

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7a3ddf2484

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=5

Fedora Core 25

kernel-4.12.14-200.fc25

192759 - Fedora Linux 27 FEDORA-2017-4f2fbc84d9 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14339

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4f2fbc84d9

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

yadifa-2.2.6-1.fc27

141743 - Red Hat Enterprise Linux RHSA-2017-2869 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7533

Description

The scan detected that the host is missing the following update:
RHSA-2017-2869

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/msg00009.html

RHEL7_2S
noarch
kernel-abi-whitelists-3.10.0-327.61.3.el7
kernel-doc-3.10.0-327.61.3.el7

x86_64
kernel-debug-3.10.0-327.61.3.el7
kernel-3.10.0-327.61.3.el7
kernel-debug-devel-3.10.0-327.61.3.el7
python-perf-debuginfo-3.10.0-327.61.3.el7
kernel-tools-debuginfo-3.10.0-327.61.3.el7
kernel-debug-debuginfo-3.10.0-327.61.3.el7
kernel-tools-3.10.0-327.61.3.el7
perf-debuginfo-3.10.0-327.61.3.el7
python-perf-3.10.0-327.61.3.el7
kernel-tools-libs-devel-3.10.0-327.61.3.el7
kernel-debuginfo-common-x86_64-3.10.0-327.61.3.el7
kernel-debuginfo-3.10.0-327.61.3.el7
kernel-devel-3.10.0-327.61.3.el7
perf-3.10.0-327.61.3.el7
kernel-headers-3.10.0-327.61.3.el7
kernel-tools-libs-3.10.0-327.61.3.el7

145971 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2649-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10507, CVE-2017-14039, CVE-2017-14040, CVE-2017-14041, CVE-2017-14164

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2649-1

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/003274.html

SuSE SLES 12 SP2
x86_64
openjpeg2-debuginfo-2.1.0-4.6.1
libopenjp2-7-2.1.0-4.6.1
libopenjp2-7-debuginfo-2.1.0-4.6.1
openjpeg2-debugsource-2.1.0-4.6.1

SuSE SLED 12 SP3
x86_64
openjpeg2-debuginfo-2.1.0-4.6.1
libopenjp2-7-2.1.0-4.6.1
libopenjp2-7-debuginfo-2.1.0-4.6.1
openjpeg2-debugsource-2.1.0-4.6.1

SuSE SLED 12 SP2
x86_64
openjpeg2-debuginfo-2.1.0-4.6.1
libopenjp2-7-2.1.0-4.6.1
libopenjp2-7-debuginfo-2.1.0-4.6.1
openjpeg2-debugsource-2.1.0-4.6.1

SuSE SLES 12 SP3
x86_64

openjpeg2-debuginfo-2.1.0-4.6.1
libopenjp2-7-2.1.0-4.6.1
libopenjp2-7-debuginfo-2.1.0-4.6.1
openjpeg2-debugsource-2.1.0-4.6.1

145973 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2686-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10507, CVE-2017-14039, CVE-2017-14040, CVE-2017-14041, CVE-2017-14164

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2686-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00032.html

SuSE Linux 42.2
x86_64
libopenjp2-7-2.1.0-13.6.1
openjpeg2-devel-2.1.0-13.6.1
libopenjp2-7-debuginfo-2.1.0-13.6.1
openjpeg2-2.1.0-13.6.1
openjpeg2-debugsource-2.1.0-13.6.1
libopenjp2-7-32bit-2.1.0-13.6.1
openjpeg2-debuginfo-2.1.0-13.6.1
libopenjp2-7-debuginfo-32bit-2.1.0-13.6.1

i586
libopenjp2-7-2.1.0-13.6.1
openjpeg2-devel-2.1.0-13.6.1
libopenjp2-7-debuginfo-2.1.0-13.6.1
openjpeg2-2.1.0-13.6.1
openjpeg2-debugsource-2.1.0-13.6.1
openjpeg2-debuginfo-2.1.0-13.6.1

SuSE Linux 42.3
x86_64
openjpeg2-debugsource-2.1.0-19.1
openjpeg2-debuginfo-2.1.0-19.1
libopenjp2-7-32bit-2.1.0-19.1
libopenjp2-7-debuginfo-32bit-2.1.0-19.1
openjpeg2-2.1.0-19.1
libopenjp2-7-debuginfo-2.1.0-19.1
libopenjp2-7-2.1.0-19.1
openjpeg2-devel-2.1.0-19.1

i586
openjpeg2-debugsource-2.1.0-19.1
openjpeg2-debuginfo-2.1.0-19.1
openjpeg2-2.1.0-19.1
libopenjp2-7-debuginfo-2.1.0-19.1
libopenjp2-7-2.1.0-19.1
openjpeg2-devel-2.1.0-19.1

185902 - Ubuntu Linux 14.04 USN-3445-1 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-3445-1

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/004083.html

Ubuntu 14.04

linux-image-3.13.0-133-powerpc-e500_3.13.0-133.182
linux-image-powerpc-smp_3.13.0.133.142
linux-image-powerpc-e500_3.13.0.133.142
linux-image-generic-lpae_3.13.0.133.142
linux-image-powerpc64-smp_3.13.0.133.142
linux-image-generic_3.13.0.133.142
linux-image-3.13.0-133-powerpc64-smp_3.13.0-133.182
linux-image-3.13.0-133-generic-lpae_3.13.0-133.182
linux-image-powerpc-e500mc_3.13.0.133.142
linux-image-lowlatency_3.13.0.133.142
linux-image-3.13.0-133-powerpc-smp_3.13.0-133.182
linux-image-3.13.0-133-lowlatency_3.13.0-133.182
linux-image-3.13.0-133-generic_3.13.0-133.182
linux-image-3.13.0-133-powerpc-e500mc_3.13.0-133.182
linux-image-3.13.0-133-powerpc64-emb_3.13.0-133.182
linux-image-powerpc64-emb_3.13.0.133.142

192753 - Fedora Linux 25 FEDORA-2017-b97f9d82dc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11423, CVE-2017-6419

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b97f9d82dc

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

libmspack-0.6-0.1.alpha.fc25

22506 - (K43945001) F5 BIG-IP F5 TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6147

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the management of SSL forward proxy feature. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

145974 - SuSE Linux 42.3 openSUSE-SU-2017:2682-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10683

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2682-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00028.html

SuSE Linux 42.3
x86_64
mpg123-debuginfo-1.25.7-10.1
mpg123-esound-debuginfo-1.25.7-10.1
mpg123-openal-1.25.7-10.1
mpg123-portaudio-debuginfo-32bit-1.25.7-10.1
libout123-0-debuginfo-1.25.7-10.1
mpg123-openal-debuginfo-1.25.7-10.1
libout123-0-debuginfo-32bit-1.25.7-10.1
mpg123-esound-32bit-1.25.7-10.1
mpg123-devel-1.25.7-10.1
libmpg123-0-debuginfo-32bit-1.25.7-10.1
mpg123-sdl-32bit-1.25.7-10.1
mpg123-pulse-debuginfo-1.25.7-10.1
mpg123-jack-1.25.7-10.1
mpg123-pulse-1.25.7-10.1
mpg123-portaudio-32bit-1.25.7-10.1
libmpg123-0-1.25.7-10.1
mpg123-jack-debuginfo-1.25.7-10.1
mpg123-debugsource-1.25.7-10.1
mpg123-openal-32bit-1.25.7-10.1
mpg123-jack-32bit-1.25.7-10.1
mpg123-openal-debuginfo-32bit-1.25.7-10.1
mpg123-pulse-32bit-1.25.7-10.1
mpg123-sdl-debuginfo-32bit-1.25.7-10.1
mpg123-sdl-debuginfo-1.25.7-10.1
mpg123-pulse-debuginfo-32bit-1.25.7-10.1
mpg123-esound-debuginfo-32bit-1.25.7-10.1
mpg123-esound-1.25.7-10.1
mpg123-1.25.7-10.1
libmpg123-0-32bit-1.25.7-10.1
mpg123-sdl-1.25.7-10.1
mpg123-portaudio-1.25.7-10.1
mpg123-portaudio-debuginfo-1.25.7-10.1
libout123-0-1.25.7-10.1
mpg123-jack-debuginfo-32bit-1.25.7-10.1
libout123-0-32bit-1.25.7-10.1
mpg123-devel-32bit-1.25.7-10.1
libmpg123-0-debuginfo-1.25.7-10.1

i586
mpg123-pulse-debuginfo-1.25.7-10.1
mpg123-sdl-debuginfo-1.25.7-10.1
mpg123-portaudio-debuginfo-1.25.7-10.1

mpg123-openal-debuginfo-1.25.7-10.1
mpg123-openal-1.25.7-10.1
mpg123-devel-1.25.7-10.1
mpg123-1.25.7-10.1
libout123-0-debuginfo-1.25.7-10.1
mpg123-jack-1.25.7-10.1
libout123-0-1.25.7-10.1
mpg123-portaudio-1.25.7-10.1
mpg123-esound-debuginfo-1.25.7-10.1
mpg123-debugsource-1.25.7-10.1
mpg123-pulse-1.25.7-10.1
libmpg123-0-debuginfo-1.25.7-10.1
mpg123-jack-debuginfo-1.25.7-10.1
mpg123-debuginfo-1.25.7-10.1
libmpg123-0-1.25.7-10.1
mpg123-esound-1.25.7-10.1
mpg123-sdl-1.25.7-10.1

160309 - CentOS 6 CESA-2017-2863 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-2017-2863

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/022564.html

CentOS 6
i686
kernel-headers-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6

noarch
kernel-firmware-2.6.32-696.13.2.el6
kernel-doc-2.6.32-696.13.2.el6
kernel-abi-whitelists-2.6.32-696.13.2.el6

x86_64
kernel-headers-2.6.32-696.13.2.el6
kernel-devel-2.6.32-696.13.2.el6
kernel-2.6.32-696.13.2.el6
perf-2.6.32-696.13.2.el6
kernel-debug-devel-2.6.32-696.13.2.el6
kernel-debug-2.6.32-696.13.2.el6
python-perf-2.6.32-696.13.2.el6

160310 - CentOS 6 CESA-2017-2860 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-2017-2860

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/022563.html

CentOS 6
x86_64
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

i686
postgresql-contrib-8.4.20-8.el6_9
postgresql-libs-8.4.20-8.el6_9
postgresql-docs-8.4.20-8.el6_9
postgresql-test-8.4.20-8.el6_9
postgresql-plpython-8.4.20-8.el6_9
postgresql-devel-8.4.20-8.el6_9
postgresql-pltcl-8.4.20-8.el6_9
postgresql-plperl-8.4.20-8.el6_9
postgresql-server-8.4.20-8.el6_9
postgresql-8.4.20-8.el6_9

178514 - Gentoo Linux GLSA-201710-03 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-201710-03

Observation

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

https://security.gentoo.org/glsa/201710-03

Affected packages:
dev-libs/icu < 58.2-r1

178516 - Gentoo Linux GLSA-201710-01 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-201710-01

Observation

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

https://security.gentoo.org/glsa/201710-01

Affected packages:
dev-ruby/rubygems < 2.6.13

178517 - Gentoo Linux GLSA-201710-02 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-201710-02

Observation

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

https://security.gentoo.org/glsa/201710-02

Affected packages:
sys-apps/file < 5.32

178518 - Gentoo Linux GLSA-201710-08 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-201710-08

Observation

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

https://security.gentoo.org/glsa/201710-08

Affected packages:
sys-cluster/pacemaker < 1.1.16

178519 - Gentoo Linux GLSA-201710-05 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-201710-05

Observation

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

https://security.gentoo.org/glsa/201710-05

Affected packages:
net-analyzer/munin < 2.0.33

178520 - Gentoo Linux GLSA-201710-09 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-201710-09

Observation

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

https://security.gentoo.org/glsa/201710-09

Affected packages:
dev-libs/libpcre2 < 10.30

182472 - FreeBSD node Access To Unintended Files (1257718e-be97-458a-9744-d938b592db42)

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

Risk Level: Medium

CVE: CVE-2017-14849

Description

The scan detected that the host is missing the following update:
node -- access to unintended files (1257718e-be97-458a-9744-d938b592db42)

Observation

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

http://www.vuxml.org/freebsd/1257718e-be97-458a-9744-d938b592db42.html

Affected packages:
8.5.0 <= node < 8.6.0

192764 - Fedora Linux 27 FEDORA-2017-b2c714515b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0375, CVE-2017-0376, CVE-2017-0380

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b2c714515b

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

tor-0.3.1.7-1.fc27

130901 - Debian Linux 9.0 DSA-3994-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14604

Description

The scan detected that the host is missing the following update:
DSA-3994-1

Observation

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

http://www.debian.org/security/2017/dsa-3994

Debian 9.0
all
nautilus_3.22.3-1+deb9u1

130903 - Debian Linux 9.0 DSA-3993-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0380

Description

The scan detected that the host is missing the following update:
DSA-3993-1

Observation

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

http://www.debian.org/security/2017/dsa-3993

Debian 9.0
all
tor_0.2.9.12-1

182475 - FreeBSD libtiff Improper Input Validation (9b5a905f-e556-452f-a00c-8f070a086181)

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

Risk Level: Medium

CVE: CVE-2017-13726, CVE-2017-13727

Description

The scan detected that the host is missing the following update:
libtiff -- Improper Input Validation (9b5a905f-e556-452f-a00c-8f070a086181)

Observation

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

http://www.vuxml.org/freebsd/9b5a905f-e556-452f-a00c-8f070a086181.html

Affected packages:
libtiff <= 4.0.8

185901 - Ubuntu Linux 16.04 USN-3443-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000255, CVE-2017-14106

Description

The scan detected that the host is missing the following update:
USN-3443-2

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/004080.html

Ubuntu 16.04

linux-image-4.10.0-37-lowlatency_4.10.0-37.41~16.04.1
linux-image-generic-lpae-hwe-16.04_4.10.0.37.39
linux-image-4.10.0-37-generic_4.10.0-37.41~16.04.1
linux-image-generic-hwe-16.04_4.10.0.37.39
linux-image-4.10.0-37-generic-lpae_4.10.0-37.41~16.04.1
linux-image-lowlatency-hwe-16.04_4.10.0.37.39

185904 - Ubuntu Linux 17.04 USN-3443-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000255, CVE-2017-14106

Description

The scan detected that the host is missing the following update:
USN-3443-1

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/004079.html

Ubuntu 17.04

linux-image-lowlatency_4.10.0.37.37
linux-image-4.10.0-37-generic_4.10.0-37.41
linux-image-generic_4.10.0.37.37
linux-image-powerpc64-smp_4.10.0.37.37
linux-image-virtual_4.10.0.37.37
linux-image-powerpc-e500mc_4.10.0.37.37
linux-image-4.10.0-37-lowlatency_4.10.0-37.41
linux-image-powerpc-smp_4.10.0.37.37
linux-image-raspi2_4.10.0.1019.20
linux-image-4.10.0-1019-raspi2_4.10.0-1019.22
linux-image-generic-lpae_4.10.0.37.37
linux-image-4.10.0-37-generic-lpae_4.10.0-37.41
linux-image-powerpc64-emb_4.10.0.37.37

192754 - Fedora Linux 27 FEDORA-2017-b4329d6ee5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13672, CVE-2017-13673

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b4329d6ee5

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

xen-4.9.0-11.fc27

192755 - Fedora Linux 26 FEDORA-2017-c9abeb3158 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10840, CVE-2017-10841

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c9abeb3158

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

WebCalendar-1.2.9-1.fc26

192758 - Fedora Linux 26 FEDORA-2017-897a192750 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-2017-897a192750

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

ImageMagick-6.9.9.15-1.fc26
rubygem-rmagick-2.16.0-7.fc26

192762 - Fedora Linux 25 FEDORA-2017-26a53ccbdf Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10840, CVE-2017-10841

Description

The scan detected that the host is missing the following update:
FEDORA-2017-26a53ccbdf

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 25

WebCalendar-1.2.9-1.fc25

192766 - Fedora Linux 27 FEDORA-2017-6abd55703b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10840, CVE-2017-10841

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6abd55703b

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

WebCalendar-1.2.9-1.fc27

130902 - Debian Linux 8.0, 9.0 DSA-3992-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254

Description

The scan detected that the host is missing the following update:
DSA-3992-1

Observation

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

http://www.debian.org/security/2017/dsa-3992

Debian 8.0
all
curl_7.38.0-4+deb8u6

Debian 9.0
all
curl_7.52.1-5+deb9u1

182473 - FreeBSD xorg-server Multiple Vulnabilities (4f8ffb9c-f388-4fbd-b90f-b3131559d888)

Category: SSH Module -> NonIntrusive -> FreeBSD 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:
xorg-server -- multiple vulnabilities (4f8ffb9c-f388-4fbd-b90f-b3131559d888)

Observation

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

http://www.vuxml.org/freebsd/4f8ffb9c-f388-4fbd-b90f-b3131559d888.html

Affected packages:
xephyr < 1.18.4_4,1
xorg-dmx < 1.18.4_4,1
xorg-nestserver < 1.19.1_1,2
xorg-server < 1.18.4_4,1
xorg-vfbserver < 1.19.1_1,1
xwayland < 1.19.1_1

182474 - FreeBSD zookeeper Denial Of Service (af61b271-9e47-4db0-a0f6-29fb032236a3)

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

Risk Level: Low

CVE: CVE-2017-5637

Description

The scan detected that the host is missing the following update:
zookeeper -- Denial Of Service (af61b271-9e47-4db0-a0f6-29fb032236a3)

Observation

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

http://www.vuxml.org/freebsd/af61b271-9e47-4db0-a0f6-29fb032236a3.html

Affected packages:
zookeeper < 3.4.10

182476 - FreeBSD rubygems Deserialization Vulnerability (2c8bd00d-ada2-11e7-82af-8dbff7d75206)

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

Risk Level: Low

CVE: CVE-2017-0903

Description

The scan detected that the host is missing the following update:
rubygems -- deserialization vulnerability (2c8bd00d-ada2-11e7-82af-8dbff7d75206)

Observation

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

http://www.vuxml.org/freebsd/2c8bd00d-ada2-11e7-82af-8dbff7d75206.html

Affected packages:
ruby22-gems < 2.6.14
ruby23-gems < 2.6.14
ruby24-gems < 2.6.14

182477 - FreeBSD tomcat Remote Code Execution (c0dae634-4820-4505-850d-b1c975d0f67d)

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

Risk Level: Low

CVE: CVE-2017-12617

Description

The scan detected that the host is missing the following update:
tomcat -- Remote Code Execution (c0dae634-4820-4505-850d-b1c975d0f67d)

Observation

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

http://www.vuxml.org/freebsd/c0dae634-4820-4505-850d-b1c975d0f67d.html

Affected packages:
7.0.0 <= tomcat <= 7.0.81
8.0.0 <= tomcat <= 8.0.46
8.5.0 <= tomcat <= 8.5.22
9.0.0 <= tomcat < 9.0.1

185903 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3438-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14867

Description

The scan detected that the host is missing the following update:
USN-3438-1

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/004073.html

Ubuntu 16.04

git_2.7.4-0ubuntu1.3

Ubuntu 14.04

git_1.9.1-1ubuntu0.7

Ubuntu 17.04

git_2.11.0-2ubuntu0.3

185908 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3435-2 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-2017-7811, CVE-2017-7812, CVE-2017-7813, CVE-2017-7814, CVE-2017-7815, CVE-2017-7816, CVE-2017-7818, CVE-2017-7819, CVE-2017-7820, CVE-2017-7821, CVE-2017-7822, CVE-2017-7823, CVE-2017-7824

Description

The scan detected that the host is missing the following update:
USN-3435-2

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/004072.html

Ubuntu 16.04

firefox_56.0+build6-0ubuntu0.16.04.2

Ubuntu 14.04

firefox_56.0+build6-0ubuntu0.14.04.2

Ubuntu 17.04

firefox_56.0+build6-0ubuntu0.17.04.2

185909 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3442-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu 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:
USN-3442-1

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/004077.html

Ubuntu 16.04

libxfont2_2.0.1-3~ubuntu16.04.2
libxfont1_1.5.1-1ubuntu0.16.04.3

Ubuntu 14.04

libxfont1_1.4.7-1ubuntu0.3

Ubuntu 17.04

libxfont2_2.0.1-3ubuntu0.1
libxfont1_1.5.2-4ubuntu0.1

192752 - Fedora Linux 26 FEDORA-2017-24f067299e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496

Description

The scan detected that the host is missing the following update:
FEDORA-2017-24f067299e

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

dnsmasq-2.76-5.fc26

192757 - Fedora Linux 27 FEDORA-2017-cf6bb19709 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-cf6bb19709

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

recode-3.6-46.fc27

192760 - Fedora Linux 25 FEDORA-2017-581be259ef Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-581be259ef

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

samba-4.5.14-0.fc25

192761 - Fedora Linux 25 FEDORA-2017-19c1fd28f5 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-2017-19c1fd28f5

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

MySQL-zrm-3.0-17.fc25

192763 - Fedora Linux 26 FEDORA-2017-3adc791de1 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-2017-3adc791de1

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 26

MySQL-zrm-3.0-17.fc26

185907 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3441-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254, CVE-2017-7407

Description

The scan detected that the host is missing the following update:
USN-3441-1

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/004076.html

Ubuntu 16.04

curl_7.47.0-1ubuntu2.3
libcurl3-nss_7.47.0-1ubuntu2.3
libcurl3_7.47.0-1ubuntu2.3
libcurl3-gnutls_7.47.0-1ubuntu2.3

Ubuntu 14.04

libcurl3-nss_7.35.0-1ubuntu2.11
libcurl3-gnutls_7.35.0-1ubuntu2.11

curl_7.35.0-1ubuntu2.11
libcurl3_7.35.0-1ubuntu2.11

Ubuntu 17.04

curl_7.52.1-4ubuntu1.2
libcurl3_7.52.1-4ubuntu1.2
libcurl3-nss_7.52.1-4ubuntu1.2
libcurl3-gnutls_7.52.1-4ubuntu1.2

192765 - Fedora Linux 26 FEDORA-2017-c0e81a1c7a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14954

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c0e81a1c7a

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 26

kernel-4.13.4-200.fc26

22597 - Microsoft Office 2016 Click-To-Run October 2017 Updates

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run.

Observation

Microsoft Office 2016 Click-to-Run is an alternative to the Windows Installer-based (MSI) installation method of the popular office suite.

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run. The flaws are present in multiple components. Such defects could lead the product to software vulnerabilities, malfunction or unexpected behavior in some of its affected components.

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.

160306 - CentOS 6 CESA-2017-2838 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14491

Update Details

CVE is updated

4617 - Microsoft Windows Service Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

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.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.