2017-SEP-28
FSL version 7.5.963

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

22461 - (APSB17-30) Vulnerabilities In Adobe ColdFusion

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

Risk Level: High

CVE: CVE-2017-11283, CVE-2017-11284, CVE-2017-11285, CVE-2017-11286

Description

Multiple vulnerabilities are present in some versions of Adobe ColdFusion.

Observation

Adobe ColdFusion is a web application development platform.

Multiple vulnerabilities are present in some versions of Adobe ColdFusion. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, or execute arbitrary code.

The update provided by Adobe bulletin APSB17-30 resolves these issues. The target system appears to be missing this update.

22492 - Schneider Electric InduSoft Web Studio Missing Authentication Vulnerability

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

Risk Level: High

CVE: CVE-2017-13997

Description

A vulnerability in some versions of Schneider Electric InduSoft Web Studio could lead to a remote code execution.

Observation

InduSoft Web Studio is a tool to build SCADA (Supervisory Control And Data Acquisition) or HMI (Human-Machine Interface) applications.

A vulnerability in some versions of Schneider Electric InduSoft Web Studio could lead to a remote code execution. The flaw lies in how the server handles user authentication. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

178509 - Gentoo Linux GLSA-201709-24 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6706

Description

The scan detected that the host is missing the following update:
GLSA-201709-24

Observation

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

https://security.gentoo.org/glsa/201709-24

Affected packages:
app-arch/rar < 5.5.0_p20170811
app-arch/unrar < 5.5.7

22464 - (K23873366) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-2177

Description

A vulnerability is present in some versions of F5's BIG-IP Products.

Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in data plane and control plane. Successful exploitation could allow an attacker to cause a denial of service condition.

22469 - IBM DB2 Privilege Escalation Vulnerability (swg22006885)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-1438

Description

A privilege escalation vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A privilege escalation vulnerability is present in some versions of IBM DB2. A flaw lies in IBM DB2 application. Successful exploitation could allow an attacker to gain privileges.

22484 - IBM AIX Java6 Multiple Vulnerabilities (java6_advisory)

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

Risk Level: High

CVE: CVE-2017-1541

Description

A vulnerability is present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

A vulnerability is present in some versions of IBM AIX. The flaws lie in Java SDK component. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

22485 - (K52320548) F5 BIG-IP Expat Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-0718

Description

A vulnerability is present in some versions of F5's BIG-IP Products.

Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in iControl SOAP, eventd component. Successful exploitation could allow an attacker to cause a denial-of-service condition or possibly run arbitrary code on target system.

22490 - WordPress Multiple Vulnerabilities Prior To 4.8.2

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of WordPress.

Observation

WordPress is a popular blog application.

Multiple vulnerabilities are present in some versions of WordPress. The flaws lie in multiple components. Successful exploitation could allow an attacker to remotely execute arbitrary code.

141725 - Red Hat Enterprise Linux RHSA-2017-2794 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
RHSA-2017-2794

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00059.html

RHEL7_2S
noarch

kernel-abi-whitelists-3.10.0-327.59.3.el7
kernel-doc-3.10.0-327.59.3.el7

x86_64
kernel-tools-3.10.0-327.59.3.el7
kernel-headers-3.10.0-327.59.3.el7
python-perf-debuginfo-3.10.0-327.59.3.el7
kernel-tools-debuginfo-3.10.0-327.59.3.el7
perf-3.10.0-327.59.3.el7
kernel-debug-debuginfo-3.10.0-327.59.3.el7
perf-debuginfo-3.10.0-327.59.3.el7
python-perf-3.10.0-327.59.3.el7
kernel-debug-3.10.0-327.59.3.el7
kernel-debug-devel-3.10.0-327.59.3.el7
kernel-devel-3.10.0-327.59.3.el7
kernel-3.10.0-327.59.3.el7
kernel-debuginfo-common-x86_64-3.10.0-327.59.3.el7
kernel-tools-libs-devel-3.10.0-327.59.3.el7
kernel-debuginfo-3.10.0-327.59.3.el7
kernel-tools-libs-3.10.0-327.59.3.el7

141726 - Red Hat Enterprise Linux RHSA-2017-2792 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5121, CVE-2017-5122

Description

The scan detected that the host is missing the following update:
RHSA-2017-2792

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00053.html

RHEL6D
x86_64
chromium-browser-debuginfo-61.0.3163.100-1.el6_9
chromium-browser-61.0.3163.100-1.el6_9

i386
chromium-browser-debuginfo-61.0.3163.100-1.el6_9
chromium-browser-61.0.3163.100-1.el6_9

RHEL6S
x86_64
chromium-browser-debuginfo-61.0.3163.100-1.el6_9
chromium-browser-61.0.3163.100-1.el6_9

i386
chromium-browser-debuginfo-61.0.3163.100-1.el6_9
chromium-browser-61.0.3163.100-1.el6_9

RHEL6WS
x86_64
chromium-browser-debuginfo-61.0.3163.100-1.el6_9

chromium-browser-61.0.3163.100-1.el6_9

i386
chromium-browser-debuginfo-61.0.3163.100-1.el6_9
chromium-browser-61.0.3163.100-1.el6_9

141727 - Red Hat Enterprise Linux RHSA-2017-2798 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
RHSA-2017-2798

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00058.html

RHEL6_5S
x86_64
kernel-debug-devel-2.6.32-431.85.1.el6
perf-2.6.32-431.85.1.el6
kernel-debug-2.6.32-431.85.1.el6
perf-debuginfo-2.6.32-431.85.1.el6
kernel-debug-debuginfo-2.6.32-431.85.1.el6
kernel-2.6.32-431.85.1.el6
kernel-devel-2.6.32-431.85.1.el6
python-perf-debuginfo-2.6.32-431.85.1.el6
kernel-debuginfo-2.6.32-431.85.1.el6
kernel-debuginfo-common-x86_64-2.6.32-431.85.1.el6
python-perf-2.6.32-431.85.1.el6
kernel-headers-2.6.32-431.85.1.el6

noarch
kernel-doc-2.6.32-431.85.1.el6
kernel-abi-whitelists-2.6.32-431.85.1.el6
kernel-firmware-2.6.32-431.85.1.el6

141728 - Red Hat Enterprise Linux RHSA-2017-2800 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
RHSA-2017-2800

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00054.html

RHEL6_2S
x86_64
python-perf-debuginfo-2.6.32-220.76.1.el6
kernel-debug-devel-2.6.32-220.76.1.el6
kernel-debug-debuginfo-2.6.32-220.76.1.el6
perf-debuginfo-2.6.32-220.76.1.el6
kernel-debuginfo-common-x86_64-2.6.32-220.76.1.el6
kernel-headers-2.6.32-220.76.1.el6
kernel-debug-2.6.32-220.76.1.el6
kernel-2.6.32-220.76.1.el6
perf-2.6.32-220.76.1.el6
python-perf-2.6.32-220.76.1.el6
kernel-devel-2.6.32-220.76.1.el6
kernel-debuginfo-2.6.32-220.76.1.el6

noarch
kernel-firmware-2.6.32-220.76.1.el6
kernel-doc-2.6.32-220.76.1.el6

141729 - Red Hat Enterprise Linux RHSA-2017-2795 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
RHSA-2017-2795

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00067.html

RHEL6D
i386
kernel-debuginfo-2.6.32-696.10.3.el6
kernel-debug-devel-2.6.32-696.10.3.el6
perf-debuginfo-2.6.32-696.10.3.el6
kernel-2.6.32-696.10.3.el6
perf-2.6.32-696.10.3.el6
python-perf-2.6.32-696.10.3.el6
kernel-headers-2.6.32-696.10.3.el6
kernel-debug-debuginfo-2.6.32-696.10.3.el6
python-perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-i686-2.6.32-696.10.3.el6
kernel-devel-2.6.32-696.10.3.el6
kernel-debug-2.6.32-696.10.3.el6

noarch
kernel-abi-whitelists-2.6.32-696.10.3.el6
kernel-firmware-2.6.32-696.10.3.el6
kernel-doc-2.6.32-696.10.3.el6

x86_64

kernel-headers-2.6.32-696.10.3.el6
python-perf-2.6.32-696.10.3.el6
kernel-debug-devel-2.6.32-696.10.3.el6
kernel-2.6.32-696.10.3.el6
python-perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-i686-2.6.32-696.10.3.el6
perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-x86_64-2.6.32-696.10.3.el6
perf-2.6.32-696.10.3.el6
kernel-debuginfo-2.6.32-696.10.3.el6
kernel-debug-debuginfo-2.6.32-696.10.3.el6
kernel-debug-2.6.32-696.10.3.el6
kernel-devel-2.6.32-696.10.3.el6

RHEL6S
i386
kernel-debuginfo-2.6.32-696.10.3.el6
kernel-debug-devel-2.6.32-696.10.3.el6
perf-debuginfo-2.6.32-696.10.3.el6
kernel-2.6.32-696.10.3.el6
perf-2.6.32-696.10.3.el6
python-perf-2.6.32-696.10.3.el6
kernel-headers-2.6.32-696.10.3.el6
kernel-debug-debuginfo-2.6.32-696.10.3.el6
python-perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-i686-2.6.32-696.10.3.el6
kernel-devel-2.6.32-696.10.3.el6
kernel-debug-2.6.32-696.10.3.el6

noarch
kernel-abi-whitelists-2.6.32-696.10.3.el6
kernel-firmware-2.6.32-696.10.3.el6
kernel-doc-2.6.32-696.10.3.el6

x86_64
kernel-headers-2.6.32-696.10.3.el6
python-perf-2.6.32-696.10.3.el6
kernel-debug-devel-2.6.32-696.10.3.el6
kernel-2.6.32-696.10.3.el6
python-perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-i686-2.6.32-696.10.3.el6
perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-x86_64-2.6.32-696.10.3.el6
perf-2.6.32-696.10.3.el6
kernel-debuginfo-2.6.32-696.10.3.el6
kernel-debug-debuginfo-2.6.32-696.10.3.el6
kernel-debug-2.6.32-696.10.3.el6
kernel-devel-2.6.32-696.10.3.el6

RHEL6WS
i386
kernel-debuginfo-2.6.32-696.10.3.el6
kernel-debug-devel-2.6.32-696.10.3.el6
perf-debuginfo-2.6.32-696.10.3.el6
kernel-2.6.32-696.10.3.el6
perf-2.6.32-696.10.3.el6
kernel-headers-2.6.32-696.10.3.el6
kernel-debug-debuginfo-2.6.32-696.10.3.el6
python-perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-i686-2.6.32-696.10.3.el6

kernel-devel-2.6.32-696.10.3.el6
kernel-debug-2.6.32-696.10.3.el6

noarch
kernel-abi-whitelists-2.6.32-696.10.3.el6
kernel-firmware-2.6.32-696.10.3.el6
kernel-doc-2.6.32-696.10.3.el6

x86_64
kernel-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-x86_64-2.6.32-696.10.3.el6
kernel-debug-devel-2.6.32-696.10.3.el6
perf-debuginfo-2.6.32-696.10.3.el6
kernel-2.6.32-696.10.3.el6
perf-2.6.32-696.10.3.el6
kernel-headers-2.6.32-696.10.3.el6
kernel-debug-debuginfo-2.6.32-696.10.3.el6
python-perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-i686-2.6.32-696.10.3.el6
kernel-devel-2.6.32-696.10.3.el6
kernel-debug-2.6.32-696.10.3.el6

141730 - Red Hat Enterprise Linux RHSA-2017-2797 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
RHSA-2017-2797

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00057.html

RHEL6_6S
x86_64
kernel-2.6.32-504.63.3.el6
perf-2.6.32-504.63.3.el6
python-perf-debuginfo-2.6.32-504.63.3.el6
kernel-debug-debuginfo-2.6.32-504.63.3.el6
kernel-debug-devel-2.6.32-504.63.3.el6
python-perf-2.6.32-504.63.3.el6
kernel-debuginfo-2.6.32-504.63.3.el6
perf-debuginfo-2.6.32-504.63.3.el6
kernel-headers-2.6.32-504.63.3.el6
kernel-debug-2.6.32-504.63.3.el6
kernel-devel-2.6.32-504.63.3.el6
kernel-debuginfo-common-x86_64-2.6.32-504.63.3.el6

noarch
kernel-firmware-2.6.32-504.63.3.el6
kernel-doc-2.6.32-504.63.3.el6
kernel-abi-whitelists-2.6.32-504.63.3.el6

141731 - Red Hat Enterprise Linux RHSA-2017-2799 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
RHSA-2017-2799

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00056.html

RHEL6_4S
x86_64
kernel-debug-devel-2.6.32-358.84.1.el6
kernel-headers-2.6.32-358.84.1.el6
kernel-debug-2.6.32-358.84.1.el6
kernel-debuginfo-common-x86_64-2.6.32-358.84.1.el6
perf-2.6.32-358.84.1.el6
python-perf-2.6.32-358.84.1.el6
python-perf-debuginfo-2.6.32-358.84.1.el6
kernel-2.6.32-358.84.1.el6
kernel-devel-2.6.32-358.84.1.el6
kernel-debuginfo-2.6.32-358.84.1.el6
kernel-debug-debuginfo-2.6.32-358.84.1.el6
perf-debuginfo-2.6.32-358.84.1.el6

noarch
kernel-doc-2.6.32-358.84.1.el6
kernel-firmware-2.6.32-358.84.1.el6

141732 - Red Hat Enterprise Linux RHSA-2017-2802 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
RHSA-2017-2802

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00066.html

RHEL5_9S
i386
kernel-headers-2.6.18-348.34.2.el5
kernel-xen-debuginfo-2.6.18-348.34.2.el5
kernel-debug-2.6.18-348.34.2.el5

kernel-xen-2.6.18-348.34.2.el5
kernel-PAE-2.6.18-348.34.2.el5
kernel-debuginfo-2.6.18-348.34.2.el5
kernel-debuginfo-common-2.6.18-348.34.2.el5
kernel-PAE-devel-2.6.18-348.34.2.el5
kernel-debug-debuginfo-2.6.18-348.34.2.el5
kernel-debug-devel-2.6.18-348.34.2.el5
kernel-PAE-debuginfo-2.6.18-348.34.2.el5
kernel-xen-devel-2.6.18-348.34.2.el5
kernel-devel-2.6.18-348.34.2.el5
kernel-2.6.18-348.34.2.el5

noarch
kernel-doc-2.6.18-348.34.2.el5

x86_64
kernel-xen-debuginfo-2.6.18-348.34.2.el5
kernel-devel-2.6.18-348.34.2.el5
kernel-headers-2.6.18-348.34.2.el5
kernel-debug-debuginfo-2.6.18-348.34.2.el5
kernel-2.6.18-348.34.2.el5
kernel-xen-devel-2.6.18-348.34.2.el5
kernel-xen-2.6.18-348.34.2.el5
kernel-debug-devel-2.6.18-348.34.2.el5
kernel-debug-2.6.18-348.34.2.el5
kernel-debuginfo-common-2.6.18-348.34.2.el5
kernel-debuginfo-2.6.18-348.34.2.el5

141733 - Red Hat Enterprise Linux RHSA-2017-2796 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
RHSA-2017-2796

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00061.html

RHEL6_7S
i386
kernel-2.6.32-573.48.1.el6
kernel-debug-2.6.32-573.48.1.el6
python-perf-debuginfo-2.6.32-573.48.1.el6
kernel-debuginfo-2.6.32-573.48.1.el6
kernel-debuginfo-common-i686-2.6.32-573.48.1.el6
kernel-debug-debuginfo-2.6.32-573.48.1.el6
python-perf-2.6.32-573.48.1.el6
kernel-debug-devel-2.6.32-573.48.1.el6
kernel-devel-2.6.32-573.48.1.el6
perf-debuginfo-2.6.32-573.48.1.el6
perf-2.6.32-573.48.1.el6
kernel-headers-2.6.32-573.48.1.el6

noarch
kernel-doc-2.6.32-573.48.1.el6
kernel-firmware-2.6.32-573.48.1.el6
kernel-abi-whitelists-2.6.32-573.48.1.el6

x86_64
python-perf-debuginfo-2.6.32-573.48.1.el6
kernel-devel-2.6.32-573.48.1.el6
kernel-headers-2.6.32-573.48.1.el6
kernel-debuginfo-2.6.32-573.48.1.el6
kernel-debuginfo-common-i686-2.6.32-573.48.1.el6
kernel-debug-debuginfo-2.6.32-573.48.1.el6
python-perf-2.6.32-573.48.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.48.1.el6
perf-2.6.32-573.48.1.el6
kernel-debug-2.6.32-573.48.1.el6
perf-debuginfo-2.6.32-573.48.1.el6
kernel-2.6.32-573.48.1.el6
kernel-debug-devel-2.6.32-573.48.1.el6

145946 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2555-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13765, CVE-2017-13766, CVE-2017-13767, CVE-2017-9617, CVE-2017-9766

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2555-1

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-September/003258.html

SuSE SLES 12 SP2
x86_64
wireshark-gtk-2.2.9-48.9.2
libwireshark8-debuginfo-2.2.9-48.9.2
libwireshark8-2.2.9-48.9.2
libwiretap6-2.2.9-48.9.2
wireshark-debugsource-2.2.9-48.9.2
wireshark-debuginfo-2.2.9-48.9.2
libwscodecs1-2.2.9-48.9.2
libwscodecs1-debuginfo-2.2.9-48.9.2
libwiretap6-debuginfo-2.2.9-48.9.2
wireshark-gtk-debuginfo-2.2.9-48.9.2
libwsutil7-debuginfo-2.2.9-48.9.2
libwsutil7-2.2.9-48.9.2
wireshark-2.2.9-48.9.2

SuSE SLED 12 SP3
x86_64
wireshark-gtk-2.2.9-48.9.2
libwireshark8-debuginfo-2.2.9-48.9.2
libwireshark8-2.2.9-48.9.2
libwiretap6-2.2.9-48.9.2

wireshark-debugsource-2.2.9-48.9.2
wireshark-debuginfo-2.2.9-48.9.2
libwscodecs1-2.2.9-48.9.2
libwscodecs1-debuginfo-2.2.9-48.9.2
libwiretap6-debuginfo-2.2.9-48.9.2
wireshark-gtk-debuginfo-2.2.9-48.9.2
libwsutil7-debuginfo-2.2.9-48.9.2
libwsutil7-2.2.9-48.9.2
wireshark-2.2.9-48.9.2

SuSE SLED 12 SP2
x86_64
wireshark-gtk-2.2.9-48.9.2
libwireshark8-debuginfo-2.2.9-48.9.2
libwireshark8-2.2.9-48.9.2
libwiretap6-2.2.9-48.9.2
wireshark-debugsource-2.2.9-48.9.2
wireshark-debuginfo-2.2.9-48.9.2
libwscodecs1-2.2.9-48.9.2
libwscodecs1-debuginfo-2.2.9-48.9.2
libwiretap6-debuginfo-2.2.9-48.9.2
wireshark-gtk-debuginfo-2.2.9-48.9.2
libwsutil7-debuginfo-2.2.9-48.9.2
libwsutil7-2.2.9-48.9.2
wireshark-2.2.9-48.9.2

SuSE SLES 12 SP3
x86_64
wireshark-gtk-2.2.9-48.9.2
libwireshark8-debuginfo-2.2.9-48.9.2
libwireshark8-2.2.9-48.9.2
libwiretap6-2.2.9-48.9.2
wireshark-debugsource-2.2.9-48.9.2
wireshark-debuginfo-2.2.9-48.9.2
libwscodecs1-2.2.9-48.9.2
libwscodecs1-debuginfo-2.2.9-48.9.2
libwiretap6-debuginfo-2.2.9-48.9.2
wireshark-gtk-debuginfo-2.2.9-48.9.2
libwsutil7-debuginfo-2.2.9-48.9.2
libwsutil7-2.2.9-48.9.2
wireshark-2.2.9-48.9.2

145947 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2557-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5121, CVE-2017-5122

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2557-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00097.html

SuSE Linux 42.2
x86_64
chromedriver-debuginfo-61.0.3163.100-104.27.1
chromedriver-61.0.3163.100-104.27.1
chromium-debugsource-61.0.3163.100-104.27.1
chromium-61.0.3163.100-104.27.1
chromium-debuginfo-61.0.3163.100-104.27.1

SuSE Linux 42.3
x86_64
chromedriver-61.0.3163.100-113.1
chromedriver-debuginfo-61.0.3163.100-113.1
chromium-debugsource-61.0.3163.100-113.1
chromium-61.0.3163.100-113.1
chromium-debuginfo-61.0.3163.100-113.1

145951 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2573-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0380

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2573-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00105.html

SuSE Linux 42.2
x86_64
tor-0.2.9.12-8.6.1
tor-debuginfo-0.2.9.12-8.6.1
tor-debugsource-0.2.9.12-8.6.1

i586
tor-0.2.9.12-8.6.1
tor-debuginfo-0.2.9.12-8.6.1
tor-debugsource-0.2.9.12-8.6.1

SuSE Linux 42.3
x86_64
tor-0.3.0.11-3.1
tor-debugsource-0.3.0.11-3.1
tor-debuginfo-0.3.0.11-3.1

i586
tor-0.3.0.11-3.1
tor-debugsource-0.3.0.11-3.1
tor-debuginfo-0.3.0.11-3.1

163462 - Oracle Enterprise Linux ELSA-2017-2788 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7555

Description

The scan detected that the host is missing the following update:
ELSA-2017-2788

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007223.html

OEL7
x86_64
augeas-1.4.0-2.el7_4.1
augeas-libs-1.4.0-2.el7_4.1
augeas-devel-1.4.0-2.el7_4.1

175266 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1709-3476)

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

Risk Level: High

CVE: CVE-2017-1000253

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1709-3476)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1709&L=scientific-linux-errata&F=&S=&P=3476

SL6
i386
kernel-debuginfo-2.6.32-696.10.3.el6
kernel-debug-devel-2.6.32-696.10.3.el6
perf-debuginfo-2.6.32-696.10.3.el6
kernel-2.6.32-696.10.3.el6
perf-2.6.32-696.10.3.el6
python-perf-2.6.32-696.10.3.el6
kernel-headers-2.6.32-696.10.3.el6
kernel-debug-debuginfo-2.6.32-696.10.3.el6
python-perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-i686-2.6.32-696.10.3.el6
kernel-devel-2.6.32-696.10.3.el6
kernel-debug-2.6.32-696.10.3.el6

noarch
kernel-abi-whitelists-2.6.32-696.10.3.el6
kernel-firmware-2.6.32-696.10.3.el6
kernel-doc-2.6.32-696.10.3.el6

x86_64
kernel-headers-2.6.32-696.10.3.el6

python-perf-2.6.32-696.10.3.el6
kernel-debug-devel-2.6.32-696.10.3.el6
kernel-2.6.32-696.10.3.el6
python-perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-i686-2.6.32-696.10.3.el6
perf-debuginfo-2.6.32-696.10.3.el6
kernel-debuginfo-common-x86_64-2.6.32-696.10.3.el6
perf-2.6.32-696.10.3.el6
kernel-debuginfo-2.6.32-696.10.3.el6
kernel-debug-debuginfo-2.6.32-696.10.3.el6
kernel-debug-2.6.32-696.10.3.el6
kernel-devel-2.6.32-696.10.3.el6

178505 - Gentoo Linux GLSA-201709-20 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-20

Observation

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

https://security.gentoo.org/glsa/201709-20

Affected packages:
mail-mta/postfix < 3.1.6

178507 - Gentoo Linux GLSA-201709-16 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-16

Observation

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

https://security.gentoo.org/glsa/201709-16

Affected packages:
www-plugins/adobe-flash < 27.0.0.130-r1

182447 - FreeBSD libraw Denial Of Service And Remote Code Execution (4cd857d9-26d2-4417-b765-69701938f9e0)

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

Risk Level: High

CVE: CVE-2017-14265

Description

The scan detected that the host is missing the following update:
libraw -- denial of service and remote code execution (4cd857d9-26d2-4417-b765-69701938f9e0)

Observation

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

http://www.vuxml.org/freebsd/4cd857d9-26d2-4417-b765-69701938f9e0.html

Affected packages:
libraw < 0.18.3

182457 - FreeBSD tcpdump Multiple Vulnerabilities (eb03d642-6724-472d-b038-f2bf074e1fc8)

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

Risk Level: High

CVE: CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004, CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010, CVE-2017-13011, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016, CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022, CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028, CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034, CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040, CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046, CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052, CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689, CVE-2017-13690, CVE-2017-13725

Description

The scan detected that the host is missing the following update:
tcpdump -- multiple vulnerabilities (eb03d642-6724-472d-b038-f2bf074e1fc8)

Observation

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

http://www.vuxml.org/freebsd/eb03d642-6724-472d-b038-f2bf074e1fc8.html

Affected packages:
tcpdump < 4.9.2

192660 - Fedora Linux 25 FEDORA-2017-56e23bc2b5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11462

Description

The scan detected that the host is missing the following update:
FEDORA-2017-56e23bc2b5

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/2017/9/?count=200&page=2

Fedora Core 25

krb5-1.14.4-9.fc25

192663 - Fedora Linux 25 FEDORA-2017-e314044789 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9224, CVE-2017-9225, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, CVE-2017-9229

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e314044789

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/2017/9/?count=200&page=1

Fedora Core 25

oniguruma-6.1.3-3.fc25

192664 - Fedora Linux 26 FEDORA-2017-90500f87f3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13735, CVE-2017-14265, CVE-2017-14348

Description

The scan detected that the host is missing the following update:
FEDORA-2017-90500f87f3

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/2017/9/?count=200&page=1

Fedora Core 26

LibRaw-0.18.5-1.fc26

192675 - Fedora Linux 26 FEDORA-2017-3202aed903 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14497

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3202aed903

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/2017/9/?count=200&page=1

Fedora Core 26

kernel-4.12.14-300.fc26

22470 - mySCADA myPRO DLL Hijacking Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-12730

Description

A DLL hijacking vulnerability is present in some versions of mySCADA myPRO Software.

Observation

mySCADA myPRO Software is a HMI/SCADA software used to create robust HMI screens to control machine, process.

A DLL hijacking vulnerability is present in some versions of mySCADA myPRO Software. The flaw is related to an uncontrolled search path element. Successful exploitation could allow an attacker to execute arbitrary code on the system.

22471 - (SYM17-008) Symantec Encryption Desktop Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-6330

Description

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

Observation

Symantec Encryption Desktop provides comprehensive security for desktops and laptops.

A vulnerability is present in some versions of Symantec Encryption Desktop. The flaw lies in an unknown component. Successful exploitation by a remote attacker could result in a denial of service condition.

22475 - IBM WebSphere Application Server Liberty Profile Multiple Java Vulnerabilities (swg22007002)

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

Risk Level: Medium

CVE: CVE-2017-10102, CVE-2017-10115, CVE-2017-10116

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server Liberty Profile.

Observation

IBM WebSphere Application Server Liberty Profile is a server engine for Java EE Web applications.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server Liberty Profile. The flaws lie in the IBM Java SDK component. Exploitation could allow a malicious unauthenticated user to obtain sensitive information or take control of the system.

145945 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2570-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13738, CVE-2017-13739, CVE-2017-13740, CVE-2017-13741, CVE-2017-13743, CVE-2017-13744

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2570-1

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-September/003260.html

SuSE SLES 12 SP2
x86_64
liblouis9-2.6.4-6.3.1
liblouis9-debuginfo-2.6.4-6.3.1
liblouis-data-2.6.4-6.3.1
python-louis-2.6.4-6.3.1
python3-louis-2.6.4-6.3.1
liblouis-debugsource-2.6.4-6.3.1

SuSE SLED 12 SP3
x86_64
liblouis9-2.6.4-6.3.1
python3-louis-2.6.4-6.3.1
liblouis-data-2.6.4-6.3.1
liblouis-debugsource-2.6.4-6.3.1
liblouis9-debuginfo-2.6.4-6.3.1

SuSE SLED 12 SP2
x86_64
liblouis9-2.6.4-6.3.1
python3-louis-2.6.4-6.3.1
liblouis-data-2.6.4-6.3.1
liblouis-debugsource-2.6.4-6.3.1
liblouis9-debuginfo-2.6.4-6.3.1

SuSE SLES 12 SP3
x86_64
liblouis9-2.6.4-6.3.1
liblouis9-debuginfo-2.6.4-6.3.1

liblouis-data-2.6.4-6.3.1
python-louis-2.6.4-6.3.1
python3-louis-2.6.4-6.3.1
liblouis-debugsource-2.6.4-6.3.1

145948 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2552-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7506

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2552-1

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-September/003257.html

SuSE SLED 12 SP3
x86_64
libspice-server1-debuginfo-0.12.8-3.9
spice-debugsource-0.12.8-3.9
libspice-server1-0.12.8-3.9

SuSE SLES 12 SP3
x86_64
libspice-server1-debuginfo-0.12.8-3.9
spice-debugsource-0.12.8-3.9
libspice-server1-0.12.8-3.9

145949 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2559-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14348

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2559-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00099.html

SuSE Linux 42.2
x86_64
libraw-tools-0.17.1-2.6.1
libraw-devel-0.17.1-2.6.1
libraw-debugsource-0.17.1-2.6.1
libraw15-0.17.1-2.6.1
libraw15-debuginfo-0.17.1-2.6.1

libraw-devel-static-0.17.1-2.6.1
libraw-tools-debuginfo-0.17.1-2.6.1

i586
libraw-tools-0.17.1-2.6.1
libraw-devel-0.17.1-2.6.1
libraw-debugsource-0.17.1-2.6.1
libraw15-0.17.1-2.6.1
libraw15-debuginfo-0.17.1-2.6.1
libraw-devel-static-0.17.1-2.6.1
libraw-tools-debuginfo-0.17.1-2.6.1

SuSE Linux 42.3
x86_64
libraw-tools-0.17.1-6.1
libraw-devel-static-0.17.1-6.1
libraw15-debuginfo-0.17.1-6.1
libraw-tools-debuginfo-0.17.1-6.1
libraw-debugsource-0.17.1-6.1
libraw15-0.17.1-6.1
libraw-devel-0.17.1-6.1

i586
libraw-tools-0.17.1-6.1
libraw-devel-static-0.17.1-6.1
libraw15-debuginfo-0.17.1-6.1
libraw-tools-debuginfo-0.17.1-6.1
libraw-debugsource-0.17.1-6.1
libraw15-0.17.1-6.1
libraw-devel-0.17.1-6.1

145950 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2569-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10371, CVE-2017-7592, CVE-2017-7593, CVE-2017-7594, CVE-2017-7595, CVE-2017-7596, CVE-2017-7597, CVE-2017-7598, CVE-2017-7599, CVE-2017-7600, CVE-2017-7601, CVE-2017-7602, CVE-2017-9403, CVE-2017-9404

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2569-1

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-September/003259.html

SuSE SLES 12 SP2
x86_64
libtiff5-4.0.8-44.3.1
libtiff5-debuginfo-32bit-4.0.8-44.3.1
libtiff5-debuginfo-4.0.8-44.3.1
tiff-debugsource-4.0.8-44.3.1
tiff-debuginfo-4.0.8-44.3.1
libtiff5-32bit-4.0.8-44.3.1
tiff-4.0.8-44.3.1

SuSE SLED 12 SP3
x86_64
libtiff5-32bit-4.0.8-44.3.1
libtiff5-debuginfo-4.0.8-44.3.1
tiff-debugsource-4.0.8-44.3.1
tiff-debuginfo-4.0.8-44.3.1
libtiff5-4.0.8-44.3.1
libtiff5-debuginfo-32bit-4.0.8-44.3.1

SuSE SLED 12 SP2
x86_64
libtiff5-32bit-4.0.8-44.3.1
libtiff5-debuginfo-4.0.8-44.3.1
tiff-debugsource-4.0.8-44.3.1
tiff-debuginfo-4.0.8-44.3.1
libtiff5-4.0.8-44.3.1
libtiff5-debuginfo-32bit-4.0.8-44.3.1

SuSE SLES 12 SP3
x86_64
libtiff5-4.0.8-44.3.1
libtiff5-debuginfo-32bit-4.0.8-44.3.1
libtiff5-debuginfo-4.0.8-44.3.1
tiff-debugsource-4.0.8-44.3.1
tiff-debuginfo-4.0.8-44.3.1
libtiff5-32bit-4.0.8-44.3.1
tiff-4.0.8-44.3.1

178503 - Gentoo Linux GLSA-201709-22 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10078, CVE-2017-10081, CVE-2017-10086, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10105, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10111, CVE-2017-10114, CVE-2017-10115, CVE-2017-10116, CVE-2017-10117, CVE-2017-10118, CVE-2017-10121, CVE-2017-10125, CVE-2017-10135, CVE-2017-10176, CVE-2017-10193, CVE-2017-10198, CVE-2017-10243

Description

The scan detected that the host is missing the following update:
GLSA-201709-22

Observation

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

https://security.gentoo.org/glsa/201709-22

Affected packages:
dev-java/oracle-jdk-bin < 1.8.0.141
dev-java/oracle-jre-bin < 1.8.0.141

182448 - FreeBSD ledger Multiple Vulnerabilities (d843a984-7f22-484f-ba81-483ddbe30dc3)

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

Risk Level: Medium

CVE: CVE-2017-2807, CVE-2017-2808

Description

The scan detected that the host is missing the following update:
ledger -- multiple vulnerabilities (d843a984-7f22-484f-ba81-483ddbe30dc3)

Observation

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

http://www.vuxml.org/freebsd/d843a984-7f22-484f-ba81-483ddbe30dc3.html

Affected packages:
ledger <= 3.1.1

182449 - FreeBSD libraw Buffer Overflow (d9f96741-47bd-4426-9aba-8736c0971b24)

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

Risk Level: Medium

CVE: CVE-2017-14348

Description

The scan detected that the host is missing the following update:
libraw -- buffer overflow (d9f96741-47bd-4426-9aba-8736c0971b24)

Observation

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

http://www.vuxml.org/freebsd/d9f96741-47bd-4426-9aba-8736c0971b24.html

Affected packages:
libraw < 0.18.4

182454 - FreeBSD sugarcrm Multiple Vulnerabilities (3b776502-f601-44e0-87cd-b63f1b9ae42a)

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

Risk Level: Medium

CVE: CVE-2017-14508, CVE-2017-14509, CVE-2017-14510

Description

The scan detected that the host is missing the following update:
sugarcrm -- multiple vulnerabilities (3b776502-f601-44e0-87cd-b63f1b9ae42a)

Observation

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

http://www.vuxml.org/freebsd/3b776502-f601-44e0-87cd-b63f1b9ae42a.html

Affected packages:
sugarcrm <= 6.5.26

182455 - FreeBSD aacplusenc Denial Of Service (7801b1e1-99b4-42ac-ab22-7646235e7c16)

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

Risk Level: Medium

CVE: CVE-2017-14181

Description

The scan detected that the host is missing the following update:
aacplusenc -- denial of service (7801b1e1-99b4-42ac-ab22-7646235e7c16)

Observation

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

http://www.vuxml.org/freebsd/7801b1e1-99b4-42ac-ab22-7646235e7c16.html

Affected packages:
aacplusenc <= 0.17.5_2

192662 - Fedora Linux 26 FEDORA-2017-982bfabc4e Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-982bfabc4e

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/2017/9/?count=200&page=1

Fedora Core 26

libmspack-0.6-0.1.alpha.fc26

192670 - Fedora Linux 25 FEDORA-2017-aa7a8871b7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13735, CVE-2017-14348

Description

The scan detected that the host is missing the following update:
FEDORA-2017-aa7a8871b7

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/2017/9/?count=200&page=1

Fedora Core 25

mingw-LibRaw-0.17.2-3.fc25

22448 - (K54225343) F5 BIG-IP Libxml2 Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-3627, CVE-2016-3705

Description

Multiple vulnerabilities are present in some versions of F5 BIG-IP systems.

Observation

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

Multiple vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in various functions in parser.c and tree.c in libxml2. Successful exploitation could allow an attacker to cause a denial of service condition.

22476 - (VMSA-2017-0015.2) VMware ESXi Out-of-bounds Write Vulnerability (CVE-2017-4924)

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

Risk Level: Medium

CVE: CVE-2017-4924

Description

A vulnerability is present in some versions of VMware ESXi.

Observation

VMware ESXi is a popular virtualization platform.

A vulnerability is present in some versions of VMware ESXi. The flaw lies in SVGA device. Successful exploitation could allow an attacker to execute arbitrary code on the host.

22477 - (VMSA-2017-0015.2) VMware ESXi Out-of-bounds Write Vulnerability (CVE-2017-4924)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4924

Description

A vulnerability is present in some versions of VMware ESXi.

Observation

VMware ESXi is a popular virtualization platform.

A vulnerability is present in some versions of VMware ESXi. The flaw lies in SVGA device. Successful exploitation could allow an attacker to execute arbitrary code on the host.

22478 - (VMSA-2017-0015.2) VMware ESXi Guest RPC NULL Pointer Dereference Vulnerability (CVE-2017-4925)

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

Risk Level: Medium

CVE: CVE-2017-4925

Description

A denial of service vulnerability is present in some versions of VMware ESXi.

Observation

VMware ESXi is a popular virtualization platform.

A denial of service vulnerability is present in some versions of VMware ESXi. The flaw lies in handling of guest RPC requests. Successful exploitation could allow an attacker to cause a denial of service condition.

22479 - (VMSA-2017-0015.2) VMware ESXi Guest RPC NULL Pointer Dereference Vulnerability (CVE-2017-4925)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4925

Description

A denial of service vulnerability is present in some versions of VMware ESXi.

Observation

VMware ESXi is a popular virtualization platform.

A denial of service vulnerability is present in some versions of VMware ESXi. The flaw lies in handling of guest RPC requests. Successful exploitation could allow an attacker to cause a denial of service condition.

22488 - Apache Tomcat Multiple Vulnerabilities Prior To 7.0.81

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12616

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information, or execute arbitrary code.

22493 - Apache HTTP Server Vulnerability Prior To 2.2.35

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

Risk Level: Medium

CVE: CVE-2017-9798

Description

A vulnerability is present in some versions of Apache HTTP Server.

Observation

Apache HTTP Server is an open source web server.

A vulnerability is present in some versions of Apache HTTP Server. The flaw lies in misconfiguration of httpd.conf. Successful exploitation could allow an attacker to obtain sensitive information.

163461 - Oracle Enterprise Linux ELSA-2017-2791 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ELSA-2017-2791

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007222.html

OEL6
x86_64
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

i386
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

163463 - Oracle Enterprise Linux ELSA-2017-2790 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ELSA-2017-2790

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007220.html

OEL7
x86_64
samba-test-4.6.2-11.el7_4
samba-winbind-clients-4.6.2-11.el7_4
samba-client-libs-4.6.2-11.el7_4
samba-python-4.6.2-11.el7_4
samba-winbind-modules-4.6.2-11.el7_4
samba-common-libs-4.6.2-11.el7_4
samba-winbind-4.6.2-11.el7_4
libwbclient-4.6.2-11.el7_4
samba-libs-4.6.2-11.el7_4
libsmbclient-4.6.2-11.el7_4
samba-vfs-glusterfs-4.6.2-11.el7_4
libsmbclient-devel-4.6.2-11.el7_4
samba-devel-4.6.2-11.el7_4
ctdb-4.6.2-11.el7_4
samba-client-4.6.2-11.el7_4
libwbclient-devel-4.6.2-11.el7_4
samba-dc-libs-4.6.2-11.el7_4
samba-dc-4.6.2-11.el7_4
samba-winbind-krb5-locator-4.6.2-11.el7_4
samba-test-libs-4.6.2-11.el7_4
ctdb-tests-4.6.2-11.el7_4
samba-common-tools-4.6.2-11.el7_4
samba-krb5-printing-4.6.2-11.el7_4
samba-4.6.2-11.el7_4
samba-pidl-4.6.2-11.el7_4
samba-common-4.6.2-11.el7_4

163464 - Oracle Enterprise Linux ELSA-2017-2789 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12150, CVE-2017-12163, CVE-2017-2619

Description

The scan detected that the host is missing the following update:
ELSA-2017-2789

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007221.html

OEL6
x86_64
samba-doc-3.6.23-45.0.1.el6_9

samba-common-3.6.23-45.0.1.el6_9
libsmbclient-devel-3.6.23-45.0.1.el6_9
samba-3.6.23-45.0.1.el6_9
samba-client-3.6.23-45.0.1.el6_9
samba-winbind-clients-3.6.23-45.0.1.el6_9
samba-winbind-3.6.23-45.0.1.el6_9
samba-glusterfs-3.6.23-45.0.1.el6_9
samba-winbind-devel-3.6.23-45.0.1.el6_9
samba-winbind-krb5-locator-3.6.23-45.0.1.el6_9
samba-domainjoin-gui-3.6.23-45.0.1.el6_9
libsmbclient-3.6.23-45.0.1.el6_9
samba-swat-3.6.23-45.0.1.el6_9

i386
samba-common-3.6.23-45.0.1.el6_9
samba-client-3.6.23-45.0.1.el6_9
samba-doc-3.6.23-45.0.1.el6_9
samba-winbind-krb5-locator-3.6.23-45.0.1.el6_9
libsmbclient-devel-3.6.23-45.0.1.el6_9
samba-winbind-3.6.23-45.0.1.el6_9
samba-3.6.23-45.0.1.el6_9
libsmbclient-3.6.23-45.0.1.el6_9
samba-domainjoin-gui-3.6.23-45.0.1.el6_9
samba-winbind-devel-3.6.23-45.0.1.el6_9
samba-swat-3.6.23-45.0.1.el6_9
samba-winbind-clients-3.6.23-45.0.1.el6_9

175265 - Scientific Linux Security ERRATA Moderate: samba on SL6.x i386/x86_64 (1709-3115)

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

Risk Level: Medium

CVE: CVE-2017-12150, CVE-2017-12163, CVE-2017-2619

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: samba on SL6.x i386/x86_64 (1709-3115)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1709&L=scientific-linux-errata&F=&S=&P=3115

SL6
x86_64
samba-debuginfo-3.6.23-45.el6_9
samba-3.6.23-45.el6_9
samba-glusterfs-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9
libsmbclient-devel-3.6.23-45.el6_9
samba-swat-3.6.23-45.el6_9
samba-doc-3.6.23-45.el6_9
samba-winbind-devel-3.6.23-45.el6_9
samba-domainjoin-gui-3.6.23-45.el6_9
samba-winbind-krb5-locator-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9

samba-winbind-3.6.23-45.el6_9

i386
samba-3.6.23-45.el6_9
samba-debuginfo-3.6.23-45.el6_9
samba-winbind-devel-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9
libsmbclient-devel-3.6.23-45.el6_9
samba-swat-3.6.23-45.el6_9
samba-doc-3.6.23-45.el6_9
samba-domainjoin-gui-3.6.23-45.el6_9
samba-winbind-krb5-locator-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9

178502 - Gentoo Linux GLSA-201709-18 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-18

Observation

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

https://security.gentoo.org/glsa/201709-18

Affected packages:
dev-vcs/mercurial < 4.3

178504 - Gentoo Linux GLSA-201709-15 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-15

Observation

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

https://security.gentoo.org/glsa/201709-15

Affected packages:
www-client/chromium < 61.0.3163.79

178506 - Gentoo Linux GLSA-201709-25 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-201709-25

Observation

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

https://security.gentoo.org/glsa/201709-25

Affected packages:
www-client/chromium < 61.0.3163.100

178508 - Gentoo Linux GLSA-201709-26 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-201709-26

Observation

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

https://security.gentoo.org/glsa/201709-26

Affected packages:
net-libs/libsoup < 2.56.1

178510 - Gentoo Linux GLSA-201709-17 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-201709-17

Observation

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

https://security.gentoo.org/glsa/201709-17

Affected packages:
dev-vcs/cvs < 1.12.12-r12

178511 - Gentoo Linux GLSA-201709-23 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-201709-23

Observation

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

https://security.gentoo.org/glsa/201709-23

Affected packages:
net-analyzer/tcpdump < 4.9.2

178512 - Gentoo Linux GLSA-201709-19 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-19

Observation

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

https://security.gentoo.org/glsa/201709-19

Affected packages:
mail-mta/exim < 4.89-r1

182446 - FreeBSD ansible Information Disclosure Flaw (478d4102-2319-4026-b3b2-a57c48f159ac)

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

Risk Level: Medium

CVE: CVE-2017-7473

Description

The scan detected that the host is missing the following update:
ansible -- information disclosure flaw (478d4102-2319-4026-b3b2-a57c48f159ac)

Observation

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

For more information see:

http://www.vuxml.org/freebsd/478d4102-2319-4026-b3b2-a57c48f159ac.html

Affected packages:
ansible <= 2.2.3

182450 - FreeBSD libgd Denial Of Servica Via Double Free (a60a2e95-acba-4b11-bc32-ffb47364e07d)

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

Risk Level: Medium

CVE: CVE-2017-6362

Description

The scan detected that the host is missing the following update:
libgd -- Denial of servica via double free (a60a2e95-acba-4b11-bc32-ffb47364e07d)

Observation

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

http://www.vuxml.org/freebsd/a60a2e95-acba-4b11-bc32-ffb47364e07d.html

Affected packages:
libgd < 2.2.5

182456 - FreeBSD libbson Denial Of Service (10214bda-0902-4e3b-a2f9-9a68ef206a73)

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

Risk Level: Medium

CVE: CVE-2017-14227

Description

The scan detected that the host is missing the following update:
libbson -- Denial of Service (10214bda-0902-4e3b-a2f9-9a68ef206a73)

Observation

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

http://www.vuxml.org/freebsd/10214bda-0902-4e3b-a2f9-9a68ef206a73.html

Affected packages:
libbson < 1.8.1

192661 - Fedora Linux 26 FEDORA-2017-b9f07dfaca Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11424

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b9f07dfaca

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/2017/9/?count=200&page=1

Fedora Core 26

python-jwt-1.5.3-1.fc26

192667 - Fedora Linux 25 FEDORA-2017-172410ec92 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10683, CVE-2017-11126, CVE-2017-12797, CVE-2017-9545

Description

The scan detected that the host is missing the following update:
FEDORA-2017-172410ec92

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/2017/9/?count=200&page=1

Fedora Core 25

mpg123-1.25.6-1.fc25

192674 - Fedora Linux 26 FEDORA-2017-a4cf96bcca Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14227

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a4cf96bcca

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/2017/9/?count=200&page=1

Fedora Core 26

libbson-1.6.3-2.fc26

192676 - Fedora Linux 25 FEDORA-2017-7edc2ea787 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14227

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7edc2ea787

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/2017/9/?count=200&page=1

Fedora Core 25

libbson-1.3.5-4.fc25

22463 - IBM DB2 Unauthorized Command Vulnerability (swg22007186)

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

Risk Level: Medium

CVE: CVE-2017-1520

Description

A vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw lies in the CLIENT authentication type. Successful exploitation could allow an attacker without proper privileges to activate database.

22473 - (VMSA-2017-0015) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4924, CVE-2017-4925

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components. Successful exploitation could allow an attacker to cause denial of service condition or execute an arbitrary code on the host.

22474 - (VMSA-2017-0015) VMware Workstation Player Multiple Vulnerabilities II

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4924, CVE-2017-4925

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components. Successful exploitation could allow an attacker to cause denial of service condition or execute an arbitrary code on the host.

22502 - (VMSA-2017-0015) VMware Workstation Player Multiple Vulnerabilities III

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

Risk Level: Medium

CVE: CVE-2017-4924, CVE-2017-4925

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components. Successful exploitation could allow an attacker to cause denial of service condition or execute an arbitrary code on the host.

22503 - (VMSA-2017-0015) VMware Workstation Player Multiple Vulnerabilities IV

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4924, CVE-2017-4925

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components. Successful exploitation could allow an attacker to cause denial of service condition or execute an arbitrary code on the host.

178513 - Gentoo Linux GLSA-201709-27 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9403

Description

The scan detected that the host is missing the following update:
GLSA-201709-27

Observation

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

For more information see:

https://security.gentoo.org/glsa/201709-27

Affected packages:
media-libs/tiff < 4.0.8

182453 - FreeBSD libzip Denial Of Service (b2952517-07e5-4d19-8850-21c5b7e0623f)

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

Risk Level: Medium

CVE: CVE-2017-14107

Description

The scan detected that the host is missing the following update:
libzip -- denial of service (b2952517-07e5-4d19-8850-21c5b7e0623f)

Observation

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

http://www.vuxml.org/freebsd/b2952517-07e5-4d19-8850-21c5b7e0623f.html

Affected packages:
libzip < 1.3.0

182458 - FreeBSD php-gd and gd Buffer Over-read Into Uninitialized Memory (5033e2fc-98ec-4ef5-8e0b-87cfbbc73081)

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

Risk Level: Medium

CVE: CVE-2017-7890

Description

The scan detected that the host is missing the following update:
php-gd and gd -- Buffer over-read into uninitialized memory (5033e2fc-98ec-4ef5-8e0b-87cfbbc73081)

Observation

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

http://www.vuxml.org/freebsd/5033e2fc-98ec-4ef5-8e0b-87cfbbc73081.html

Affected packages:
libgd < 2.2.5
php70-gd < 7.0.21
php71-gd < 7.1.7

22486 - (VMSA-2017-0015) VMware vCenter Cross-Site Scripting Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2017-4926

Description

A vulnerability is present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

A vulnerability is present in some versions of VMware vCenter Server. The flaw lies in the H5 Client. Successful exploitation could allow an attacker to inject malicious java-scripts.

22491 - (VMSA-2017-0015) VMware vCenter Cross-Site Scripting Vulnerability

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

Risk Level: Low

CVE: CVE-2017-4926

Description

A vulnerability is present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

A vulnerability is present in some versions of VMware vCenter Server. The flaw lies in the H5 Client. Successful exploitation could allow an attacker to inject malicious java-scripts.

130892 - Debian Linux 8.0, 9.0 DSA-3983-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
DSA-3983-1

Observation

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

http://www.debian.org/security/2017/dsa-3983

Debian 8.0
all
samba_2:4.2.14+dfsg-0+deb8u8

Debian 9.0
all
samba_2:4.5.8+dfsg-2+deb9u2

182451 - FreeBSD weechat Crash In Logger Plugin (b63421b6-a1e0-11e7-ac58-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-14727

Description

The scan detected that the host is missing the following update:
weechat -- crash in logger plugin (b63421b6-a1e0-11e7-ac58-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/b63421b6-a1e0-11e7-ac58-b499baebfeaf.html

Affected packages:
weechat < 1.9.1

182452 - FreeBSD perl Multiple Vulnerabilities (d9e82328-a129-11e7-987e-4f174049b30a)

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

Risk Level: Low

CVE: CVE-2017-12814, CVE-2017-12837, CVE-2017-12883

Description

The scan detected that the host is missing the following update:
perl -- multiple vulnerabilities (d9e82328-a129-11e7-987e-4f174049b30a)

Observation

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

http://www.vuxml.org/freebsd/d9e82328-a129-11e7-987e-4f174049b30a.html

Affected packages:
5.24.0 <= perl5 < 5.24.3
5.26.0 <= perl5 < 5.26.1

182459 - FreeBSD chromium Multiple Vulnerabilities (917e5519-9fdd-11e7-8b58-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-5121, CVE-2017-5122

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (917e5519-9fdd-11e7-8b58-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/917e5519-9fdd-11e7-8b58-e8e0b747a45a.html

Affected packages:
chromium < 61.0.3163.100

192665 - Fedora Linux 25 FEDORA-2017-f27641a807 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-f27641a807

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/2017/9/?count=200&page=2

Fedora Core 25

drupal7-views-3.18-1.fc25

192666 - Fedora Linux 26 FEDORA-2017-63f99b3977 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-2017-63f99b3977

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/2017/9/?count=200&page=2

Fedora Core 26

drupal7-views-3.18-1.fc26

192668 - Fedora Linux 26 FEDORA-2017-a52f252521 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a52f252521

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/2017/9/?count=200&page=2

Fedora Core 26

httpd-2.4.27-3.fc26

192669 - Fedora Linux 26 FEDORA-2017-5a0a31c04e Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5a0a31c04e

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/2017/9/?count=200&page=1

Fedora Core 26

samba-4.6.8-0.fc26

192671 - Fedora Linux 26 FEDORA-2017-11afc3cde9 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-2017-11afc3cde9

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/2017/9/?count=200&page=1

Fedora Core 26

pkgconf-1.3.9-1.fc26

192672 - Fedora Linux 27 FEDORA-2017-23dba9fb5d 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-2017-23dba9fb5d

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/2017/9/?count=200&page=1

Fedora Core 27

kernel-4.13.3-300.fc27

192673 - Fedora Linux 26 FEDORA-2017-ebc4d197b2 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-ebc4d197b2

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/2017/9/?count=200&page=2

Fedora Core 26

gnome-shell-3.24.3-2.fc26

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.

132400 - Oracle VM OVMSA-2017-0151 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Update Details

Risk is updated

141703 - Red Hat Enterprise Linux RHSA-2017-2681 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Update Details

Risk is updated

141708 - Red Hat Enterprise Linux RHSA-2017-2682 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

141709 - Red Hat Enterprise Linux RHSA-2017-2707 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

141711 - Red Hat Enterprise Linux RHSA-2017-2683 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

141713 - Red Hat Enterprise Linux RHSA-2017-2706 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

141714 - Red Hat Enterprise Linux RHSA-2017-2679 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

141719 - Red Hat Enterprise Linux RHSA-2017-2731 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details

Risk is updated

145930 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2523-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

145931 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2521-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

145934 - SuSE SLES 11 SP4 SUSE-SU-2017:2548-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

160296 - CentOS 6 CESA-2017-2681 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

163453 - Oracle Enterprise Linux ELSA-2017-2681 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251

Update Details
Risk is updated

163455 - Oracle Enterprise Linux ELSA-2017-2679 Update Is Not Installed

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

CVE: CVE-2017-1000251

Update Details

Risk is updated

163458 - Oracle Enterprise Linux ELSA-2017-3620 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Update Details

Risk is updated

175258 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1709-1083)

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

Risk Level: High

CVE: CVE-2017-1000251

Update Details

Risk is updated

175259 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1709-756)

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

Risk Level: High

CVE: CVE-2017-1000251

Update Details

Risk is updated

185887 - Ubuntu Linux 12.04 USN-3423-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Update Details

Risk is updated

192638 - Fedora Linux 26 FEDORA-2017-7369ea045c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-12153, CVE-2017-12154

Update Details

Risk is updated

192657 - Fedora Linux 25 FEDORA-2017-e07d7fb18e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000251, CVE-2017-12153, CVE-2017-12154

Update Details
Risk is updated

22462 - (CTX227185) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2017-14316, CVE-2017-14318, CVE-2017-14319

Update Details
Risk is updated

130870 - Debian Linux 8.0, 9.0 DSA-3964-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14099, CVE-2017-14100

Update Details
Risk is updated

181572 - FreeBSD libpgf Use After Free (9a71953a-474a-11e5-adde-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-6673

Update Details
Risk is updated

182435 - FreeBSD asterisk Unauthorized Data Disclosure And Shell Access Command Injection In App_minivm (c599f95c-8ee5-11e7-8be8-001999f8

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14099, CVE-2017-14100

Update Details
Risk is updated

192629 - Fedora Linux 26 FEDORA-2017-10c74147f9 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-11462

Update Details

Risk is updated

192651 - Fedora Linux 26 FEDORA-2017-e399a9008c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14316, CVE-2017-14317, CVE-2017-14318, CVE-2017-14319

Update Details

Risk is updated

170794 - Amazon Linux AMI ALAS-2017-819 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8714

Update Details

Risk is updated

182440 - FreeBSD cyrus-imapd Broken "other Users" Behaviour (f9f76a50-9642-11e7-ab09-080027b00c2e)

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

Risk Level: Medium

CVE: CVE-2017-14230

Update Details

Risk is updated

192642 - Fedora Linux 26 FEDORA-2017-e4609f71f6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14230

Update Details

Risk is updated

181653 - FreeBSD Joomla! Core - Open Redirect Vulnerability (deaba148-7ac5-11e5-b35a-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-5608

Update Details

Risk is updated

182444 - FreeBSD asterisk RTP/RTCP Information Leak (c2ea3b31-9d75-11e7-bb13-001999f8d30b)

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

Risk Level: Medium

CVE: CVE-2017-14099

Update Details

Risk is updated

192639 - Fedora Linux 26 FEDORA-2017-63ff51c0dc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14226

Update Details

Risk is updated

22358 - AzeoTech DAQFactory Multiple Vulnerabilities Prior To 17.1

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

Risk Level: Medium

CVE: CVE-2017-12699, CVE-2017-5147

Update Details

Risk is updated

181453 - FreeBSD devel/ipython Remote Execution (a4460ac7-192c-11e5-9c01-bcaec55be5e5)

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

Risk Level: Medium

CVE: CVE-2015-4706, CVE-2015-4707

Update Details

Risk is updated

141710 - Red Hat Enterprise Linux RHSA-2017-2685 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000250

Update Details

Risk is updated

163454 - Oracle Enterprise Linux ELSA-2017-2685 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000250

Update Details

Risk is updated

175257 - Scientific Linux Security ERRATA Moderate: bluez on SL6.x, SL7.x i386/x86_64 (1709-422)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Low
CVE: CVE-2017-1000250

Update Details
Risk is updated

182445 - FreeBSD rubygem-geminabox XSS & CSRF Vulnerabilities (2bffdf2f-9d45-11e7-a25c-471bafc3262f)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2017-14506, CVE-2017-14683

Update Details
CVE is updated

14479 - HP-UX Obsolete Version Detection

Category: SSH Module -> NonIntrusive -> EOL and Obsolete Software
Risk Level: Informational
CVE: CVE-MAP-NOMATCH

Update Details
Observation is updated FASLScript is updated

14482 - Apache HTTP Server Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software
Risk Level: Informational
CVE: CVE-MAP-NOMATCH

Update Details
FASLScript is updated

70029 - db2.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category
Risk Level: Informational
CVE: CVE-MAP-NOMATCH

Update Details
FASLScript 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

DELETED CHECKS

21191 - Microsoft Windows SMBv2/SMBv3 Client Denial Of Service Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

ADDITIONAL NOTES

- **21191** - is replaced by FID 21418

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.