2017-OCT-25
FSL version 7.5.970

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

141759 - Red Hat Enterprise Linux RHSA-2017-2930 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558

Description

The scan detected that the host is missing the following update:
RHSA-2017-2930

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/msg00025.html

RHEL7D
x86_64
kernel-debug-3.10.0-693.5.2.el7
perf-debuginfo-3.10.0-693.5.2.el7
kernel-headers-3.10.0-693.5.2.el7
kernel-debuginfo-common-x86_64-3.10.0-693.5.2.el7
kernel-tools-3.10.0-693.5.2.el7
kernel-tools-debuginfo-3.10.0-693.5.2.el7
python-perf-debuginfo-3.10.0-693.5.2.el7
kernel-tools-libs-3.10.0-693.5.2.el7
kernel-debuginfo-3.10.0-693.5.2.el7
kernel-3.10.0-693.5.2.el7
kernel-devel-3.10.0-693.5.2.el7
python-perf-3.10.0-693.5.2.el7
kernel-debug-debuginfo-3.10.0-693.5.2.el7
kernel-tools-libs-devel-3.10.0-693.5.2.el7
perf-3.10.0-693.5.2.el7
kernel-debug-devel-3.10.0-693.5.2.el7

noarch
kernel-abi-whitelists-3.10.0-693.5.2.el7
kernel-doc-3.10.0-693.5.2.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-693.5.2.el7
kernel-doc-3.10.0-693.5.2.el7

x86_64

kernel-debug-3.10.0-693.5.2.el7
perf-debuginfo-3.10.0-693.5.2.el7
kernel-headers-3.10.0-693.5.2.el7
kernel-debuginfo-common-x86_64-3.10.0-693.5.2.el7
kernel-tools-3.10.0-693.5.2.el7
kernel-tools-debuginfo-3.10.0-693.5.2.el7
python-perf-debuginfo-3.10.0-693.5.2.el7
kernel-tools-libs-3.10.0-693.5.2.el7
kernel-debuginfo-3.10.0-693.5.2.el7
kernel-3.10.0-693.5.2.el7
kernel-devel-3.10.0-693.5.2.el7
python-perf-3.10.0-693.5.2.el7
kernel-debug-debuginfo-3.10.0-693.5.2.el7
kernel-tools-libs-devel-3.10.0-693.5.2.el7
perf-3.10.0-693.5.2.el7
kernel-debug-devel-3.10.0-693.5.2.el7

RHEL7WS
x86_64
kernel-debug-3.10.0-693.5.2.el7
perf-debuginfo-3.10.0-693.5.2.el7
kernel-headers-3.10.0-693.5.2.el7
kernel-debuginfo-common-x86_64-3.10.0-693.5.2.el7
kernel-tools-3.10.0-693.5.2.el7
kernel-tools-debuginfo-3.10.0-693.5.2.el7
python-perf-debuginfo-3.10.0-693.5.2.el7
kernel-tools-libs-3.10.0-693.5.2.el7
kernel-debuginfo-3.10.0-693.5.2.el7
kernel-3.10.0-693.5.2.el7
kernel-devel-3.10.0-693.5.2.el7
python-perf-3.10.0-693.5.2.el7
kernel-debug-debuginfo-3.10.0-693.5.2.el7
kernel-tools-libs-devel-3.10.0-693.5.2.el7
perf-3.10.0-693.5.2.el7
kernel-debug-devel-3.10.0-693.5.2.el7

noarch
kernel-abi-whitelists-3.10.0-693.5.2.el7
kernel-doc-3.10.0-693.5.2.el7

163479 - Oracle Enterprise Linux ELSA-2017-2930 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-1000251, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558

Description

The scan detected that the host is missing the following update:
ELSA-2017-2930

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/007297.html
http://oss.oracle.com/pipermail/el-errata/2017-October/007282.html

OEL7
x86_64
kernel-headers-3.10.0-693.5.2.0.1.el7
kernel-debug-3.10.0-693.5.2.el7
kernel-doc-3.10.0-693.5.2.el7
python-perf-3.10.0-693.5.2.0.1.el7
kernel-headers-3.10.0-693.5.2.el7
kernel-tools-libs-3.10.0-693.5.2.0.1.el7
kernel-tools-3.10.0-693.5.2.el7
kernel-debug-3.10.0-693.5.2.0.1.el7
kernel-doc-3.10.0-693.5.2.0.1.el7
kernel-tools-libs-devel-3.10.0-693.5.2.0.1.el7
kernel-abi-whitelists-3.10.0-693.5.2.0.1.el7
kernel-debug-devel-3.10.0-693.5.2.0.1.el7
perf-3.10.0-693.5.2.0.1.el7
kernel-tools-libs-3.10.0-693.5.2.el7
kernel-abi-whitelists-3.10.0-693.5.2.el7
kernel-devel-3.10.0-693.5.2.0.1.el7
kernel-3.10.0-693.5.2.el7
kernel-tools-3.10.0-693.5.2.0.1.el7
kernel-devel-3.10.0-693.5.2.el7
python-perf-3.10.0-693.5.2.el7
kernel-3.10.0-693.5.2.0.1.el7
kernel-tools-libs-devel-3.10.0-693.5.2.el7
perf-3.10.0-693.5.2.el7
kernel-debug-devel-3.10.0-693.5.2.el7

175275 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1710-12344)

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

Risk Level: High

CVE: CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1710-12344)

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=12344

SL7
x86_64
kernel-debug-3.10.0-693.5.2.el7
perf-debuginfo-3.10.0-693.5.2.el7
kernel-headers-3.10.0-693.5.2.el7
kernel-debuginfo-common-x86_64-3.10.0-693.5.2.el7
kernel-tools-3.10.0-693.5.2.el7
kernel-tools-debuginfo-3.10.0-693.5.2.el7
python-perf-debuginfo-3.10.0-693.5.2.el7
kernel-tools-libs-3.10.0-693.5.2.el7
kernel-debuginfo-3.10.0-693.5.2.el7
kernel-3.10.0-693.5.2.el7
kernel-devel-3.10.0-693.5.2.el7
python-perf-3.10.0-693.5.2.el7

kernel-debug-debuginfo-3.10.0-693.5.2.el7
kernel-tools-libs-devel-3.10.0-693.5.2.el7
perf-3.10.0-693.5.2.el7
kernel-debug-devel-3.10.0-693.5.2.el7

noarch
kernel-abi-whitelists-3.10.0-693.5.2.el7
kernel-doc-3.10.0-693.5.2.el7

22615 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52.4

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

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

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful exploitation could allow a malicious user to conduct spoofing attacks and cross-site scripting (XSS) attacks, bypass security restrictions, cause a denial of service condition or remotely execute arbitrary code on the target system.

22616 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52.4

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

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

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful exploitation could allow a malicious user to conduct spoofing attacks and cross-site scripting (XSS) attacks, bypass security restrictions, cause a denial of service condition or remotely execute arbitrary code on the target system.

146010 - SuSE Linux 42.2 openSUSE-SU-2017:2757-1 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:
openSUSE-SU-2017:2757-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00056.html

SuSE Linux 42.2
x86_64
git-2.12.3-5.14.1
git-svn-2.12.3-5.14.1
git-svn-debuginfo-2.12.3-5.14.1
git-credential-gnome-keyring-debuginfo-2.12.3-5.14.1
git-arch-2.12.3-5.14.1
gitk-2.12.3-5.14.1
git-cvs-2.12.3-5.14.1
git-debugsource-2.12.3-5.14.1
git-web-2.12.3-5.14.1
git-gui-2.12.3-5.14.1
git-credential-gnome-keyring-2.12.3-5.14.1
git-core-debuginfo-2.12.3-5.14.1
git-core-2.12.3-5.14.1
git-daemon-2.12.3-5.14.1
git-email-2.12.3-5.14.1
git-daemon-debuginfo-2.12.3-5.14.1

noarch
git-doc-2.12.3-5.14.1

160316 - CentOS 6, 7 CESA-2017-2998 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-2017-2998

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/022571.html
http://lists.centos.org/pipermail/centos-announce/2017-October/022603.html

CentOS 7
i686
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el7_4

java-1.8.0-openjdk-src-1.8.0.151-1.b12.el7_4

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.151-1.b12.el7_4

x86_64
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el7_4

CentOS 6
i686
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el6_9

x86_64
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9

22620 - Cisco IOS Software Common Industrial Protocol Request Denial of Service Vulnerabilities (sa-20170927-cip)

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

Risk Level: High

CVE: CVE-2017-12233, CVE-2017-12234

Description

Multiple vulnerabilities are present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

Multiple vulnerabilities are present in some versions of Cisco IOS. The flaws occur due to an improper handling of CIP requests. Successful exploitation by a remote attacker could result in a denial of service condition.

22609 - Wireshark Vulnerability Prior To 2.0.16

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

Risk Level: High

CVE: CVE-2017-15191

Description

A vulnerability is present in some versions of Wireshark.

Observation

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

A vulnerability is present in some versions of Wireshark. The flaw lies in the DMP dissector. Successful exploitation could allow an attacker to cause a denial of service condition.

22612 - LAVA Ether-Serial Link Authentication Bypass Vulnerability

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

Risk Level: High

CVE: CVE-2017-14003

Description

A vulnerability is present in some versions of LAVA Ether-Serial Link.

Observation

LAVA Ether-Serial Link is a networking device working over serial ports.

A vulnerability is present in some versions of LAVA Ether-Serial Link. The flaw lies in the authentication component. Successful exploitation could allow a remote attacker to bypass security restrictions and access sensitive information.

22613 - (JSA10818) Juniper Junos PAM Remote Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-10615

Description

A vulnerability is present in some versions of Juniper JunOS.

Observation

Juniper JunOS is an operating system used in Juniper switches and routers.

A vulnerability is present in some versions of Juniper JunOS. The flaw lies in the Pluggable Authentication Module (PAM). Successful exploitation could allow an attacker to crash certain daemons or remotely execute arbitrary code on the target system.

22617 - (JSA10825) Juniper SRX Series ISC BIND Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-3137

Description

A vulnerability is present in some versions of Juniper JunOS.

Observation

Juniper JunOS is an operating system used in Juniper switches and routers.

A vulnerability is present in some versions of Juniper JunOS. The flaws lie in the BIND DNS server feature. Successful exploitation could allow an attacker to cause denial of service.

22618 - (JSA10822) Juniper SRX Series Antivirus Updates Downloaded Without Verification Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-10620

Description

A vulnerability is present in some versions of Juniper JunOS.

Observation

Juniper JunOS is a operating system used in Juniper switches and routers.

A vulnerability is present in some versions of Juniper JunOS. The flaw is due to failure to verify the HTTPS server certificate before downloading anti-virus updates. Successful exploitation could allow an attacker to inject bogus signatures to cause service disruptions.

22628 - (JSA10813) Juniper SRX Series Flowd Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-10610

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper switches and routers.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in the flowd (flow daemon) process. Successful exploitation could allow an attacker to cause denial-of-service.

22629 - (JSA10811) Juniper SRX Series Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-10608

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw occurs when IPv6 traffic is processed by SUN/MS-RPC Application Layer Gateways. Successful exploitation could allow an attacker to cause a denial of service condition.

22631 - Oracle Secure Global Desktop (SGD) Critical Patch Update October 2017

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-3167

Description

A vulnerability is present in some versions of Oracle Secure Global Desktop.

Observation

Oracle Secure Global Desktop is a secure remote access solution.

A vulnerability is present in some versions of Oracle Secure Global Desktop. The flaw lies in the web server component. Successful exploitation could allow an attacker to disclose private information or cause a denial of service condition.

130910 - Debian Linux 9.0 DSA-4001-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14339

Description

The scan detected that the host is missing the following update:
DSA-4001-1

Observation

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

http://www.debian.org/security/2017/dsa-4001

Debian 9.0
all
yadifa_2.2.3-1+deb9u1

132405 - Oracle VM OVMSA-2017-0157 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14316, CVE-2017-14317, CVE-2017-14319

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0157

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/000787.html

OVM3.4
x86_64
xen-tools-4.4.4-155.0.1.el6
xen-4.4.4-155.0.1.el6

132406 - Oracle VM OVMSA-2017-0158 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0158

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/000788.html

OVM3.3
x86_64
xen-4.3.0-55.el6.186.48
xen-tools-4.3.0-55.el6.186.48

132407 - Oracle VM OVMSA-2017-0159 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0159

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/000789.html

OVM3.2
x86_64
xen-tools-4.1.3-25.el5.223.86
xen-devel-4.1.3-25.el5.223.86
xen-4.1.3-25.el5.223.86

141751 - Red Hat Enterprise Linux RHSA-2017-3046 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10293, CVE-2017-10295, 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

The scan detected that the host is missing the following update:
RHSA-2017-3046

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/msg00035.html

RHEL7D
x86_64
java-1.7.0-oracle-javafx-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-src-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-plugin-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-devel-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-jdbc-1.7.0.161-1jpp.4.el7

RHEL7S
x86_64
java-1.7.0-oracle-javafx-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-src-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-plugin-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-devel-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-jdbc-1.7.0.161-1jpp.4.el7

RHEL7WS
x86_64
java-1.7.0-oracle-javafx-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-src-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-plugin-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-devel-1.7.0.161-1jpp.4.el7
java-1.7.0-oracle-jdbc-1.7.0.161-1jpp.4.el7

141756 - Red Hat Enterprise Linux RHSA-2017-3047 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10293, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
RHSA-2017-3047

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/msg00036.html

RHEL7D
x86_64
java-1.6.0-sun-jdbc-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-src-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-devel-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-demo-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-plugin-1.6.0.171-1jpp.4.el7

RHEL7S
x86_64
java-1.6.0-sun-jdbc-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-src-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-devel-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-demo-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-plugin-1.6.0.171-1jpp.4.el7

RHEL7WS
x86_64
java-1.6.0-sun-jdbc-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-src-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-devel-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-demo-1.6.0.171-1jpp.4.el7
java-1.6.0-sun-plugin-1.6.0.171-1jpp.4.el7

141758 - Red Hat Enterprise Linux RHSA-2017-2999 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, 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

The scan detected that the host is missing the following update:
RHSA-2017-2999

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/msg00031.html

RHEL7D
x86_64
java-1.8.0-oracle-jdbc-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-src-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-javafx-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-devel-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-plugin-1.8.0.151-1jpp.5.el7

java-1.8.0-oracle-1.8.0.151-1jpp.5.el7

RHEL7S
x86_64
java-1.8.0-oracle-jdbc-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-src-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-javafx-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-devel-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-plugin-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-1.8.0.151-1jpp.5.el7

RHEL7WS
x86_64
java-1.8.0-oracle-jdbc-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-src-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-javafx-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-devel-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-plugin-1.8.0.151-1jpp.5.el7
java-1.8.0-oracle-1.8.0.151-1jpp.5.el7

141760 - Red Hat Enterprise Linux RHSA-2017-2997 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

Description

The scan detected that the host is missing the following update:
RHSA-2017-2997

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/msg00029.html

RHEL6D
x86_64
chromium-browser-62.0.3202.62-2.el6_9
chromium-browser-debuginfo-62.0.3202.62-2.el6_9

i386
chromium-browser-62.0.3202.62-2.el6_9
chromium-browser-debuginfo-62.0.3202.62-2.el6_9

RHEL6S
x86_64
chromium-browser-62.0.3202.62-2.el6_9
chromium-browser-debuginfo-62.0.3202.62-2.el6_9

i386
chromium-browser-62.0.3202.62-2.el6_9
chromium-browser-debuginfo-62.0.3202.62-2.el6_9

RHEL6WS
x86_64

chromium-browser-62.0.3202.62-2.el6_9
chromium-browser-debuginfo-62.0.3202.62-2.el6_9

i386
chromium-browser-62.0.3202.62-2.el6_9
chromium-browser-debuginfo-62.0.3202.62-2.el6_9

146005 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2823-1 Update Is Not Installed

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

Risk Level: High

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:
openSUSE-SU-2017:2823-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00074.html

SuSE Linux 42.2
x86_64
xorg-x11-server-7.6_1.18.3-12.26.1
xorg-x11-server-debuginfo-7.6_1.18.3-12.26.1
xorg-x11-server-debugsource-7.6_1.18.3-12.26.1
xorg-x11-server-extra-7.6_1.18.3-12.26.1
xorg-x11-server-extra-debuginfo-7.6_1.18.3-12.26.1
xorg-x11-server-source-7.6_1.18.3-12.26.1
xorg-x11-server-sdk-7.6_1.18.3-12.26.1

i586
xorg-x11-server-7.6_1.18.3-12.26.1
xorg-x11-server-debuginfo-7.6_1.18.3-12.26.1
xorg-x11-server-debugsource-7.6_1.18.3-12.26.1
xorg-x11-server-extra-7.6_1.18.3-12.26.1
xorg-x11-server-extra-debuginfo-7.6_1.18.3-12.26.1
xorg-x11-server-source-7.6_1.18.3-12.26.1
xorg-x11-server-sdk-7.6_1.18.3-12.26.1

SuSE Linux 42.3
x86_64
xorg-x11-server-debugsource-7.6_1.18.3-28.1
xorg-x11-server-debuginfo-7.6_1.18.3-28.1
xorg-x11-server-7.6_1.18.3-28.1
xorg-x11-server-source-7.6_1.18.3-28.1
xorg-x11-server-extra-debuginfo-7.6_1.18.3-28.1
xorg-x11-server-sdk-7.6_1.18.3-28.1
xorg-x11-server-extra-7.6_1.18.3-28.1

i586
xorg-x11-server-debugsource-7.6_1.18.3-28.1
xorg-x11-server-debuginfo-7.6_1.18.3-28.1
xorg-x11-server-7.6_1.18.3-28.1
xorg-x11-server-source-7.6_1.18.3-28.1

xorg-x11-server-extra-debuginfo-7.6_1.18.3-28.1
xorg-x11-server-sdk-7.6_1.18.3-28.1
xorg-x11-server-extra-7.6_1.18.3-28.1

146007 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2825-1 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-2017:2825-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00076.html

SuSE Linux 42.2
noarch
xerces-j2-2.8.1-6.3.1
xerces-j2-xml-resolver-2.8.1-6.3.1
xerces-j2-scripts-2.8.1-6.3.1
xerces-j2-xml-apis-2.8.1-6.3.1
xerces-j2-demo-2.8.1-6.3.1

SuSE Linux 42.3
noarch
xerces-j2-demo-2.8.1-9.1
xerces-j2-xml-resolver-2.8.1-9.1
xerces-j2-2.8.1-9.1
xerces-j2-scripts-2.8.1-9.1
xerces-j2-xml-apis-2.8.1-9.1

146008 - SuSE Linux 42.2 openSUSE-SU-2017:2822-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12791, CVE-2017-14695, CVE-2017-14696

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2822-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00073.html

SuSE Linux 42.2
x86_64
salt-ssh-2017.7.2-5.3.1
salt-master-2017.7.2-5.3.1

salt-2017.7.2-5.3.1
salt-syndic-2017.7.2-5.3.1
salt-proxy-2017.7.2-5.3.1
salt-minion-2017.7.2-5.3.1
salt-api-2017.7.2-5.3.1
salt-doc-2017.7.2-5.3.1
salt-cloud-2017.7.2-5.3.1

noarch
salt-fish-completion-2017.7.2-5.3.1
salt-zsh-completion-2017.7.2-5.3.1
salt-bash-completion-2017.7.2-5.3.1

146009 - SuSE Linux 42.3 openSUSE-SU-2017:2824-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14695, CVE-2017-14696

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2824-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00075.html

SuSE Linux 42.3
x86_64
salt-proxy-2017.7.2-14.1
salt-ssh-2017.7.2-14.1
salt-2017.7.2-14.1
salt-master-2017.7.2-14.1
salt-doc-2017.7.2-14.1
salt-api-2017.7.2-14.1
salt-minion-2017.7.2-14.1
salt-syndic-2017.7.2-14.1
salt-cloud-2017.7.2-14.1

noarch
salt-bash-completion-2017.7.2-14.1
salt-fish-completion-2017.7.2-14.1
salt-zsh-completion-2017.7.2-14.1

146011 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2755-1 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:
openSUSE-SU-2017:2755-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00055.html

SuSE Linux 42.2
x86_64
wpa_supplicant-2.2-9.3.1
wpa_supplicant-gui-debuginfo-2.2-9.3.1
wpa_supplicant-debuginfo-2.2-9.3.1
wpa_supplicant-debugsource-2.2-9.3.1
wpa_supplicant-gui-2.2-9.3.1

i586
wpa_supplicant-2.2-9.3.1
wpa_supplicant-gui-debuginfo-2.2-9.3.1
wpa_supplicant-debuginfo-2.2-9.3.1
wpa_supplicant-debugsource-2.2-9.3.1
wpa_supplicant-gui-2.2-9.3.1

SuSE Linux 42.3
x86_64
wpa_supplicant-2.2-13.1
wpa_supplicant-debuginfo-2.2-13.1
wpa_supplicant-debugsource-2.2-13.1
wpa_supplicant-gui-2.2-13.1
wpa_supplicant-gui-debuginfo-2.2-13.1

i586
wpa_supplicant-2.2-13.1
wpa_supplicant-debuginfo-2.2-13.1
wpa_supplicant-debugsource-2.2-13.1
wpa_supplicant-gui-2.2-13.1
wpa_supplicant-gui-debuginfo-2.2-13.1

146012 - SuSE Linux 42.2 openSUSE-SU-2017:2833-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4074

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2833-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00083.html

SuSE Linux 42.2
x86_64
libjq-devel-1.5-8.3.1
jq-debugsource-1.5-8.3.1
libjq1-1.5-8.3.1
jq-1.5-8.3.1

libjq1-debuginfo-1.5-8.3.1
jq-debuginfo-1.5-8.3.1

i586
libjq-devel-1.5-8.3.1
jq-debugsource-1.5-8.3.1
libjq1-1.5-8.3.1
jq-1.5-8.3.1
libjq1-debuginfo-1.5-8.3.1
jq-debuginfo-1.5-8.3.1

146014 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2766-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15056

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2766-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00065.html

SuSE Linux 42.2
x86_64
upx-3.94-6.3.1
upx-debugsource-3.94-6.3.1
upx-debuginfo-3.94-6.3.1

SuSE Linux 42.3
x86_64
upx-3.94-9.1
upx-debuginfo-3.94-9.1
upx-debugsource-3.94-9.1

146017 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2831-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000254, CVE-2017-1000257

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2831-1

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/003350.html

SuSE SLES 12 SP2

x86_64
libcurl4-7.37.0-37.8.1
curl-debugsource-7.37.0-37.8.1
curl-7.37.0-37.8.1
libcurl4-debuginfo-32bit-7.37.0-37.8.1
libcurl4-32bit-7.37.0-37.8.1
libcurl4-debuginfo-7.37.0-37.8.1
curl-debuginfo-7.37.0-37.8.1

SuSE SLED 12 SP3
x86_64
libcurl4-7.37.0-37.8.1
curl-debugsource-7.37.0-37.8.1
curl-7.37.0-37.8.1
libcurl4-debuginfo-7.37.0-37.8.1
libcurl4-32bit-7.37.0-37.8.1
libcurl4-debuginfo-32bit-7.37.0-37.8.1
curl-debuginfo-7.37.0-37.8.1

SuSE SLED 12 SP2
x86_64
libcurl4-7.37.0-37.8.1
curl-debugsource-7.37.0-37.8.1
curl-7.37.0-37.8.1
libcurl4-debuginfo-7.37.0-37.8.1
libcurl4-32bit-7.37.0-37.8.1
libcurl4-debuginfo-32bit-7.37.0-37.8.1
curl-debuginfo-7.37.0-37.8.1

SuSE SLES 12 SP3
x86_64
libcurl4-7.37.0-37.8.1
curl-debugsource-7.37.0-37.8.1
curl-7.37.0-37.8.1
libcurl4-debuginfo-32bit-7.37.0-37.8.1
libcurl4-32bit-7.37.0-37.8.1
libcurl4-debuginfo-7.37.0-37.8.1
curl-debuginfo-7.37.0-37.8.1

160315 - CentOS 6 CESA-2017-2911 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-2017-2911

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/022570.html

CentOS 6
x86_64
wpa_supplicant-0.7.3-9.el6_9.2

i686
wpa_supplicant-0.7.3-9.el6_9.2

160317 - CentOS 7 CESA-2017-2930 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-2017-2930

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/022605.html

CentOS 7
x86_64
kernel-tools-libs-devel-3.10.0-693.5.2.el7
kernel-headers-3.10.0-693.5.2.el7
kernel-debug-devel-3.10.0-693.5.2.el7
kernel-3.10.0-693.5.2.el7
python-perf-3.10.0-693.5.2.el7
kernel-debug-3.10.0-693.5.2.el7
perf-3.10.0-693.5.2.el7
kernel-devel-3.10.0-693.5.2.el7
kernel-tools-3.10.0-693.5.2.el7
kernel-tools-libs-3.10.0-693.5.2.el7

noarch
kernel-abi-whitelists-3.10.0-693.5.2.el7
kernel-doc-3.10.0-693.5.2.el7

182494 - FreeBSD krb5 Multiple Vulnerabilities (3f3837cc-48fb-4414-aa46-5b1c23c9feae)

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

Risk Level: High

CVE: CVE-2017-11368, CVE-2017-11462

Description

The scan detected that the host is missing the following update:
krb5 -- Multiple vulnerabilities (3f3837cc-48fb-4414-aa46-5b1c23c9feae)

Observation

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

http://www.vuxml.org/freebsd/3f3837cc-48fb-4414-aa46-5b1c23c9feae.html

Affected packages:
krb5 < 1.14.6
1.15 <= krb5 < 1.15.2

krb5-devel < 1.14.6
1.15 <= krb5-devel < 1.15.2
krb5-115 < 1.15.2
krb5-114 < 1.14.6
krb5-113 < 1.14.6

182496 - FreeBSD arj Multiple Vulnerabilities (b95e5674-b4d6-11e7-b895-0cc47a494882)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
arj -- multiple vulnerabilities (b95e5674-b4d6-11e7-b895-0cc47a494882)

Observation

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

http://www.vuxml.org/freebsd/b95e5674-b4d6-11e7-b895-0cc47a494882.html

Affected packages:
arj < 3.10.22_5

185929 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3461-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6257, CVE-2017-6259, CVE-2017-6266, CVE-2017-6267, CVE-2017-6272

Description

The scan detected that the host is missing the following update:
USN-3461-1

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/004103.html

Ubuntu 16.04

nvidia-384_384.90-0ubuntu0.16.04.1

Ubuntu 14.04

nvidia-384_384.90-0ubuntu0.14.04.1

Ubuntu 17.04

nvidia-384_384.90-0ubuntu0.17.04.1

192804 - Fedora Linux 25 FEDORA-2017-515264ae24 Update Is Not Installed

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

Risk Level: High

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-2017-515264ae24

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

dnsmasq-2.76-4.fc25

192808 - Fedora Linux 27 FEDORA-2017-0d3fdd3d1f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15670, CVE-2017-15671

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0d3fdd3d1f

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

glibc-2.26-15.fc27

192809 - Fedora Linux 27 FEDORA-2017-7106a157f5 Update Is Not Installed

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

Risk Level: High

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-2017-7106a157f5

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

dnsmasq-2.77-9.fc27

130911 - Debian Linux 9.0 DSA-4005-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10086, CVE-2017-10114

Description

The scan detected that the host is missing the following update:
DSA-4005-1

Observation

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

http://www.debian.org/security/2017/dsa-4005

Debian 9.0
all
openjfx_8u141-b14-3~deb9u1

130914 - Debian Linux 9.0 DSA-4006-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14685, CVE-2017-14686, CVE-2017-14687, CVE-2017-15587

Description

The scan detected that the host is missing the following update:
DSA-4006-1

Observation

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

http://www.debian.org/security/2017/dsa-4006

Debian 9.0
all
mupdf_1.9a+ds1-4+deb9u1

146001 - SuSE SLES 11 SP4 SUSE-SU-2017:2838-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6329, CVE-2017-12166, CVE-2017-7478, CVE-2017-7479

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2838-1

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/003351.html

SuSE SLES 11 SP4
i586
openvpn-2.0.9-143.47.3.1
openvpn-auth-pam-plugin-2.0.9-143.47.3.1

x86_64
openvpn-2.0.9-143.47.3.1
openvpn-auth-pam-plugin-2.0.9-143.47.3.1

146003 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2839-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12166

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2839-1

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/003352.html

SuSE SLES 12 SP2
x86_64
openvpn-debugsource-2.3.8-16.20.1
openvpn-2.3.8-16.20.1
openvpn-auth-pam-plugin-debuginfo-2.3.8-16.20.1
openvpn-debuginfo-2.3.8-16.20.1
openvpn-auth-pam-plugin-2.3.8-16.20.1

SuSE SLED 12 SP3
x86_64
openvpn-debugsource-2.3.8-16.20.1
openvpn-debuginfo-2.3.8-16.20.1
openvpn-2.3.8-16.20.1

SuSE SLED 12 SP2
x86_64
openvpn-debugsource-2.3.8-16.20.1
openvpn-debuginfo-2.3.8-16.20.1
openvpn-2.3.8-16.20.1

SuSE SLES 12 SP3
x86_64
openvpn-debugsource-2.3.8-16.20.1
openvpn-2.3.8-16.20.1
openvpn-auth-pam-plugin-debuginfo-2.3.8-16.20.1
openvpn-debuginfo-2.3.8-16.20.1
openvpn-auth-pam-plugin-2.3.8-16.20.1

192806 - Fedora Linux 27 FEDORA-2017-aa9927961f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000255, CVE-2017-12190, CVE-2017-15265, CVE-2017-15299, CVE-2017-5123

Description

The scan detected that the host is missing the following update:
FEDORA-2017-aa9927961f

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

kernel-4.13.8-300.fc27

22606 - (JSA10820) Juniper Junos RPD Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10618

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper switches and routers.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw is due to bgp-error-tolerance feature, when enabled could be exploited with BGP UPDATE message containing a specifically crafted set attributes. Successful exploitation could allow an attacker to crash and restart RPD routing process and cause a denial of service condition.

22621 - (JSA10810) Juniper Junos Rpd Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10607

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is a operating system used in Juniper switches and routers.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw is due to receipt of specially crafted BGP packet. Successful exploitation could allow an attacker to crash and restart RPD routing process and cause a denial of service condition.

22625 - (JSA10827) Juniper ScreenOS Wi-Fi Protected Access Protocols Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of Juniper ScreenOS.

Observation

Juniper ScreenOS is an operating system used in Juniper firewall and VPN.

Multiple vulnerabilities are present in some versions of Juniper ScreenOS. This is a series of protocol level vulnerabilities. Successful exploitation could allow an attacker to decrypt wireless packets, replay, forge or inject packets into a wireless network.

141749 - Red Hat Enterprise Linux RHSA-2017-2912 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1000232, CVE-2017-15010

Description

The scan detected that the host is missing the following update:
RHSA-2017-2912

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/msg00022.html

RHEL6_7S
noarch
rh-nodejs4-nodejs-tough-cookie-2.3.3-2.el6

RHEL6S
noarch
rh-nodejs4-nodejs-tough-cookie-2.3.3-2.el6

RHEL6WS
noarch
rh-nodejs4-nodejs-tough-cookie-2.3.3-2.el6

RHEL7S
noarch
rh-nodejs4-nodejs-tough-cookie-2.3.3-2.el7

RHEL7WS
noarch
rh-nodejs4-nodejs-tough-cookie-2.3.3-2.el7

141750 - Red Hat Enterprise Linux RHSA-2017-2972 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12171, CVE-2017-9798

Description

The scan detected that the host is missing the following update:
RHSA-2017-2972

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/msg00028.html

RHEL6D
i386
httpd-debuginfo-2.2.15-60.el6_9.6
mod_ssl-2.2.15-60.el6_9.6
httpd-devel-2.2.15-60.el6_9.6
httpd-2.2.15-60.el6_9.6
httpd-tools-2.2.15-60.el6_9.6

noarch
httpd-manual-2.2.15-60.el6_9.6

x86_64
httpd-debuginfo-2.2.15-60.el6_9.6
mod_ssl-2.2.15-60.el6_9.6
httpd-devel-2.2.15-60.el6_9.6
httpd-2.2.15-60.el6_9.6
httpd-tools-2.2.15-60.el6_9.6

RHEL6S
i386
httpd-debuginfo-2.2.15-60.el6_9.6
mod_ssl-2.2.15-60.el6_9.6
httpd-devel-2.2.15-60.el6_9.6
httpd-2.2.15-60.el6_9.6
httpd-tools-2.2.15-60.el6_9.6

noarch
httpd-manual-2.2.15-60.el6_9.6

x86_64
httpd-debuginfo-2.2.15-60.el6_9.6
mod_ssl-2.2.15-60.el6_9.6
httpd-devel-2.2.15-60.el6_9.6
httpd-2.2.15-60.el6_9.6
httpd-tools-2.2.15-60.el6_9.6

RHEL6WS
i386
httpd-debuginfo-2.2.15-60.el6_9.6
mod_ssl-2.2.15-60.el6_9.6
httpd-devel-2.2.15-60.el6_9.6
httpd-2.2.15-60.el6_9.6
httpd-tools-2.2.15-60.el6_9.6

noarch
httpd-manual-2.2.15-60.el6_9.6

x86_64
httpd-debuginfo-2.2.15-60.el6_9.6
mod_ssl-2.2.15-60.el6_9.6
httpd-devel-2.2.15-60.el6_9.6
httpd-2.2.15-60.el6_9.6
httpd-tools-2.2.15-60.el6_9.6

141752 - Red Hat Enterprise Linux RHSA-2017-3018 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-2017-3018

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/msg00034.html

RHEL6_7S
x86_64
httpd24-mod_ldap-2.4.27-8.el6
httpd24-httpd-debuginfo-2.4.27-8.el6
httpd24-scldevel-1.1-18.el6
httpd24-runtime-1.1-18.el6
httpd24-httpd-devel-2.4.27-8.el6
httpd24-mod_session-2.4.27-8.el6
httpd24-1.1-18.el6
httpd24-mod_ssl-2.4.27-8.el6
httpd24-httpd-tools-2.4.27-8.el6
httpd24-httpd-2.4.27-8.el6
httpd24-mod_proxy_html-2.4.27-8.el6

noarch
httpd24-httpd-manual-2.4.27-8.el6

RHEL6S
x86_64
httpd24-mod_ldap-2.4.27-8.el6
httpd24-httpd-debuginfo-2.4.27-8.el6
httpd24-scldevel-1.1-18.el6
httpd24-runtime-1.1-18.el6
httpd24-httpd-devel-2.4.27-8.el6
httpd24-mod_session-2.4.27-8.el6
httpd24-1.1-18.el6
httpd24-mod_ssl-2.4.27-8.el6
httpd24-httpd-tools-2.4.27-8.el6
httpd24-httpd-2.4.27-8.el6
httpd24-mod_proxy_html-2.4.27-8.el6

noarch
httpd24-httpd-manual-2.4.27-8.el6

RHEL6WS

x86_64
httpd24-mod_ldap-2.4.27-8.el6
httpd24-httpd-debuginfo-2.4.27-8.el6
httpd24-scldevel-1.1-18.el6
httpd24-runtime-1.1-18.el6
httpd24-httpd-devel-2.4.27-8.el6
httpd24-mod_session-2.4.27-8.el6
httpd24-1.1-18.el6
httpd24-mod_ssl-2.4.27-8.el6
httpd24-httpd-tools-2.4.27-8.el6
httpd24-httpd-2.4.27-8.el6
httpd24-mod_proxy_html-2.4.27-8.el6

noarch
httpd24-httpd-manual-2.4.27-8.el6

RHEL7S
noarch
httpd24-httpd-manual-2.4.27-8.el7

x86_64
httpd24-runtime-1.1-18.el7
httpd24-curl-debuginfo-7.47.1-4.el7
httpd24-scldevel-1.1-18.el7
httpd24-mod_session-2.4.27-8.el7
httpd24-libcurl-7.47.1-4.el7
httpd24-mod_auth_kerb-5.4-33.el7
httpd24-mod_ssl-2.4.27-8.el7
httpd24-httpd-2.4.27-8.el7
httpd24-httpd-devel-2.4.27-8.el7
httpd24-nghttp2-debuginfo-1.7.1-6.el7
httpd24-libcurl-devel-7.47.1-4.el7
httpd24-httpd-debuginfo-2.4.27-8.el7
httpd24-libnghttp2-devel-1.7.1-6.el7
httpd24-nghttp2-1.7.1-6.el7
httpd24-mod_ldap-2.4.27-8.el7
httpd24-1.1-18.el7
httpd24-mod_auth_kerb-debuginfo-5.4-33.el7
httpd24-mod_proxy_html-2.4.27-8.el7
httpd24-httpd-tools-2.4.27-8.el7
httpd24-libnghttp2-1.7.1-6.el7
httpd24-curl-7.47.1-4.el7

RHEL7WS
x86_64
httpd24-runtime-1.1-18.el7
httpd24-curl-debuginfo-7.47.1-4.el7
httpd24-scldevel-1.1-18.el7
httpd24-mod_session-2.4.27-8.el7
httpd24-libcurl-7.47.1-4.el7
httpd24-mod_auth_kerb-5.4-33.el7
httpd24-mod_ssl-2.4.27-8.el7
httpd24-httpd-2.4.27-8.el7
httpd24-httpd-devel-2.4.27-8.el7
httpd24-nghttp2-debuginfo-1.7.1-6.el7
httpd24-libcurl-devel-7.47.1-4.el7
httpd24-httpd-debuginfo-2.4.27-8.el7
httpd24-libnghttp2-devel-1.7.1-6.el7
httpd24-nghttp2-1.7.1-6.el7
httpd24-mod_ldap-2.4.27-8.el7

httpd24-1.1-18.el7
httpd24-mod_auth_kerb-debuginfo-5.4-33.el7
httpd24-mod_proxy_html-2.4.27-8.el7
httpd24-httpd-tools-2.4.27-8.el7
httpd24-libnghttp2-1.7.1-6.el7
httpd24-curl-7.47.1-4.el7

noarch
httpd24-httpd-manual-2.4.27-8.el7

141753 - Red Hat Enterprise Linux RHSA-2017-2913 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15010

Description

The scan detected that the host is missing the following update:
RHSA-2017-2913

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/msg00023.html

RHEL6_7S
noarch
rh-nodejs6-nodejs-tough-cookie-2.3.3-1.el6

RHEL6S
noarch
rh-nodejs6-nodejs-tough-cookie-2.3.3-1.el6

RHEL6WS
noarch
rh-nodejs6-nodejs-tough-cookie-2.3.3-1.el6

RHEL7S
noarch
rh-nodejs6-nodejs-tough-cookie-2.3.3-1.el7

RHEL7WS
noarch
rh-nodejs6-nodejs-tough-cookie-2.3.3-1.el7

141754 - Red Hat Enterprise Linux RHSA-2017-2908 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11499

Description

The scan detected that the host is missing the following update:
RHSA-2017-2908

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/msg00020.html

RHEL6_7S
x86_64
rh-nodejs6-nodejs-debuginfo-6.11.3-2.el6
rh-nodejs6-nodejs-6.11.3-2.el6
rh-nodejs6-nodejs-devel-6.11.3-2.el6

noarch
rh-nodejs6-nodejs-docs-6.11.3-2.el6

RHEL6S
x86_64
rh-nodejs6-nodejs-debuginfo-6.11.3-2.el6
rh-nodejs6-nodejs-6.11.3-2.el6
rh-nodejs6-nodejs-devel-6.11.3-2.el6

noarch
rh-nodejs6-nodejs-docs-6.11.3-2.el6

RHEL6WS
x86_64
rh-nodejs6-nodejs-debuginfo-6.11.3-2.el6
rh-nodejs6-nodejs-6.11.3-2.el6
rh-nodejs6-nodejs-devel-6.11.3-2.el6

noarch
rh-nodejs6-nodejs-docs-6.11.3-2.el6

RHEL7S
x86_64
rh-nodejs6-nodejs-debuginfo-6.11.3-2.el7
rh-nodejs6-nodejs-6.11.3-2.el7
rh-nodejs6-nodejs-devel-6.11.3-2.el7

noarch
rh-nodejs6-nodejs-docs-6.11.3-2.el7

RHEL7WS
x86_64
rh-nodejs6-nodejs-debuginfo-6.11.3-2.el7
rh-nodejs6-nodejs-6.11.3-2.el7
rh-nodejs6-nodejs-devel-6.11.3-2.el7

noarch
rh-nodejs6-nodejs-docs-6.11.3-2.el7

141755 - Red Hat Enterprise Linux RHSA-2017-2998 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, 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

The scan detected that the host is missing the following update:
RHSA-2017-2998

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/msg00030.html

RHEL7S
noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.151-1.b12.el7_4

x86_64
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el7_4

RHEL6S
i386
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el6_9

x86_64
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9

java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9

RHEL6WS
x86_64
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9

i386
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9

RHEL7D
x86_64
java-1.8.0-openjdk-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el7_4

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.151-1.b12.el7_4

RHEL6D
i386
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el6_9

x86_64
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9

java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9

RHEL7WS
x86_64
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el7_4

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.151-1.b12.el7_4

141757 - Red Hat Enterprise Linux RHSA-2017-3002 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11499

Description

The scan detected that the host is missing the following update:
RHSA-2017-3002

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/msg00032.html

RHEL6_7S
x86_64
rh-nodejs4-runtime-2.4-4.el6
rh-nodejs4-nodejs-4.6.2-7.el6
rh-nodejs4-nodejs-devel-4.6.2-7.el6
rh-nodejs4-2.4-4.el6
rh-nodejs4-scldevel-2.4-4.el6
rh-nodejs4-nodejs-debuginfo-4.6.2-7.el6

noarch

rh-nodejs4-node-gyp-3.3.1-5.el6
rh-nodejs4-nodejs-docs-4.6.2-7.el6

RHEL6S
x86_64
rh-nodejs4-runtime-2.4-4.el6
rh-nodejs4-nodejs-4.6.2-7.el6
rh-nodejs4-nodejs-devel-4.6.2-7.el6
rh-nodejs4-2.4-4.el6
rh-nodejs4-scldevel-2.4-4.el6
rh-nodejs4-nodejs-debuginfo-4.6.2-7.el6

noarch
rh-nodejs4-node-gyp-3.3.1-5.el6
rh-nodejs4-nodejs-docs-4.6.2-7.el6

RHEL6WS
x86_64
rh-nodejs4-runtime-2.4-4.el6
rh-nodejs4-nodejs-4.6.2-7.el6
rh-nodejs4-nodejs-devel-4.6.2-7.el6
rh-nodejs4-2.4-4.el6
rh-nodejs4-scldevel-2.4-4.el6
rh-nodejs4-nodejs-debuginfo-4.6.2-7.el6

noarch
rh-nodejs4-node-gyp-3.3.1-5.el6
rh-nodejs4-nodejs-docs-4.6.2-7.el6

RHEL7S
x86_64
rh-nodejs4-2.4-3.el7
rh-nodejs4-nodejs-devel-4.6.2-6.el7
rh-nodejs4-scldevel-2.4-3.el7
rh-nodejs4-runtime-2.4-3.el7
rh-nodejs4-nodejs-4.6.2-6.el7
rh-nodejs4-nodejs-debuginfo-4.6.2-6.el7

noarch
rh-nodejs4-nodejs-docs-4.6.2-6.el7

RHEL7WS
x86_64
rh-nodejs4-2.4-3.el7
rh-nodejs4-nodejs-devel-4.6.2-6.el7
rh-nodejs4-scldevel-2.4-3.el7
rh-nodejs4-runtime-2.4-3.el7
rh-nodejs4-nodejs-4.6.2-6.el7
rh-nodejs4-nodejs-debuginfo-4.6.2-6.el7

noarch
rh-nodejs4-nodejs-docs-4.6.2-6.el7

141761 - Red Hat Enterprise Linux RHSA-2017-2911 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-2017-13087

Description

The scan detected that the host is missing the following update:
RHSA-2017-2911

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/msg00021.html

RHEL6D
x86_64
wpa_supplicant-0.7.3-9.el6_9.2
wpa_supplicant-debuginfo-0.7.3-9.el6_9.2

i386
wpa_supplicant-0.7.3-9.el6_9.2
wpa_supplicant-debuginfo-0.7.3-9.el6_9.2

RHEL6S
i386
wpa_supplicant-0.7.3-9.el6_9.2
wpa_supplicant-debuginfo-0.7.3-9.el6_9.2

x86_64
wpa_supplicant-0.7.3-9.el6_9.2
wpa_supplicant-debuginfo-0.7.3-9.el6_9.2

RHEL6WS
x86_64
wpa_supplicant-0.7.3-9.el6_9.2
wpa_supplicant-debuginfo-0.7.3-9.el6_9.2

i386
wpa_supplicant-0.7.3-9.el6_9.2
wpa_supplicant-debuginfo-0.7.3-9.el6_9.2

146006 - SuSE Linux 42.3 openSUSE-SU-2017:2820-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11424, CVE-2017-12880

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2820-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00071.html

SuSE Linux 42.3
noarch
python3-PyJWT-1.4.2-3.1

146013 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2832-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15227, CVE-2017-15228, CVE-2017-15721, CVE-2017-15722, CVE-2017-15723

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2832-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00082.html

SuSE Linux 42.2
x86_64
irssi-devel-1.0.5-14.14.1
irssi-debuginfo-1.0.5-14.14.1
irssi-1.0.5-14.14.1
irssi-debugsource-1.0.5-14.14.1

i586
irssi-devel-1.0.5-14.14.1
irssi-debuginfo-1.0.5-14.14.1
irssi-1.0.5-14.14.1
irssi-debugsource-1.0.5-14.14.1

SuSE Linux 42.3
x86_64
irssi-debuginfo-1.0.5-17.1
irssi-debugsource-1.0.5-17.1
irssi-1.0.5-17.1
irssi-devel-1.0.5-17.1

i586
irssi-debuginfo-1.0.5-17.1
irssi-debugsource-1.0.5-17.1
irssi-1.0.5-17.1
irssi-devel-1.0.5-17.1

146016 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2818-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11591, CVE-2017-11683, CVE-2017-14859, CVE-2017-14862, CVE-2017-14865

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2818-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00070.html

SuSE Linux 42.2
i586
exiv2-debugsource-0.25-7.3.1
libexiv2-14-0.25-7.3.1
exiv2-0.25-7.3.1
libexiv2-14-debuginfo-0.25-7.3.1
exiv2-debuginfo-0.25-7.3.1
libexiv2-devel-0.25-7.3.1

noarch
exiv2-lang-0.25-7.3.1

x86_64
exiv2-debugsource-0.25-7.3.1
libexiv2-14-0.25-7.3.1
libexiv2-14-32bit-0.25-7.3.1
exiv2-0.25-7.3.1
libexiv2-14-debuginfo-0.25-7.3.1
libexiv2-14-debuginfo-32bit-0.25-7.3.1
exiv2-debuginfo-0.25-7.3.1
libexiv2-devel-0.25-7.3.1

SuSE Linux 42.3
i586
libexiv2-14-debuginfo-0.25-10.1
exiv2-0.25-10.1
libexiv2-14-0.25-10.1
exiv2-debuginfo-0.25-10.1
exiv2-debugsource-0.25-10.1
libexiv2-devel-0.25-10.1

noarch
exiv2-lang-0.25-10.1

x86_64
libexiv2-14-debuginfo-32bit-0.25-10.1
libexiv2-14-32bit-0.25-10.1
libexiv2-14-debuginfo-0.25-10.1
exiv2-0.25-10.1
libexiv2-14-0.25-10.1
exiv2-debuginfo-0.25-10.1
exiv2-debugsource-0.25-10.1
libexiv2-devel-0.25-10.1

160314 - CentOS 6 CESA-2017-2972 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-2017-2972

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/022601.html

CentOS 6
i686
httpd-2.2.15-60.el6.centos.6
mod_ssl-2.2.15-60.el6.centos.6
httpd-tools-2.2.15-60.el6.centos.6
httpd-devel-2.2.15-60.el6.centos.6

noarch
httpd-manual-2.2.15-60.el6.centos.6

x86_64
httpd-2.2.15-60.el6.centos.6
mod_ssl-2.2.15-60.el6.centos.6
httpd-tools-2.2.15-60.el6.centos.6
httpd-devel-2.2.15-60.el6.centos.6

163480 - Oracle Enterprise Linux ELSA-2017-2972 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12171, CVE-2017-9798

Description

The scan detected that the host is missing the following update:
ELSA-2017-2972

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/007268.html

OEL6
x86_64
httpd-devel-2.2.15-60.0.1.el6_9.6
httpd-tools-2.2.15-60.0.1.el6_9.6
httpd-manual-2.2.15-60.0.1.el6_9.6
httpd-2.2.15-60.0.1.el6_9.6
mod_ssl-2.2.15-60.0.1.el6_9.6

i386
httpd-devel-2.2.15-60.0.1.el6_9.6
httpd-tools-2.2.15-60.0.1.el6_9.6
httpd-manual-2.2.15-60.0.1.el6_9.6
httpd-2.2.15-60.0.1.el6_9.6
mod_ssl-2.2.15-60.0.1.el6_9.6

163481 - Oracle Enterprise Linux ELSA-2017-2911 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-2017-13087

Description

The scan detected that the host is missing the following update:
ELSA-2017-2911

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/007267.html

OEL6
x86_64
wpa_supplicant-0.7.3-9.el6_9.2

i386
wpa_supplicant-0.7.3-9.el6_9.2

163482 - Oracle Enterprise Linux ELSA-2017-2998 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, 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

The scan detected that the host is missing the following update:
ELSA-2017-2998

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/007295.html
http://oss.oracle.com/pipermail/el-errata/2017-October/007294.html

OEL7
x86_64
java-1.8.0-openjdk-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el7_4

OEL6

x86_64
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el6_9

i386
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el6_9

175276 - Scientific Linux Security ERRATA Moderate: httpd on SL6.x i386/x86_64 (1710-12001)

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

Risk Level: Medium

CVE: CVE-2017-12171, CVE-2017-9798

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: httpd on SL6.x i386/x86_64 (1710-12001)

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=12001

SL6
i386
httpd-debuginfo-2.2.15-60.el6_9.6
mod_ssl-2.2.15-60.el6_9.6
httpd-devel-2.2.15-60.el6_9.6
httpd-2.2.15-60.el6_9.6
httpd-tools-2.2.15-60.el6_9.6

noarch
httpd-manual-2.2.15-60.el6_9.6

x86_64
httpd-debuginfo-2.2.15-60.el6_9.6
mod_ssl-2.2.15-60.el6_9.6

httpd-devel-2.2.15-60.el6_9.6
httpd-2.2.15-60.el6_9.6
httpd-tools-2.2.15-60.el6_9.6

175277 - Scientific Linux Security ERRATA Critical: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1710-12826)

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

Risk Level: Medium

CVE: CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, 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

The scan detected that the host is missing the following update:
Security ERRATA Critical: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1710-12826)

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=12826

SL7
x86_64
java-1.8.0-openjdk-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el7_4

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.151-1.b12.el7_4

SL6
i386
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.el6_9

x86_64
java-1.8.0-openjdk-headless-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-debug-1.8.0.151-1.b12.el6_9
java-1.8.0-openjdk-src-1.8.0.151-1.b12.el6_9

175278 - Scientific Linux Security ERRATA Important: wpa_supplicant on SL7.x x86_64 (1710-11151)

Category: SSH Module -> NonIntrusive -> Scientific 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:
Security ERRATA Important: wpa_supplicant on SL7.x x86_64 (1710-11151)

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=11151

SL7
x86_64
wpa_supplicant-debuginfo-2.6-5.el7_4.1
wpa_supplicant-2.6-5.el7_4.1

175279 - Scientific Linux Security ERRATA Important: wpa_supplicant on SL6.x i386/x86_64 (1710-11600)

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

Risk Level: Medium

CVE: CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13087

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: wpa_supplicant on SL6.x i386/x86_64 (1710-11600)

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=11600

SL6

x86_64
wpa_supplicant-0.7.3-9.el6_9.2
wpa_supplicant-debuginfo-0.7.3-9.el6_9.2

i386
wpa_supplicant-0.7.3-9.el6_9.2
wpa_supplicant-debuginfo-0.7.3-9.el6_9.2

178533 - Gentoo Linux GLSA-201710-26 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-201710-26

Observation

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

https://security.gentoo.org/glsa/201710-26

Affected packages:
media-libs/openjpeg < 2.3.0

178534 - Gentoo Linux GLSA-201710-27 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-201710-27

Observation

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

https://security.gentoo.org/glsa/201710-27

Affected packages:
net-dns/dnsmasq < 2.78

178535 - Gentoo Linux GLSA-201710-21 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-201710-21

Observation

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

https://security.gentoo.org/glsa/201710-21

Affected packages:
media-tv/kodi < 17.3-r1

178536 - Gentoo Linux GLSA-201710-24 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-201710-24

Observation

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

https://security.gentoo.org/glsa/201710-24

Affected packages:
www-client/chromium < 62.0.3202.62
www-client/google-chrome < 62.0.3202.62

178537 - Gentoo Linux GLSA-201710-22 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-201710-22

Observation

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

https://security.gentoo.org/glsa/201710-22

Affected packages:
www-plugins/adobe-flash < 27.0.0.170

178538 - Gentoo Linux GLSA-201710-23 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-201710-23

Observation

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

https://security.gentoo.org/glsa/201710-23

Affected packages:
dev-lang/go < 1.9.1

178539 - Gentoo Linux GLSA-201710-25 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-201710-25

Observation

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

https://security.gentoo.org/glsa/201710-25

Affected packages:
dev-libs/libpcre < 8.41

182493 - FreeBSD MySQL Multiple Vulnerabilities (c41bedfd-b3f9-11e7-ac58-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10165, CVE-2017-10167, CVE-2017-10203, CVE-2017-10227, CVE-2017-10268, CVE-2017-10277, CVE-2017-10279, CVE-2017-10283, CVE-2017-10284, CVE-2017-10286, CVE-2017-10294, CVE-2017-10296, CVE-2017-10311, CVE-2017-10313, CVE-2017-10314, CVE-2017-10320, CVE-2017-10365, CVE-2017-10376, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

The scan detected that the host is missing the following update:
MySQL -- multiple vulnerabilities (c41bedfd-b3f9-11e7-ac58-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/c41bedfd-b3f9-11e7-ac58-b499baebfeaf.html

Affected packages:
mariadb55-server < 5.5.58

mariadb100-server < 10.0.33
mariadb101-server < 10.1.29
mariadb102-server < 10.2.10
mysql55-server < 5.5.58
mysql56-server < 5.6.38
mysql57-server < 5.7.20
percona55-server < 5.5.58
percona56-server < 5.6.38
percona57-server < 5.7.20

182497 - FreeBSD irssi Multiple Vulnerabilities (85e2c7eb-b74b-11e7-8546-5cf3fcfdd1f1)

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

Risk Level: Medium

CVE: CVE-2017-15227, CVE-2017-15228, CVE-2017-15721, CVE-2017-15722, CVE-2017-15723

Description

The scan detected that the host is missing the following update:
irssi -- multiple vulnerabilities (85e2c7eb-b74b-11e7-8546-5cf3fcfdd1f1)

Observation

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

http://www.vuxml.org/freebsd/85e2c7eb-b74b-11e7-8546-5cf3fcfdd1f1.html

Affected packages:
irssi < 1.0.5,1

185930 - Ubuntu Linux 14.04, 16.04 USN-3462-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7035, CVE-2016-7797

Description

The scan detected that the host is missing the following update:
USN-3462-1

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/004107.html

Ubuntu 14.04

pacemaker_1.1.10+git20130802-1ubuntu2.4

Ubuntu 16.04

pacemaker_1.1.14-2ubuntu1.2

185936 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3459-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10165, CVE-2017-10167, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10283, CVE-2017-10286, CVE-2017-10294, CVE-2017-10311, CVE-2017-10313, CVE-2017-10314, CVE-2017-10320, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

The scan detected that the host is missing the following update:
USN-3459-1

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/004100.html

Ubuntu 16.04

mysql-server-5.7_5.7.20-0ubuntu0.16.04.1

Ubuntu 14.04

mysql-server-5.5_5.5.58-0ubuntu0.14.04.1

Ubuntu 17.04

mysql-server-5.7_5.7.20-0ubuntu0.17.04.1

Ubuntu 17.10

mysql-server-5.7_5.7.20-0ubuntu0.17.10.1

192803 - Fedora Linux 25 FEDORA-2017-6e66393536 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14226

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6e66393536

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

libwpd-0.10.2-1.fc25

22619 - (SYM17-010) Symantec Endpoint Encryption Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-13675

Description

A vulnerability is present in some versions of Symantec Endpoint Encryption.

Observation

Symantec Endpoint Virtualization is a suite of products used for data storing in virtual layers.

A vulnerability is present in some versions of Symantec Endpoint Encryption. The flaw lies in an unspecified component. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

130915 - Debian Linux 8.0 DSA-4002-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10268, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

The scan detected that the host is missing the following update:
DSA-4002-1

Observation

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

http://www.debian.org/security/2017/dsa-4002

Debian 8.0
all
mysql-server_5.5.58-0+deb8u1
libmysqlclient-dev_5.5.58-0+deb8u1
mysql-testsuite_5.5.58-0+deb8u1
mysql-common_5.5.58-0+deb8u1
mysql-client-5.5_5.5.58-0+deb8u1
mysql-testsuite-5.5_5.5.58-0+deb8u1
mysql-server-5.5_5.5.58-0+deb8u1
mysql-client_5.5.58-0+deb8u1
libmysqld-dev_5.5.58-0+deb8u1
libmysqlclient18_5.5.58-0+deb8u1
mysql-source-5.5_5.5.58-0+deb8u1
libmysqld-pic_5.5.58-0+deb8u1
mysql-server-core-5.5_5.5.58-0+deb8u1

146000 - SuSE SLES 11 SP4 SUSE-SU-2017:2815-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-5526

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2815-1

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/003348.html

SuSE SLES 11 SP4
x86_64
xen-tools-domU-4.4.4_24-61.12.1
xen-libs-4.4.4_24-61.12.1
xen-kmp-default-4.4.4_24_3.0.101_108.10-61.12.1
xen-doc-html-4.4.4_24-61.12.1
xen-tools-4.4.4_24-61.12.1
xen-4.4.4_24-61.12.1
xen-libs-32bit-4.4.4_24-61.12.1

i586
xen-tools-domU-4.4.4_24-61.12.1
xen-kmp-default-4.4.4_24_3.0.101_108.10-61.12.1
xen-libs-4.4.4_24-61.12.1
xen-kmp-pae-4.4.4_24_3.0.101_108.10-61.12.1

146002 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2810-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7837, CVE-2017-1000250

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2810-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00069.html

SuSE Linux 42.2
x86_64
libbluetooth3-debuginfo-5.41-2.5.1
libbluetooth3-32bit-5.41-2.5.1
bluez-5.41-2.5.1
bluez-test-5.41-2.5.1
bluez-devel-5.41-2.5.1
bluez-debugsource-5.41-2.5.1
libbluetooth3-5.41-2.5.1
bluez-cups-debuginfo-5.41-2.5.1
libbluetooth3-debuginfo-32bit-5.41-2.5.1
bluez-debuginfo-5.41-2.5.1
bluez-test-debuginfo-5.41-2.5.1
bluez-cups-5.41-2.5.1
bluez-devel-32bit-5.41-2.5.1

i586
bluez-debugsource-5.41-2.5.1
bluez-debuginfo-5.41-2.5.1
bluez-cups-5.41-2.5.1

bluez-test-debuginfo-5.41-2.5.1
bluez-5.41-2.5.1
bluez-test-5.41-2.5.1
libbluetooth3-5.41-2.5.1
libbluetooth3-debuginfo-5.41-2.5.1
bluez-cups-debuginfo-5.41-2.5.1
bluez-devel-5.41-2.5.1

SuSE Linux 42.3
x86_64
bluez-debuginfo-5.41-6.1
libbluetooth3-32bit-5.41-6.1
bluez-devel-5.41-6.1
libbluetooth3-debuginfo-5.41-6.1
bluez-5.41-6.1
libbluetooth3-debuginfo-32bit-5.41-6.1
bluez-debugsource-5.41-6.1
bluez-test-debuginfo-5.41-6.1
bluez-cups-5.41-6.1
libbluetooth3-5.41-6.1
bluez-test-5.41-6.1
bluez-cups-debuginfo-5.41-6.1
bluez-devel-32bit-5.41-6.1

i586
bluez-test-5.41-6.1
libbluetooth3-debuginfo-5.41-6.1
bluez-cups-5.41-6.1
bluez-cups-debuginfo-5.41-6.1
bluez-devel-5.41-6.1
bluez-5.41-6.1
bluez-test-debuginfo-5.41-6.1
bluez-debugsource-5.41-6.1
bluez-debuginfo-5.41-6.1
libbluetooth3-5.41-6.1

146004 - SuSE Linux 42.3 openSUSE-SU-2017:2821-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15591, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-5526

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2821-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00072.html

SuSE Linux 42.3
x86_64
xen-libs-4.9.0_14-10.1
xen-tools-domU-4.9.0_14-10.1
xen-4.9.0_14-10.1

xen-doc-html-4.9.0_14-10.1
xen-libs-debuginfo-4.9.0_14-10.1
xen-tools-domU-debuginfo-4.9.0_14-10.1
xen-tools-debuginfo-4.9.0_14-10.1
xen-debugsource-4.9.0_14-10.1
xen-devel-4.9.0_14-10.1
xen-tools-4.9.0_14-10.1

146015 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2765-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15194

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2765-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00064.html

SuSE Linux 42.2
i586
cacti-spine-debugsource-1.1.26-7.9.1
cacti-spine-debuginfo-1.1.26-7.9.1
cacti-spine-1.1.26-7.9.1

noarch
cacti-1.1.26-16.9.1
cacti-doc-1.1.26-16.9.1

x86_64
cacti-spine-debugsource-1.1.26-7.9.1
cacti-spine-debuginfo-1.1.26-7.9.1
cacti-spine-1.1.26-7.9.1

SuSE Linux 42.3
i586
cacti-spine-debugsource-1.1.26-16.1
cacti-spine-1.1.26-16.1
cacti-spine-debuginfo-1.1.26-16.1

noarch
cacti-doc-1.1.26-25.1
cacti-1.1.26-25.1

x86_64
cacti-spine-debugsource-1.1.26-16.1
cacti-spine-1.1.26-16.1
cacti-spine-debuginfo-1.1.26-16.1

182495 - FreeBSD cacti Cross Site Scripting Issue (e1cb9dc9-daa9-44db-adde-e94d900e2f7f)

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

Risk Level: Medium

CVE: CVE-2017-15194

Description

The scan detected that the host is missing the following update:
cacti -- Cross Site Scripting issue (e1cb9dc9-daa9-44db-adde-e94d900e2f7f)

Observation

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

http://www.vuxml.org/freebsd/e1cb9dc9-daa9-44db-adde-e94d900e2f7f.html

Affected packages:
cacti < 1.1.26

192800 - Fedora Linux 25 FEDORA-2017-6bbb922009 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-2017-6bbb922009

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

check-mk-1.2.8p26-1.fc25

192811 - Fedora Linux 26 FEDORA-2017-9f36da1aac 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-2017-9f36da1aac

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

check-mk-1.2.8p26-1.fc26

130912 - Debian Linux 9.0 DSA-4003-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000256

Description

The scan detected that the host is missing the following update:
DSA-4003-1

Observation

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

http://www.debian.org/security/2017/dsa-4003

Debian 9.0
all
libvirt-daemon_3.0.0-4+deb9u1
libvirt-dev_3.0.0-4+deb9u1
libvirt-doc_3.0.0-4+deb9u1
libvirt-sanlock_3.0.0-4+deb9u1
libnss-libvirt_3.0.0-4+deb9u1
libvirt-daemon-system_3.0.0-4+deb9u1
libvirt-clients_3.0.0-4+deb9u1
libvirt0_3.0.0-4+deb9u1

130913 - Debian Linux 8.0, 9.0 DSA-4004-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7525

Description

The scan detected that the host is missing the following update:
DSA-4004-1

Observation

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

http://www.debian.org/security/2017/dsa-4004

Debian 8.0
all
libjackson2-databind-java-doc_2.4.2-2+deb8u1
libjackson2-databind-java_2.4.2-2+deb8u1

Debian 9.0
all
libjackson2-databind-java_2.8.6-1+deb9u1
libjackson2-databind-java-doc_2.8.6-1+deb9u1

182492 - FreeBSD chromium Multiple Vulnerabilities (a692bffe-b6ad-11e7-a1c2-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (a692bffe-b6ad-11e7-a1c2-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/a692bffe-b6ad-11e7-a1c2-e8e0b747a45a.html

Affected packages:
chromium < 62.0.3202.62

182498 - FreeBSD cURL Out Of Bounds Read (143ec3d6-b7cf-11e7-ac58-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-1000257

Description

The scan detected that the host is missing the following update:
cURL -- out of bounds read (143ec3d6-b7cf-11e7-ac58-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/143ec3d6-b7cf-11e7-ac58-b499baebfeaf.html

Affected packages:
7.20 <= curl < 7.56.1

182499 - FreeBSD h2o DoS In Workers (10c0fabc-b5da-11e7-816e-00bd5d1fff09)

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

Risk Level: Low

CVE: CVE-2017-10868, CVE-2017-10869

Description

The scan detected that the host is missing the following update:
h2o -- DoS in workers (10c0fabc-b5da-11e7-816e-00bd5d1fff09)

Observation

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

http://www.vuxml.org/freebsd/10c0fabc-b5da-11e7-816e-00bd5d1fff09.html

Affected packages:
h2o < 2.2.3

185933 - Ubuntu Linux 16.04, 17.04 USN-3460-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7087, CVE-2017-7089, CVE-2017-7090, CVE-2017-7091, CVE-2017-7092, CVE-2017-7093, CVE-2017-7095, CVE-2017-7096, CVE-2017-7098, CVE-2017-7100, CVE-2017-7102, CVE-2017-7104, CVE-2017-7107, CVE-2017-7109, CVE-2017-7111, CVE-2017-7117, CVE-2017-7120

Description

The scan detected that the host is missing the following update:
USN-3460-1

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/004101.html

Ubuntu 17.04

libjavascriptcoregtk-4.0-18_2.18.0-0ubuntu0.17.04.2
libwebkit2gtk-4.0-37_2.18.0-0ubuntu0.17.04.2

Ubuntu 16.04

libwebkit2gtk-4.0-37_2.18.0-0ubuntu0.16.04.2
libjavascriptcoregtk-4.0-18_2.18.0-0ubuntu0.16.04.2

185938 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3457-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000257

Description

The scan detected that the host is missing the following update:
USN-3457-1

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/004099.html

Ubuntu 16.04

libcurl3-gnutls_7.47.0-1ubuntu2.4
libcurl3_7.47.0-1ubuntu2.4
libcurl3-nss_7.47.0-1ubuntu2.4
curl_7.47.0-1ubuntu2.4

Ubuntu 14.04

curl_7.35.0-1ubuntu2.12
libcurl3-nss_7.35.0-1ubuntu2.12
libcurl3_7.35.0-1ubuntu2.12
libcurl3-gnutls_7.35.0-1ubuntu2.12

Ubuntu 17.04

curl_7.52.1-4ubuntu1.3
libcurl3-nss_7.52.1-4ubuntu1.3
libcurl3-gnutls_7.52.1-4ubuntu1.3
libcurl3_7.52.1-4ubuntu1.3

Ubuntu 17.10

libcurl3-gnutls_7.55.1-1ubuntu2.1
curl_7.55.1-1ubuntu2.1
libcurl3_7.55.1-1ubuntu2.1
libcurl3-nss_7.55.1-1ubuntu2.1

192798 - Fedora Linux 27 FEDORA-2017-ce403f01ce Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2888

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ce403f01ce

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

SDL2-2.0.6-4.fc27

192799 - Fedora Linux 26 FEDORA-2017-a62dd57720 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-a62dd57720

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-6.9.9.19-1.fc26
rubygem-rmagick-2.16.0-8.fc26

192801 - Fedora Linux 25 FEDORA-2017-3c5282ada7 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-2017-3c5282ada7

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

rubygem-rmagick-2.16.0-8.fc25
ImageMagick-6.9.9.19-1.fc25

192802 - Fedora Linux 25 FEDORA-2017-caafcbd6b9 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-caafcbd6b9

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

upx-3.94-1.fc25

192805 - Fedora Linux 27 FEDORA-2017-39c5f8cd7e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
FEDORA-2017-39c5f8cd7e

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

sssd-1.15.3-5.fc27

192807 - Fedora Linux 25 FEDORA-2017-15987a1b7f 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-2017-15987a1b7f

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

SDL2_image-2.0.1-8.fc25

192810 - Fedora Linux 25 FEDORA-2017-8f7bca960b 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-2017-8f7bca960b

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

golang-1.7.6-3.fc25

192812 - Fedora Linux 26 FEDORA-2017-d22c391318 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-d22c391318

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

upx-3.94-1.fc26

192813 - Fedora Linux 26 FEDORA-2017-65b543b628 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
FEDORA-2017-65b543b628

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

sssd-1.15.3-5.fc26

192814 - Fedora Linux 26 FEDORA-2017-9b0095a6f2 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-2017-9b0095a6f2

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

SDL2_image-2.0.1-8.fc26

22610 - (HPESBHF03705) HPE Integrated Lights-Out Information Disclosure Vulnerability

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

Risk Level: Low

CVE: CVE-2017-12543

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 disclose private information.

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.

20382 - (MS16-099) Security Update for Microsoft Office (3177451)

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

Risk Level: High

CVE: CVE-2016-3313, CVE-2016-3315, CVE-2016-3316, CVE-2016-3317, CVE-2016-3318

Update Details

FASLScript is updated

21805 - (MSPT-May2017) Microsoft Office Remote Code Execution Vulnerability (CVE-2017-0281)

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

Risk Level: High

CVE: CVE-2017-0281

Update Details

FASLScript is updated

130900 - Debian Linux 8.0, 9.0 DSA-3984-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14867

Update Details

Risk is updated

145968 - SuSE Linux 42.3 openSUSE-SU-2017:2614-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14867

Update Details

Risk is updated

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: High

CVE: CVE-2017-14867

Update Details

Risk is updated

22611 - Wireshark Multiple Vulnerabilities Prior To 2.4.2

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

Risk Level: High

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

Update Details

Risk is updated

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

Update Details

Risk is updated

130899 - Debian Linux 8.0, 9.0 DSA-3989-1 Update Is Not Installed

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

Risk Level: High

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

Update Details

Risk is updated

132401 - Oracle VM OVMSA-2017-0160 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2017-14491

Update Details
Risk is updated

141734 - Red Hat Enterprise Linux RHSA-2017-2838 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491

Update Details
Risk is updated

141735 - Red Hat Enterprise Linux RHSA-2017-2836 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496

Update Details
Risk is updated

141736 - Red Hat Enterprise Linux RHSA-2017-2839 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491

Update Details
Risk is updated

141737 - Red Hat Enterprise Linux RHSA-2017-2837 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494

Update Details
Risk is updated

141740 - Red Hat Enterprise Linux RHSA-2017-2841 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491

Update Details
Risk is updated

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
Risk is updated

163467 - Oracle Enterprise Linux ELSA-2017-2840 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491

Update Details
Risk is updated

163469 - Oracle Enterprise Linux ELSA-2017-2836 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496

Update Details
Risk is updated

163470 - Oracle Enterprise Linux ELSA-2017-2838 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491

Update Details
Risk is updated

170880 - Amazon Linux AMI ALAS-2017-907 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496

Update Details
Risk is updated

175267 - Scientific Linux Security ERRATA Critical: dnsmasq on SL6.x i386/x86_64 (1710-78)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: High
CVE: CVE-2017-14491

Update Details

Risk is updated

175270 - Scientific Linux Security ERRATA Critical: dnsmasq on SL7.x x86_64 (1710-406)

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

Risk Level: High

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

Update Details

Risk is updated

182416 - FreeBSD Mercurial Multiple Vulnerabilities (1d33cdee-7f6b-11e7-a9b5-3debb10a6871)

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

Risk Level: High

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

Update Details

Risk is updated

182460 - FreeBSD dnsmasq Multiple Vulnerabilities (b77b5646-a778-11e7-ac58-b499baebfeaf)

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

Risk Level: High

CVE: CVE-2017-13704, CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496

Update Details

Risk is updated

185896 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3430-1 Update Is Not Installed

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

Risk Level: High

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

Update Details

Risk is updated

192570 - Fedora Linux 26 FEDORA-2017-f03b04acbb Update Is Not Installed

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

Risk Level: High

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

Update Details

Risk is updated

192698 - Fedora Linux 25 FEDORA-2017-fa1d8ad61a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000115, CVE-2017-1000116

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496

Update Details
Risk is updated

182471 - FreeBSD OpenVPN Out-of-bounds Write In Legacy Key-method 1 (3dd6ccf4-a3c6-11e7-a52e-0800279f2ff8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12166

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12617

Update Details
Risk is updated

192703 - Fedora Linux 27 FEDORA-2017-5882331351 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12166

Update Details
Risk is updated

192729 - Fedora Linux 26 FEDORA-2017-700915e34f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12166

Update Details
Risk is updated

20379 - (MS16-099) Microsoft Office Graphics Component Memory Corruption Remote Code Execution (3177451)

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

Risk Level: Medium

CVE: CVE-2016-3318

Update Details

FASLScript is updated

21755 - (MSPT-May2017) Microsoft .Net Security Feature Bypass Vulnerability (CVE-2017-0248)

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

Risk Level: Medium

CVE: CVE-2017-0248

Update Details

FASLScript is updated

192705 - Fedora Linux 27 FEDORA-2017-274d763ed8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13704

Update Details

Risk is updated

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

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

Risk Level: Medium

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

Update Details

Risk is updated

145489 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2174-1 Update Is Not Installed

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

Risk Level: Medium

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

Update Details

Risk is updated

145862 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2205-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2017-1000100, CVE-2017-1000101

Update Details
Risk is updated

170855 - Amazon Linux AMI ALAS-2017-889 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000099, CVE-2017-1000100, CVE-2017-1000101

Update Details
Risk is updated

182410 - FreeBSD cURL Multiple Vulnerabilities (69cfa386-7cd0-11e7-867f-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000099, CVE-2017-1000100, CVE-2017-1000101

Update Details
Risk is updated

192508 - Fedora Linux 25 FEDORA-2017-f2df9d7772 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000100, CVE-2017-1000101

Update Details
Risk is updated

192520 - Fedora Linux 26 FEDORA-2017-f1ffd18079 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000100, CVE-2017-1000101

Update Details
Risk is updated

192528 - Fedora Linux 25 FEDORA-2017-571e659c85 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000100, CVE-2017-1000101, CVE-2017-7000

Update Details
Risk is updated

70116 - scada.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.