2017-NOV-02
FSL version 7.5.972

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

132409 - Oracle VM OVMSA-2017-0164 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-11176, CVE-2017-7542

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0164

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/000794.html

OVM3.3
x86_64
kernel-uek-3.8.13-118.19.10.el6uek
kernel-uek-firmware-3.8.13-118.19.10.el6uek

146025 - SuSE SLES 11 SP4 SUSE-SU-2017:2907-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-2699, CVE-2010-0425, CVE-2012-0021, CVE-2014-0118, CVE-2017-3167, CVE-2017-3169, CVE-2017-7668, CVE-2017-7679, CVE-2017-9798

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2907-1

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/003365.html

SuSE SLES 11 SP4
i586
apache2-doc-2.2.34-70.12.1
apache2-prefork-2.2.34-70.12.1
apache2-worker-2.2.34-70.12.1
apache2-example-pages-2.2.34-70.12.1

apache2-utils-2.2.34-70.12.1
apache2-2.2.34-70.12.1

x86_64
apache2-doc-2.2.34-70.12.1
apache2-prefork-2.2.34-70.12.1
apache2-worker-2.2.34-70.12.1
apache2-example-pages-2.2.34-70.12.1
apache2-utils-2.2.34-70.12.1
apache2-2.2.34-70.12.1

163486 - Oracle Enterprise Linux ELSA-2017-3632 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-11176, CVE-2017-7542

Description

The scan detected that the host is missing the following update:
ELSA-2017-3632

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/007304.html
http://oss.oracle.com/pipermail/el-errata/2017-October/007305.html

OEL7
x86_64
kernel-uek-devel-3.8.13-118.19.10.el7uek
kernel-uek-3.8.13-118.19.10.el7uek
kernel-uek-doc-3.8.13-118.19.10.el7uek
kernel-uek-firmware-3.8.13-118.19.10.el7uek
dtrace-modules-3.8.13-118.19.10.el7uek-0.4.5-3.el7
kernel-uek-debug-devel-3.8.13-118.19.10.el7uek
kernel-uek-debug-3.8.13-118.19.10.el7uek

OEL6
x86_64
kernel-uek-firmware-3.8.13-118.19.10.el6uek
kernel-uek-devel-3.8.13-118.19.10.el6uek
kernel-uek-debug-3.8.13-118.19.10.el6uek
kernel-uek-doc-3.8.13-118.19.10.el6uek
kernel-uek-3.8.13-118.19.10.el6uek
dtrace-modules-3.8.13-118.19.10.el6uek-0.4.5-3.el6
kernel-uek-debug-devel-3.8.13-118.19.10.el6uek

163489 - Oracle Enterprise Linux ELSA-2017-3633 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-11176, CVE-2017-7542

Description

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

ELSA-2017-3633

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/007306.html

OEL6
x86_64
kernel-uek-debug-2.6.39-400.297.11.el6uek
kernel-uek-firmware-2.6.39-400.297.11.el6uek
kernel-uek-devel-2.6.39-400.297.11.el6uek
kernel-uek-doc-2.6.39-400.297.11.el6uek
kernel-uek-debug-devel-2.6.39-400.297.11.el6uek
kernel-uek-2.6.39-400.297.11.el6uek

i386
kernel-uek-2.6.39-400.297.11.el6uek
kernel-uek-firmware-2.6.39-400.297.11.el6uek
kernel-uek-devel-2.6.39-400.297.11.el6uek
kernel-uek-doc-2.6.39-400.297.11.el6uek
kernel-uek-debug-devel-2.6.39-400.297.11.el6uek
kernel-uek-debug-2.6.39-400.297.11.el6uek

185941 - Ubuntu Linux 17.04 USN-3468-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000252, CVE-2017-10663, CVE-2017-10911, CVE-2017-11176, CVE-2017-14340

Description

The scan detected that the host is missing the following update:
USN-3468-1

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/004119.html

Ubuntu 17.04

linux-image-raspi2_4.10.0.1020.21
linux-image-generic-lpae_4.10.0.38.38
linux-image-lowlatency_4.10.0.38.38
linux-image-4.10.0-38-lowlatency_4.10.0-38.42
linux-image-4.10.0-38-generic_4.10.0-38.42
linux-image-4.10.0-38-generic-lpae_4.10.0-38.42
linux-image-4.10.0-1020-raspi2_4.10.0-1020.23
linux-image-generic_4.10.0.38.38

185942 - Ubuntu Linux 12.04 USN-3470-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8632, CVE-2017-10661, CVE-2017-10662, CVE-2017-10663, CVE-2017-10911, CVE-2017-11176, CVE-2017-14340

Description

The scan detected that the host is missing the following update:
USN-3470-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004126.html

Ubuntu 12.04

linux-image-generic-lpae-lts-trusty_3.13.0.135.125
linux-image-generic-lts-trusty_3.13.0.135.125
linux-image-3.13.0-135-generic_3.13.0-135.184~precise1
linux-image-3.13.0-135-generic-lpae_3.13.0-135.184~precise1

185946 - Ubuntu Linux 16.04 USN-3468-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000252, CVE-2017-10663, CVE-2017-10911, CVE-2017-11176, CVE-2017-14340

Description

The scan detected that the host is missing the following update:
USN-3468-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004120.html

Ubuntu 16.04

linux-image-generic-hwe-16.04_4.10.0.38.40
linux-image-lowlatency-hwe-16.04_4.10.0.38.40
linux-image-generic-lpae-hwe-16.04_4.10.0.38.40
linux-image-4.10.0-38-lowlatency_4.10.0-38.42~16.04.1
linux-image-4.10.0-38-generic_4.10.0-38.42~16.04.1
linux-image-4.10.0-38-generic-lpae_4.10.0-38.42~16.04.1

185948 - Ubuntu Linux 14.04 USN-3470-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8632, CVE-2017-10661, CVE-2017-10662, CVE-2017-10663, CVE-2017-10911, CVE-2017-11176, CVE-2017-14340

Description

The scan detected that the host is missing the following update:
USN-3470-1

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/004124.html

Ubuntu 14.04

linux-image-3.13.0-135-powerpc-smp_3.13.0-135.184
linux-image-3.13.0-135-powerpc-e500mc_3.13.0-135.184
linux-image-3.13.0-135-powerpc-e500_3.13.0-135.184
linux-image-3.13.0-135-powerpc64-emb_3.13.0-135.184
linux-image-powerpc64-emb_3.13.0.135.144
linux-image-3.13.0-135-generic-lpae_3.13.0-135.184
linux-image-3.13.0-135-generic_3.13.0-135.184
linux-image-3.13.0-135-lowlatency_3.13.0-135.184
linux-image-powerpc64-smp_3.13.0.135.144
linux-image-3.13.0-135-powerpc64-smp_3.13.0-135.184
linux-image-generic-lpae_3.13.0.135.144
linux-image-powerpc-e500_3.13.0.135.144
linux-image-powerpc-e500mc_3.13.0.135.144
linux-image-lowlatency_3.13.0.135.144
linux-image-generic_3.13.0.135.144
linux-image-powerpc-smp_3.13.0.135.144

185950 - Ubuntu Linux 16.04 USN-3468-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000252, CVE-2017-10663, CVE-2017-10911, CVE-2017-11176, CVE-2017-14340

Description

The scan detected that the host is missing the following update:
USN-3468-3

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004121.html

Ubuntu 16.04

linux-image-4.10.0-1008-gcp_4.10.0-1008.8
linux-image-gcp_4.10.0.1008.10

22487 - iniNet Solutions GmbH SCADA Webserver Improper Authentication Vulnerability

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

Risk Level: High

CVE: CVE-2017-13995

Description

A vulnerability is present in some versions of iniNet Solutions GmbH SCADA Web Server.

Observation

iniNet Solutions GmbH SCADA Web Server is a software management platform.

A vulnerability is present in some versions of iniNet Solutions GmbH SCADA Web Server. The flaw lies in the authentication component. Successful exploitation could allow a remote attacker to bypass security restrictions and access sensitive information.

22626 - iniNet Solutions GmbH SCADA Webserver Improper Authentication Vulnerability

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

Risk Level: High

CVE: CVE-2017-13995

Description

A vulnerability is present in some versions of iniNet Solutions GmbH SCADA Web Server.

Observation

iniNet Solutions GmbH SCADA Web Server is a software management platform.

A vulnerability is present in some versions of iniNet Solutions GmbH SCADA Web Server. The flaw lies in the authentication component. Successful exploitation could allow a remote attacker to bypass security restrictions and access sensitive information.

22634 - Google Chrome Multiple Vulnerabilities Prior To 62.0.3202.62

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

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

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct spoofing attacks, cause buffer overflow, or execute arbitrary code affecting integrity, confidentiality or availability..

22635 - Google Chrome Multiple Vulnerabilities Prior To 62.0.3202.62

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

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

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct spoofing attacks, cause buffer overflow, or execute arbitrary code affecting integrity, confidentiality or availability..

22648 - (K02692210) F5 BIG-IP BIG-IP Virtual Server With HTTP Explicit Proxy And/Or SOCKS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6157

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw occurs when HTTP Explicit Proxy functionality and/or SOCKS profiles are configured on virtual servers. Successful exploitation could allow an attacker to execute arbitrary code, retrieve sensitive data or make unauthorized modifications on the target system.

170891 - Amazon Linux AMI ALAS-2017-915 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0898, CVE-2017-0899, CVE-2017-0900, CVE-2017-0901, CVE-2017-0902, CVE-2017-10784, CVE-2017-14033, CVE-2017-14064

Description

The scan detected that the host is missing the following update:
ALAS-2017-915

Observation

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

https://alas.aws.amazon.com/ALAS-2017-915.html

Amazon Linux AMI
i686
rubygem24-io-console-0.4.6-1.30.4.amzn1
ruby24-devel-2.4.2-1.30.4.amzn1
ruby24-libs-2.4.2-1.30.4.amzn1
rubygem24-xmlrpc-0.2.1-1.30.4.amzn1
ruby24-debuginfo-2.4.2-1.30.4.amzn1
rubygem24-json-2.0.4-1.30.4.amzn1
ruby24-2.4.2-1.30.4.amzn1
rubygem24-bigdecimal-1.3.0-1.30.4.amzn1
rubygem24-psych-2.2.2-1.30.4.amzn1

noarch
rubygems24-devel-2.6.13-1.30.4.amzn1
ruby24-doc-2.4.2-1.30.4.amzn1
ruby24-irb-2.4.2-1.30.4.amzn1
rubygem24-did_you_mean-1.1.0-1.30.4.amzn1
rubygems24-2.6.13-1.30.4.amzn1

x86_64
rubygem24-io-console-0.4.6-1.30.4.amzn1
ruby24-devel-2.4.2-1.30.4.amzn1
rubygem24-psych-2.2.2-1.30.4.amzn1
rubygem24-xmlrpc-0.2.1-1.30.4.amzn1
ruby24-2.4.2-1.30.4.amzn1
ruby24-debuginfo-2.4.2-1.30.4.amzn1
rubygem24-json-2.0.4-1.30.4.amzn1
rubygem24-bigdecimal-1.3.0-1.30.4.amzn1
ruby24-libs-2.4.2-1.30.4.amzn1

170892 - Amazon Linux AMI ALAS-2017-914 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-12154, CVE-2017-12192, CVE-2017-14340, CVE-2017-14991, CVE-2017-15274

Description

The scan detected that the host is missing the following update:
ALAS-2017-914

Observation

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

https://alas.aws.amazon.com/ALAS-2017-914.html

Amazon Linux AMI
i686
kernel-debuginfo-common-i686-4.9.58-18.51.amzn1
perf-4.9.58-18.51.amzn1
kernel-tools-devel-4.9.58-18.51.amzn1
kernel-4.9.58-18.51.amzn1
kernel-debuginfo-4.9.58-18.51.amzn1
perf-debuginfo-4.9.58-18.51.amzn1
kernel-headers-4.9.58-18.51.amzn1
kernel-devel-4.9.58-18.51.amzn1
kernel-tools-debuginfo-4.9.58-18.51.amzn1
kernel-tools-4.9.58-18.51.amzn1

noarch
kernel-doc-4.9.58-18.51.amzn1

x86_64
kernel-tools-4.9.58-18.51.amzn1
perf-4.9.58-18.51.amzn1
kernel-tools-devel-4.9.58-18.51.amzn1
kernel-devel-4.9.58-18.51.amzn1
kernel-debuginfo-4.9.58-18.51.amzn1
kernel-debuginfo-common-x86_64-4.9.58-18.51.amzn1
perf-debuginfo-4.9.58-18.51.amzn1
kernel-headers-4.9.58-18.51.amzn1
kernel-tools-debuginfo-4.9.58-18.51.amzn1
kernel-4.9.58-18.51.amzn1

22623 - (JSA10807) Juniper Junos OS "Dirty COW" Local Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5195

Description

A vulnerability is present in some versions of Juniper Junos OS.

Observation

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

A vulnerability is present in some versions of Juniper Junos OS. The flaw is due to incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping. Successful exploitation could allow an attacker to escalate privileges.

22627 - (CTX228867) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

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

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in multiple components. Successful exploitation could allow a malicious administrator of a guest VM to compromise the host.

22650 - Apache OpenOffice Multiple Vulnerabilities Prior To 4.1.4

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

Risk Level: High

CVE: CVE-2017-12607, CVE-2017-12608, CVE-2017-3157, CVE-2017-9806

Description

Multiple vulnerabilities are present in some versions of Apache OpenOffice.

Observation

Apache OpenOffice is an open source office software suite.

Multiple vulnerabilities are present in some versions of Apache OpenOffice. The flaws lie in several components. Successful exploitation could allow an attacker to cause a remote code execution, a denial-of-service or to obtain sensitive information from the victim's system.

22652 - Oracle MySQL Enterprise Monitor Critical Patch Update October 2017

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

Risk Level: High

CVE: CVE-2017-10424, CVE-2017-5664

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL Enterprise Monitor.

Observation

Oracle MySQL Enterprise Monitor enables monitoring of multiple Oracle MySQL instances.

Multiple vulnerabilities are present in some versions of Oracle MySQL Enterprise Monitor. The flaws lie in multiple components. Successful exploitation could allow an attacker to affect confidentiality, integrity, and availability.

88894 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-300-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1283

Description

The scan detected that the host is missing the following update:
SSA:2017-300-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.428808

Slackware 14.0
x86_64
php-5.6.32-x86_64-1

Slackware 14.2
x86_64
php-5.6.32-x86_64-1

i586
php-5.6.32-i586-1

Slackware 14.1
x86_64
php-5.6.32-x86_64-1

130921 - Debian Linux 8.0 DSA-4012-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8365, CVE-2017-7208, CVE-2017-7862, CVE-2017-9992

Description

The scan detected that the host is missing the following update:
DSA-4012-1

Observation

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

http://www.debian.org/security/2017/dsa-4012

Debian 8.0
all
libavcodec-extra-56_6:11.11-1~deb8u1
libswscale3_6:11.11-1~deb8u1
libavfilter-dev_6:11.11-1~deb8u1
libavcodec-dev_6:11.11-1~deb8u1
libavutil54_6:11.11-1~deb8u1
libavdevice-dev_6:11.11-1~deb8u1
libswscale-dev_6:11.11-1~deb8u1
libavformat-dev_6:11.11-1~deb8u1
libavutil-dev_6:11.11-1~deb8u1
libav-doc_6:11.11-1~deb8u1
libavdevice55_6:11.11-1~deb8u1
libavcodec-extra_6:11.11-1~deb8u1
libavresample-dev_6:11.11-1~deb8u1
libav-tools_6:11.11-1~deb8u1
libavresample2_6:11.11-1~deb8u1
libavfilter5_6:11.11-1~deb8u1
libavcodec56_6:11.11-1~deb8u1
libav-dbg_6:11.11-1~deb8u1
libavformat56_6:11.11-1~deb8u1

132408 - Oracle VM OVMSA-2017-0166 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-15597

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0166

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/000797.html

OVM3.4
x86_64
xen-4.4.4-105.0.25.el6
xen-tools-4.4.4-105.0.25.el6

132410 - Oracle VM OVMSA-2017-0165 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-5211, CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518, CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0165

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/000795.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-October/000796.html

OVM3.3
x86_64
ntpdate-4.2.6p5-12.0.1.el6_9.1
ntp-4.2.6p5-12.0.1.el6_9.1

OVM3.4
x86_64
ntpdate-4.2.6p5-12.0.1.el6_9.1
ntp-4.2.6p5-12.0.1.el6_9.1

132411 - Oracle VM OVMSA-2017-0162 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-15597

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0162

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/000790.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-October/000792.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-October/000791.html

OVM3.4
x86_64
xen-4.4.4-155.0.2.el6
xen-tools-4.4.4-155.0.2.el6

OVM3.2
x86_64
xen-tools-4.1.3-25.el5.223.96
xen-devel-4.1.3-25.el5.223.96
xen-4.1.3-25.el5.223.96

OVM3.3
x86_64
xen-4.3.0-55.el6.186.60
xen-tools-4.3.0-55.el6.186.60

141765 - Red Hat Enterprise Linux RHSA-2017-3082 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15396

Description

The scan detected that the host is missing the following update:
RHSA-2017-3082

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/msg00041.html

RHEL6D
x86_64
chromium-browser-debuginfo-62.0.3202.75-1.el6_9
chromium-browser-62.0.3202.75-1.el6_9

i386
chromium-browser-debuginfo-62.0.3202.75-1.el6_9
chromium-browser-62.0.3202.75-1.el6_9

RHEL6S
x86_64
chromium-browser-debuginfo-62.0.3202.75-1.el6_9
chromium-browser-62.0.3202.75-1.el6_9

i386
chromium-browser-debuginfo-62.0.3202.75-1.el6_9
chromium-browser-62.0.3202.75-1.el6_9

RHEL6WS
x86_64
chromium-browser-debuginfo-62.0.3202.75-1.el6_9
chromium-browser-62.0.3202.75-1.el6_9

i386
chromium-browser-debuginfo-62.0.3202.75-1.el6_9
chromium-browser-62.0.3202.75-1.el6_9

141768 - Red Hat Enterprise Linux RHSA-2017-3075 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
RHSA-2017-3075

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/msg00038.html

RHEL7D
x86_64
wget-1.14-15.el7_4.1

wget-debuginfo-1.14-15.el7_4.1

RHEL7S
x86_64
wget-1.14-15.el7_4.1
wget-debuginfo-1.14-15.el7_4.1

RHEL7WS
x86_64
wget-1.14-15.el7_4.1
wget-debuginfo-1.14-15.el7_4.1

146020 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2847-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000252, CVE-2017-11472, CVE-2017-12134, CVE-2017-12153, CVE-2017-12154, CVE-2017-13080, CVE-2017-14051, CVE-2017-14106, CVE-2017-14489, CVE-2017-15265, CVE-2017-15649

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2847-1

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/003353.html

SuSE SLED 12 SP3
x86_64
kernel-syms-4.4.92-6.18.1
kernel-default-debugsource-4.4.92-6.18.1
kernel-default-4.4.92-6.18.1
kernel-default-debuginfo-4.4.92-6.18.1
kernel-default-devel-4.4.92-6.18.1
kernel-default-extra-4.4.92-6.18.1
kernel-default-extra-debuginfo-4.4.92-6.18.1

noarch
kernel-devel-4.4.92-6.18.1
kernel-macros-4.4.92-6.18.1
kernel-source-4.4.92-6.18.1

SuSE SLES 12 SP3
noarch
kernel-devel-4.4.92-6.18.1
kernel-macros-4.4.92-6.18.1
kernel-source-4.4.92-6.18.1

x86_64
kernel-default-base-4.4.92-6.18.1
kernel-default-debugsource-4.4.92-6.18.1
kernel-default-base-debuginfo-4.4.92-6.18.1
kernel-default-4.4.92-6.18.1
kernel-default-debuginfo-4.4.92-6.18.1
kernel-default-devel-4.4.92-6.18.1
kernel-syms-4.4.92-6.18.1

146021 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2850-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000256

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2850-1

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/003354.html

SuSE SLED 12 SP3
x86_64
libvirt-admin-3.3.0-5.8.1
libvirt-daemon-driver-nodedev-3.3.0-5.8.1
libvirt-daemon-driver-storage-mpath-3.3.0-5.8.1
libvirt-daemon-driver-storage-logical-3.3.0-5.8.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-5.8.1
libvirt-doc-3.3.0-5.8.1
libvirt-daemon-driver-storage-rbd-3.3.0-5.8.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-interface-3.3.0-5.8.1
libvirt-daemon-driver-secret-3.3.0-5.8.1
libvirt-daemon-driver-storage-iscsi-3.3.0-5.8.1
libvirt-debugsource-3.3.0-5.8.1
libvirt-daemon-driver-storage-3.3.0-5.8.1
libvirt-daemon-debuginfo-3.3.0-5.8.1
libvirt-libs-3.3.0-5.8.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-5.8.1
libvirt-daemon-config-nwfilter-3.3.0-5.8.1
libvirt-admin-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-network-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-5.8.1
libvirt-daemon-qemu-3.3.0-5.8.1
libvirt-libs-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-scsi-3.3.0-5.8.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-5.8.1
libvirt-daemon-xen-3.3.0-5.8.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-libxl-3.3.0-5.8.1
libvirt-daemon-driver-storage-disk-3.3.0-5.8.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-nwfilter-3.3.0-5.8.1
libvirt-client-3.3.0-5.8.1
libvirt-daemon-driver-network-3.3.0-5.8.1
libvirt-3.3.0-5.8.1
libvirt-daemon-config-network-3.3.0-5.8.1
libvirt-daemon-lxc-3.3.0-5.8.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-5.8.1

libvirt-daemon-3.3.0-5.8.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-lxc-3.3.0-5.8.1
libvirt-client-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-qemu-3.3.0-5.8.1
libvirt-daemon-driver-storage-core-3.3.0-5.8.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-5.8.1

SuSE SLES 12 SP3
x86_64
libvirt-daemon-xen-3.3.0-5.8.1
libvirt-admin-3.3.0-5.8.1
libvirt-daemon-driver-nodedev-3.3.0-5.8.1
libvirt-daemon-driver-storage-mpath-3.3.0-5.8.1
libvirt-lock-sanlock-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-logical-3.3.0-5.8.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-5.8.1
libvirt-doc-3.3.0-5.8.1
libvirt-daemon-driver-storage-rbd-3.3.0-5.8.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-interface-3.3.0-5.8.1
libvirt-daemon-driver-secret-3.3.0-5.8.1
libvirt-daemon-driver-storage-iscsi-3.3.0-5.8.1
libvirt-debugsource-3.3.0-5.8.1
libvirt-daemon-driver-storage-3.3.0-5.8.1
libvirt-daemon-debuginfo-3.3.0-5.8.1
libvirt-libs-3.3.0-5.8.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-5.8.1
libvirt-daemon-config-nwfilter-3.3.0-5.8.1
libvirt-admin-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-network-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-5.8.1
libvirt-daemon-qemu-3.3.0-5.8.1
libvirt-libs-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-scsi-3.3.0-5.8.1
libvirt-nss-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-libxl-3.3.0-5.8.1
libvirt-lock-sanlock-3.3.0-5.8.1
libvirt-client-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-storage-disk-3.3.0-5.8.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-nwfilter-3.3.0-5.8.1
libvirt-client-3.3.0-5.8.1
libvirt-daemon-driver-network-3.3.0-5.8.1
libvirt-3.3.0-5.8.1
libvirt-daemon-config-network-3.3.0-5.8.1
libvirt-daemon-lxc-3.3.0-5.8.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-5.8.1
libvirt-daemon-3.3.0-5.8.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-lxc-3.3.0-5.8.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-5.8.1
libvirt-daemon-driver-qemu-3.3.0-5.8.1
libvirt-daemon-driver-storage-core-3.3.0-5.8.1
libvirt-nss-3.3.0-5.8.1

libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-5.8.1

146022 - SuSE Linux 42.3 openSUSE-SU-2017:2878-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000256

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2878-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00096.html

SuSE Linux 42.3
x86_64
libvirt-daemon-driver-storage-rbd-3.3.0-9.1
libvirt-devel-32bit-3.3.0-9.1
libvirt-daemon-driver-nodedev-3.3.0-9.1
libvirt-daemon-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-iscsi-3.3.0-9.1
libvirt-admin-debuginfo-3.3.0-9.1
libvirt-lock-sanlock-debuginfo-3.3.0-9.1
libvirt-debugsource-3.3.0-9.1
libvirt-daemon-uml-3.3.0-9.1
libvirt-daemon-driver-storage-3.3.0-9.1
libvirt-client-debuginfo-3.3.0-9.1
libvirt-libs-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-9.1
libvirt-daemon-lxc-3.3.0-9.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-core-3.3.0-9.1
libvirt-daemon-config-network-3.3.0-9.1
libvirt-daemon-driver-uml-debuginfo-3.3.0-9.1
libvirt-client-debuginfo-32bit-3.3.0-9.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-9.1
libvirt-daemon-driver-qemu-3.3.0-9.1
libvirt-daemon-qemu-3.3.0-9.1
libvirt-daemon-driver-storage-mpath-3.3.0-9.1
libvirt-3.3.0-9.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-9.1
libvirt-doc-3.3.0-9.1
libvirt-daemon-driver-storage-disk-3.3.0-9.1
libvirt-daemon-driver-network-3.3.0-9.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-9.1
libvirt-devel-3.3.0-9.1
libvirt-daemon-driver-storage-logical-3.3.0-9.1
libvirt-daemon-driver-interface-3.3.0-9.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-9.1
libvirt-daemon-driver-secret-3.3.0-9.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-9.1
libvirt-daemon-vbox-3.3.0-9.1
libvirt-daemon-driver-nwfilter-3.3.0-9.1

libvirt-daemon-driver-lxc-debuginfo-3.3.0-9.1
libvirt-daemon-driver-vbox-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-scsi-3.3.0-9.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-9.1
libvirt-daemon-3.3.0-9.1
libvirt-daemon-driver-vbox-3.3.0-9.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-9.1
libvirt-daemon-driver-network-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-9.1
libvirt-daemon-driver-lxc-3.3.0-9.1
libvirt-client-3.3.0-9.1
libvirt-daemon-xen-3.3.0-9.1
libvirt-admin-3.3.0-9.1
libvirt-daemon-driver-libxl-3.3.0-9.1
libvirt-nss-3.3.0-9.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-9.1
libvirt-daemon-driver-uml-3.3.0-9.1
libvirt-nss-debuginfo-3.3.0-9.1
libvirt-libs-3.3.0-9.1
libvirt-lock-sanlock-3.3.0-9.1
libvirt-daemon-config-nwfilter-3.3.0-9.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-9.1

i586
libvirt-daemon-driver-nodedev-3.3.0-9.1
libvirt-daemon-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-iscsi-3.3.0-9.1
libvirt-admin-debuginfo-3.3.0-9.1
libvirt-lock-sanlock-debuginfo-3.3.0-9.1
libvirt-debugsource-3.3.0-9.1
libvirt-daemon-uml-3.3.0-9.1
libvirt-daemon-driver-storage-3.3.0-9.1
libvirt-client-debuginfo-3.3.0-9.1
libvirt-libs-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-9.1
libvirt-daemon-lxc-3.3.0-9.1
libvirt-daemon-driver-storage-core-3.3.0-9.1
libvirt-daemon-config-network-3.3.0-9.1
libvirt-daemon-driver-uml-debuginfo-3.3.0-9.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-9.1
libvirt-daemon-driver-qemu-3.3.0-9.1
libvirt-daemon-qemu-3.3.0-9.1
libvirt-daemon-driver-storage-mpath-3.3.0-9.1
libvirt-3.3.0-9.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-9.1
libvirt-doc-3.3.0-9.1
libvirt-daemon-driver-storage-disk-3.3.0-9.1
libvirt-daemon-driver-network-3.3.0-9.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-9.1
libvirt-devel-3.3.0-9.1
libvirt-daemon-driver-storage-logical-3.3.0-9.1
libvirt-daemon-driver-interface-3.3.0-9.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-9.1
libvirt-daemon-driver-secret-3.3.0-9.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-9.1
libvirt-daemon-vbox-3.3.0-9.1
libvirt-daemon-driver-nwfilter-3.3.0-9.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-9.1
libvirt-daemon-driver-vbox-debuginfo-3.3.0-9.1

libvirt-daemon-driver-storage-scsi-3.3.0-9.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-9.1
libvirt-daemon-3.3.0-9.1
libvirt-daemon-driver-vbox-3.3.0-9.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-9.1
libvirt-daemon-driver-network-debuginfo-3.3.0-9.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-9.1
libvirt-daemon-driver-lxc-3.3.0-9.1
libvirt-client-3.3.0-9.1
libvirt-admin-3.3.0-9.1
libvirt-nss-3.3.0-9.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-9.1
libvirt-daemon-driver-uml-3.3.0-9.1
libvirt-nss-debuginfo-3.3.0-9.1
libvirt-libs-3.3.0-9.1
libvirt-lock-sanlock-3.3.0-9.1
libvirt-daemon-config-nwfilter-3.3.0-9.1

146023 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2875-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, 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:
openSUSE-SU-2017:2875-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00093.html

SuSE Linux 42.2
x86_64
tcpdump-debugsource-4.9.2-6.6.1
tcpdump-debuginfo-4.9.2-6.6.1
tcpdump-4.9.2-6.6.1

SuSE Linux 42.3
x86_64
tcpdump-debugsource-4.9.2-9.1
tcpdump-debuginfo-4.9.2-9.1
tcpdump-4.9.2-9.1

146026 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2854-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, 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:
SUSE-SU-2017:2854-1

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/003355.html

SuSE SLES 12 SP2
x86_64
tcpdump-debugsource-4.9.2-14.5.1
tcpdump-debuginfo-4.9.2-14.5.1
tcpdump-4.9.2-14.5.1

SuSE SLED 12 SP3
x86_64
tcpdump-debugsource-4.9.2-14.5.1
tcpdump-debuginfo-4.9.2-14.5.1
tcpdump-4.9.2-14.5.1

SuSE SLED 12 SP2
x86_64
tcpdump-debugsource-4.9.2-14.5.1
tcpdump-debuginfo-4.9.2-14.5.1
tcpdump-4.9.2-14.5.1

SuSE SLES 12 SP3
x86_64
tcpdump-debugsource-4.9.2-14.5.1
tcpdump-debuginfo-4.9.2-14.5.1
tcpdump-4.9.2-14.5.1

146027 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2895-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2888

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2895-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00113.html

SuSE Linux 42.2
x86_64
libSDL2-2_0-0-debuginfo-32bit-2.0.3-9.5.1
libSDL2-2_0-0-debuginfo-2.0.3-9.5.1
SDL2-debugsource-2.0.3-9.5.1
libSDL2-devel-2.0.3-9.5.1
libSDL2-devel-32bit-2.0.3-9.5.1
libSDL2-2_0-0-2.0.3-9.5.1
libSDL2-2_0-0-32bit-2.0.3-9.5.1

i586
SDL2-debugsource-2.0.3-9.5.1
libSDL2-2_0-0-2.0.3-9.5.1
libSDL2-2_0-0-debuginfo-2.0.3-9.5.1
libSDL2-devel-2.0.3-9.5.1

SuSE Linux 42.3
x86_64
SDL2-debugsource-2.0.3-14.1
libSDL2-2_0-0-debuginfo-2.0.3-14.1
libSDL2-2_0-0-32bit-2.0.3-14.1
libSDL2-2_0-0-debuginfo-32bit-2.0.3-14.1
libSDL2-devel-2.0.3-14.1
libSDL2-devel-32bit-2.0.3-14.1
libSDL2-2_0-0-2.0.3-14.1

i586
libSDL2-2_0-0-2.0.3-14.1
libSDL2-2_0-0-debuginfo-2.0.3-14.1
libSDL2-devel-2.0.3-14.1
SDL2-debugsource-2.0.3-14.1

146029 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2860-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2860-1

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/003358.html

SuSE SLES 12 SP2
x86_64
libwscodecs1-2.2.10-48.12.1
wireshark-debugsource-2.2.10-48.12.1
libwsutil7-2.2.10-48.12.1
libwscodecs1-debuginfo-2.2.10-48.12.1
libwireshark8-debuginfo-2.2.10-48.12.1
wireshark-gtk-debuginfo-2.2.10-48.12.1
wireshark-debuginfo-2.2.10-48.12.1
libwireshark8-2.2.10-48.12.1
libwiretap6-debuginfo-2.2.10-48.12.1
wireshark-2.2.10-48.12.1
libwiretap6-2.2.10-48.12.1
libwsutil7-debuginfo-2.2.10-48.12.1
wireshark-gtk-2.2.10-48.12.1

SuSE SLED 12 SP3
x86_64
libwscodecs1-2.2.10-48.12.1
wireshark-debugsource-2.2.10-48.12.1
libwsutil7-2.2.10-48.12.1
libwscodecs1-debuginfo-2.2.10-48.12.1
libwireshark8-debuginfo-2.2.10-48.12.1
wireshark-gtk-debuginfo-2.2.10-48.12.1
wireshark-debuginfo-2.2.10-48.12.1
libwireshark8-2.2.10-48.12.1
libwiretap6-debuginfo-2.2.10-48.12.1
wireshark-2.2.10-48.12.1
libwiretap6-2.2.10-48.12.1
libwsutil7-debuginfo-2.2.10-48.12.1
wireshark-gtk-2.2.10-48.12.1

SuSE SLED 12 SP2
x86_64
libwscodecs1-2.2.10-48.12.1
wireshark-debugsource-2.2.10-48.12.1
libwsutil7-2.2.10-48.12.1
libwscodecs1-debuginfo-2.2.10-48.12.1
libwireshark8-debuginfo-2.2.10-48.12.1
wireshark-gtk-debuginfo-2.2.10-48.12.1
wireshark-debuginfo-2.2.10-48.12.1
libwireshark8-2.2.10-48.12.1
libwiretap6-debuginfo-2.2.10-48.12.1
wireshark-2.2.10-48.12.1
libwiretap6-2.2.10-48.12.1
libwsutil7-debuginfo-2.2.10-48.12.1
wireshark-gtk-2.2.10-48.12.1

SuSE SLES 12 SP3
x86_64
libwscodecs1-2.2.10-48.12.1
wireshark-debugsource-2.2.10-48.12.1
libwsutil7-2.2.10-48.12.1
libwscodecs1-debuginfo-2.2.10-48.12.1
libwireshark8-debuginfo-2.2.10-48.12.1
wireshark-gtk-debuginfo-2.2.10-48.12.1
wireshark-debuginfo-2.2.10-48.12.1
libwireshark8-2.2.10-48.12.1
libwiretap6-debuginfo-2.2.10-48.12.1
wireshark-2.2.10-48.12.1

libwiretap6-2.2.10-48.12.1
libwsutil7-debuginfo-2.2.10-48.12.1
wireshark-gtk-2.2.10-48.12.1

146031 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2894-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12936, CVE-2017-12937, CVE-2017-13063, CVE-2017-13064, CVE-2017-13139, CVE-2017-13775

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2894-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00112.html

SuSE Linux 42.2
x86_64
GraphicsMagick-1.3.25-11.34.1
perl-GraphicsMagick-1.3.25-11.34.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.34.1
GraphicsMagick-debuginfo-1.3.25-11.34.1
libGraphicsMagickWand-Q16-2-1.3.25-11.34.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.34.1
libGraphicsMagick-Q16-3-1.3.25-11.34.1
GraphicsMagick-debugsource-1.3.25-11.34.1
libGraphicsMagick++-Q16-12-1.3.25-11.34.1
perl-GraphicsMagick-debuginfo-1.3.25-11.34.1
libGraphicsMagick++-devel-1.3.25-11.34.1
libGraphicsMagick3-config-1.3.25-11.34.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.34.1
GraphicsMagick-devel-1.3.25-11.34.1

i586
GraphicsMagick-1.3.25-11.34.1
perl-GraphicsMagick-1.3.25-11.34.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.34.1
GraphicsMagick-debuginfo-1.3.25-11.34.1
libGraphicsMagickWand-Q16-2-1.3.25-11.34.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.34.1
libGraphicsMagick-Q16-3-1.3.25-11.34.1
GraphicsMagick-debugsource-1.3.25-11.34.1
libGraphicsMagick++-Q16-12-1.3.25-11.34.1
perl-GraphicsMagick-debuginfo-1.3.25-11.34.1
libGraphicsMagick++-devel-1.3.25-11.34.1
libGraphicsMagick3-config-1.3.25-11.34.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.34.1
GraphicsMagick-devel-1.3.25-11.34.1

SuSE Linux 42.3
x86_64
GraphicsMagick-1.3.25-34.1
GraphicsMagick-debugsource-1.3.25-34.1
GraphicsMagick-debuginfo-1.3.25-34.1

libGraphicsMagick3-config-1.3.25-34.1
libGraphicsMagick++-Q16-12-1.3.25-34.1
GraphicsMagick-devel-1.3.25-34.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-34.1
libGraphicsMagick++-devel-1.3.25-34.1
libGraphicsMagickWand-Q16-2-1.3.25-34.1
perl-GraphicsMagick-debuginfo-1.3.25-34.1
libGraphicsMagick-Q16-3-1.3.25-34.1
perl-GraphicsMagick-1.3.25-34.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-34.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-34.1

i586
GraphicsMagick-1.3.25-34.1
GraphicsMagick-debugsource-1.3.25-34.1
GraphicsMagick-debuginfo-1.3.25-34.1
libGraphicsMagick3-config-1.3.25-34.1
libGraphicsMagick++-Q16-12-1.3.25-34.1
GraphicsMagick-devel-1.3.25-34.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-34.1
libGraphicsMagick++-devel-1.3.25-34.1
libGraphicsMagickWand-Q16-2-1.3.25-34.1
perl-GraphicsMagick-debuginfo-1.3.25-34.1
libGraphicsMagick-Q16-3-1.3.25-34.1
perl-GraphicsMagick-1.3.25-34.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-34.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-34.1

146034 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2864-1 Update Is Not Installed

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

Risk Level: High

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:
SUSE-SU-2017:2864-1

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/003360.html

SuSE SLED 12 SP2
x86_64
xen-libs-debuginfo-4.7.3_06-43.15.1
xen-libs-4.7.3_06-43.15.1
xen-libs-32bit-4.7.3_06-43.15.1
xen-4.7.3_06-43.15.1
xen-debugsource-4.7.3_06-43.15.1
xen-libs-debuginfo-32bit-4.7.3_06-43.15.1

SuSE SLES 12 SP2
x86_64
xen-libs-debuginfo-4.7.3_06-43.15.1
xen-tools-domU-debuginfo-4.7.3_06-43.15.1

xen-libs-4.7.3_06-43.15.1
xen-tools-domU-4.7.3_06-43.15.1
xen-tools-4.7.3_06-43.15.1
xen-libs-32bit-4.7.3_06-43.15.1
xen-4.7.3_06-43.15.1
xen-debugsource-4.7.3_06-43.15.1
xen-tools-debuginfo-4.7.3_06-43.15.1
xen-libs-debuginfo-32bit-4.7.3_06-43.15.1
xen-doc-html-4.7.3_06-43.15.1

146035 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2902-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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-2017-15396, 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:
openSUSE-SU-2017:2902-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00118.html

SuSE Linux 42.2
x86_64
chromium-62.0.3202.75-104.32.1
chromedriver-62.0.3202.75-104.32.1
chromium-debuginfo-62.0.3202.75-104.32.1
chromium-debugsource-62.0.3202.75-104.32.1
chromedriver-debuginfo-62.0.3202.75-104.32.1

SuSE Linux 42.3
x86_64
chromedriver-62.0.3202.75-118.1
chromium-debugsource-62.0.3202.75-118.1
chromium-62.0.3202.75-118.1
chromedriver-debuginfo-62.0.3202.75-118.1
chromium-debuginfo-62.0.3202.75-118.1

146037 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2869-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000252, CVE-2017-10810, CVE-2017-11472, CVE-2017-11473, CVE-2017-12134, CVE-2017-12153, CVE-2017-12154, CVE-2017-13080, CVE-2017-14051, CVE-2017-14106, CVE-2017-14489, CVE-2017-15649, CVE-2017-7518, CVE-2017-7541, CVE-2017-7542, CVE-2017-8831

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2869-1

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/003361.html

SuSE SLED 12 SP2
x86_64
kernel-syms-4.4.90-92.45.1
kernel-default-debugsource-4.4.90-92.45.1
kernel-default-extra-4.4.90-92.45.1
kernel-default-debuginfo-4.4.90-92.45.1
kernel-default-devel-4.4.90-92.45.1
kernel-default-4.4.90-92.45.1
kernel-default-extra-debuginfo-4.4.90-92.45.1

noarch
kernel-devel-4.4.90-92.45.1
kernel-macros-4.4.90-92.45.1
kernel-source-4.4.90-92.45.1

SuSE SLES 12 SP2
noarch
kernel-devel-4.4.90-92.45.1
kernel-macros-4.4.90-92.45.1
kernel-source-4.4.90-92.45.1

x86_64
kernel-syms-4.4.90-92.45.1
kernel-default-debugsource-4.4.90-92.45.1
kernel-default-base-4.4.90-92.45.1
kernel-default-base-debuginfo-4.4.90-92.45.1
kernel-default-debuginfo-4.4.90-92.45.1
kernel-default-devel-4.4.90-92.45.1
kernel-default-4.4.90-92.45.1

146038 - SuSE SLES 11 SP4 SUSE-SU-2017:2872-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2872-1

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/003363.html

SuSE SLES 11 SP4
i586
mozilla-nss-3.29.5-47.6.1
libfreebl3-3.29.5-47.6.1
mozilla-nss-tools-3.29.5-47.6.1

MozillaFirefox-52.4.0esr-72.13.2
libsoftokn3-3.29.5-47.6.1
MozillaFirefox-translations-52.4.0esr-72.13.2

x86_64
mozilla-nss-3.29.5-47.6.1
libsoftokn3-32bit-3.29.5-47.6.1
libfreebl3-3.29.5-47.6.1
mozilla-nss-tools-3.29.5-47.6.1
MozillaFirefox-52.4.0esr-72.13.2
libfreebl3-32bit-3.29.5-47.6.1
libsoftokn3-3.29.5-47.6.1
MozillaFirefox-translations-52.4.0esr-72.13.2
mozilla-nss-32bit-3.29.5-47.6.1

146040 - SuSE Linux 42.2 openSUSE-SU-2017:2845-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10983, CVE-2017-10984, CVE-2017-10985, CVE-2017-10986, CVE-2017-10987

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2845-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00087.html

SuSE Linux 42.2
x86_64
freeradius-server-perl-debuginfo-3.0.12-2.9.1
freeradius-server-libs-3.0.12-2.9.1
freeradius-server-sqlite-debuginfo-3.0.12-2.9.1
freeradius-server-utils-3.0.12-2.9.1
freeradius-server-perl-3.0.12-2.9.1
freeradius-server-python-3.0.12-2.9.1
freeradius-server-doc-3.0.12-2.9.1
freeradius-server-mysql-debuginfo-3.0.12-2.9.1
freeradius-server-sqlite-3.0.12-2.9.1
freeradius-server-debuginfo-3.0.12-2.9.1
freeradius-server-ldap-debuginfo-3.0.12-2.9.1
freeradius-server-krb5-3.0.12-2.9.1
freeradius-server-3.0.12-2.9.1
freeradius-server-postgresql-3.0.12-2.9.1
freeradius-server-python-debuginfo-3.0.12-2.9.1
freeradius-server-devel-3.0.12-2.9.1
freeradius-server-mysql-3.0.12-2.9.1
freeradius-server-debugsource-3.0.12-2.9.1
freeradius-server-krb5-debuginfo-3.0.12-2.9.1
freeradius-server-ldap-3.0.12-2.9.1
freeradius-server-libs-debuginfo-3.0.12-2.9.1
freeradius-server-postgresql-debuginfo-3.0.12-2.9.1
freeradius-server-utils-debuginfo-3.0.12-2.9.1

146041 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2884-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2884-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00102.html

SuSE Linux 42.2
x86_64
wget-debuginfo-1.14-8.6.1
wget-1.14-8.6.1
wget-debugsource-1.14-8.6.1

i586
wget-debuginfo-1.14-8.6.1
wget-1.14-8.6.1
wget-debugsource-1.14-8.6.1

SuSE Linux 42.3
x86_64
wget-debugsource-1.14-12.1
wget-debuginfo-1.14-12.1
wget-1.14-12.1

i586
wget-debugsource-1.14-12.1
wget-debuginfo-1.14-12.1
wget-1.14-12.1

160320 - CentOS 7 CESA-2017-3075 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
CESA-2017-3075

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/022609.html

CentOS 7
x86_64

wget-1.14-15.el7_4.1

163484 - Oracle Enterprise Linux ELSA-2017-3075 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
ELSA-2017-3075

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/007314.html

OEL7
x86_64
wget-1.14-15.el7_4.1

163487 - Oracle Enterprise Linux ELSA-2017-3071 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-5211, CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518, CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
ELSA-2017-3071

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/007313.html

OEL6
x86_64
ntpdate-4.2.6p5-12.0.1.el6_9.1
ntp-doc-4.2.6p5-12.0.1.el6_9.1
ntp-perl-4.2.6p5-12.0.1.el6_9.1
ntp-4.2.6p5-12.0.1.el6_9.1

i386
ntpdate-4.2.6p5-12.0.1.el6_9.1
ntp-doc-4.2.6p5-12.0.1.el6_9.1
ntp-perl-4.2.6p5-12.0.1.el6_9.1
ntp-4.2.6p5-12.0.1.el6_9.1

170894 - Amazon Linux AMI ALAS-2017-916 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
ALAS-2017-916

Observation

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

https://alas.aws.amazon.com/ALAS-2017-916.html

Amazon Linux AMI
x86_64
wget-debuginfo-1.18-3.28.amzn1
wget-1.18-3.28.amzn1

i686
wget-1.18-3.28.amzn1
wget-debuginfo-1.18-3.28.amzn1

175283 - Scientific Linux Security ERRATA Important: wget on SL7.x x86_64 (1710-18419)

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

Risk Level: High

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: wget on SL7.x x86_64 (1710-18419)

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=18419

SL7
x86_64
wget-1.14-15.el7_4.1
wget-debuginfo-1.14-15.el7_4.1

182500 - FreeBSD PHP Denial Of Service Attack (de7a2b32-bd7d-11e7-b627-d43d7e971a1b)

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

Risk Level: High

CVE: CVE-2016-1283

Description

The scan detected that the host is missing the following update:
PHP -- denial of service attack (de7a2b32-bd7d-11e7-b627-d43d7e971a1b)

Observation

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

http://www.vuxml.org/freebsd/de7a2b32-bd7d-11e7-b627-d43d7e971a1b.html

Affected packages:
php56 < 5.6.31
php70 < 7.0.24
php71 < 7.1.10

182505 - FreeBSD wireshark Multiple Security Issues (4684a426-774d-4390-aa19-b8dd481c4c94)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
wireshark -- multiple security issues (4684a426-774d-4390-aa19-b8dd481c4c94)

Observation

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

http://www.vuxml.org/freebsd/4684a426-774d-4390-aa19-b8dd481c4c94.html

Affected packages:
2.2.0 <= wireshark <= 2.2.9
2.4.0 <= wireshark <= 2.4.1

185940 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3465-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10965, CVE-2017-10966, 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:
USN-3465-1

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/004115.html

Ubuntu 16.04

irssi_0.8.19-1ubuntu1.5

Ubuntu 14.04

irssi_0.8.15-5ubuntu3.3

Ubuntu 17.04

irssi_0.8.20-2ubuntu2.2

Ubuntu 17.10

irssi_1.0.4-1ubuntu2.1

185945 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3471-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16227, CVE-2017-5495

Description

The scan detected that the host is missing the following update:
USN-3471-1

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/004125.html

Ubuntu 16.04

quagga_0.99.24.1-2ubuntu1.3

Ubuntu 14.04

quagga_0.99.22.4-3ubuntu1.4

Ubuntu 17.04

quagga-bgpd_1.1.1-1ubuntu0.1
quagga_1.1.1-1ubuntu0.1

Ubuntu 17.10

quagga-bgpd_1.1.1-3ubuntu0.1
quagga_1.1.1-3ubuntu0.1

185949 - Ubuntu Linux 14.04 USN-3469-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10911, CVE-2017-12153, CVE-2017-12154, CVE-2017-12192, CVE-2017-14051, CVE-2017-14156, CVE-2017-14340, CVE-2017-14489, CVE-2017-14991, CVE-2017-15537, CVE-2017-9984, CVE-2017-9985

Description

The scan detected that the host is missing the following update:
USN-3469-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-October/004123.html

Ubuntu 14.04

linux-image-powerpc64-emb-lts-xenial_4.4.0.98.82
linux-image-generic-lpae-lts-xenial_4.4.0.98.82
linux-image-4.4.0-98-lowlatency_4.4.0-98.121~14.04.1
linux-image-4.4.0-98-generic-lpae_4.4.0-98.121~14.04.1
linux-image-4.4.0-98-powerpc64-emb_4.4.0-98.121~14.04.1
linux-image-powerpc-smp-lts-xenial_4.4.0.98.82
linux-image-4.4.0-98-powerpc-e500mc_4.4.0-98.121~14.04.1
linux-image-4.4.0-98-generic_4.4.0-98.121~14.04.1
linux-image-4.4.0-98-powerpc64-smp_4.4.0-98.121~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.98.82
linux-image-powerpc64-smp-lts-xenial_4.4.0.98.82
linux-image-generic-lts-xenial_4.4.0.98.82
linux-image-powerpc-e500mc-lts-xenial_4.4.0.98.82
linux-image-4.4.0-98-powerpc-smp_4.4.0-98.121~14.04.1

185952 - Ubuntu Linux 16.04 USN-3469-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10911, CVE-2017-12153, CVE-2017-12154, CVE-2017-12192, CVE-2017-14051, CVE-2017-14156, CVE-2017-14340, CVE-2017-14489, CVE-2017-14991, CVE-2017-15537, CVE-2017-9984, CVE-2017-9985

Description

The scan detected that the host is missing the following update:
USN-3469-1

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/004122.html

Ubuntu 16.04

linux-image-kvm_4.4.0.1009.9
linux-image-4.4.0-1033-gke_4.4.0-1033.33
linux-image-4.4.0-98-powerpc64-smp_4.4.0-98.121
linux-image-generic-lpae_4.4.0.98.103
linux-image-4.4.0-1039-aws_4.4.0-1039.48
linux-image-4.4.0-1078-snapdragon_4.4.0-1078.83
linux-image-4.4.0-98-powerpc64-emb_4.4.0-98.121
linux-image-lowlatency_4.4.0.98.103
linux-image-aws_4.4.0.1039.41
linux-image-generic_4.4.0.98.103
linux-image-4.4.0-98-lowlatency_4.4.0-98.121
linux-image-powerpc-smp_4.4.0.98.103
linux-image-powerpc64-emb_4.4.0.98.103
linux-image-4.4.0-98-powerpc-e500mc_4.4.0-98.121
linux-image-4.4.0-98-powerpc-smp_4.4.0-98.121
linux-image-raspi2_4.4.0.1076.76
linux-image-gke_4.4.0.1033.34
linux-image-4.4.0-98-generic_4.4.0-98.121
linux-image-snapdragon_4.4.0.1078.70
linux-image-4.4.0-98-generic-lpae_4.4.0-98.121

linux-image-powerpc-e500mc_4.4.0.98.103
linux-image-4.4.0-1009-kvm_4.4.0-1009.14
linux-image-powerpc64-smp_4.4.0.98.103
linux-image-4.4.0-1076-raspi2_4.4.0-1076.84

192821 - Fedora Linux 25 FEDORA-2017-7e5ac0896e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14737, CVE-2017-2801

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7e5ac0896e

Observation

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

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

Fedora Core 25

botan-1.10.17-1.fc25

192825 - Fedora Linux 26 FEDORA-2017-d4248ba346 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14737, CVE-2017-2801

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d4248ba346

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

botan-1.10.17-1.fc26

192826 - Fedora Linux 26 FEDORA-2017-c2882ae75b Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c2882ae75b

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

tnef-1.4.15-1.fc26

192833 - Fedora Linux 25 FEDORA-2017-2b28a055f2 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2b28a055f2

Observation

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

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

Fedora Core 25

tnef-1.4.15-1.fc25

22630 - NVIDIA GeForce Experience Vulnerability 10-2017

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

Risk Level: Medium

CVE: CVE-2017-0316

Description

A vulnerability is present in some versions of the NVIDIA GeForce Experience.

Observation

NVIDIA is a technology company which manufactures graphics processing units.

A vulnerability is present in some versions of the NVIDIA GeForce Experience. The flaw occurs within NVISystemService64. Successful exploitation could allow an attacker to escalate privileges or cause a denial of service condition.

22632 - (JSA10816) Juniper Junos OS Kernel Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10613

Description

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

Observation

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

A denial-of-service vulnerability is present in some versions of Juniper Junos OS. The flaw lies in a specific loopback filter action command. Successful exploitation could allow an attacker to hang the kernel.

130920 - Debian Linux 8.0, 9.0 DSA-4010-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12976

Description

The scan detected that the host is missing the following update:
DSA-4010-1

Observation

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

http://www.debian.org/security/2017/dsa-4010

Debian 8.0
all
git-annex_5.20141125+deb8u1

Debian 9.0
all
git-annex_6.20170101-1+deb9u1

132412 - Oracle VM OVMSA-2017-0163 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000112, CVE-2017-7542

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0163

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/000793.html

OVM3.4
x86_64
kernel-uek-4.1.12-103.7.4.el6uek
kernel-uek-firmware-4.1.12-103.7.4.el6uek

141763 - Red Hat Enterprise Linux RHSA-2017-3080 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617, CVE-2017-5647, CVE-2017-5664

Description

The scan detected that the host is missing the following update:
RHSA-2017-3080

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/msg00039.html

RHEL6S
noarch
tomcat6-lib-6.0.24-111.el6_9
tomcat6-docs-webapp-6.0.24-111.el6_9
tomcat6-javadoc-6.0.24-111.el6_9
tomcat6-webapps-6.0.24-111.el6_9
tomcat6-admin-webapps-6.0.24-111.el6_9
tomcat6-jsp-2.1-api-6.0.24-111.el6_9
tomcat6-6.0.24-111.el6_9
tomcat6-el-2.1-api-6.0.24-111.el6_9
tomcat6-servlet-2.5-api-6.0.24-111.el6_9

RHEL6WS
noarch
tomcat6-6.0.24-111.el6_9
tomcat6-lib-6.0.24-111.el6_9
tomcat6-jsp-2.1-api-6.0.24-111.el6_9
tomcat6-servlet-2.5-api-6.0.24-111.el6_9
tomcat6-el-2.1-api-6.0.24-111.el6_9

RHEL6D
noarch
tomcat6-webapps-6.0.24-111.el6_9
tomcat6-lib-6.0.24-111.el6_9
tomcat6-docs-webapp-6.0.24-111.el6_9
tomcat6-6.0.24-111.el6_9
tomcat6-admin-webapps-6.0.24-111.el6_9
tomcat6-jsp-2.1-api-6.0.24-111.el6_9
tomcat6-javadoc-6.0.24-111.el6_9
tomcat6-el-2.1-api-6.0.24-111.el6_9
tomcat6-servlet-2.5-api-6.0.24-111.el6_9

141767 - Red Hat Enterprise Linux RHSA-2017-3081 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617, CVE-2017-5647, CVE-2017-7674

Description

The scan detected that the host is missing the following update:
RHSA-2017-3081

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/msg00040.html

RHEL7D
noarch
tomcat-javadoc-7.0.76-3.el7_4
tomcat-jsp-2.2-api-7.0.76-3.el7_4
tomcat-lib-7.0.76-3.el7_4
tomcat-7.0.76-3.el7_4
tomcat-docs-webapp-7.0.76-3.el7_4
tomcat-servlet-3.0-api-7.0.76-3.el7_4
tomcat-el-2.2-api-7.0.76-3.el7_4
tomcat-admin-webapps-7.0.76-3.el7_4
tomcat-jsvc-7.0.76-3.el7_4
tomcat-webapps-7.0.76-3.el7_4

RHEL7S
noarch
tomcat-lib-7.0.76-3.el7_4
tomcat-jsp-2.2-api-7.0.76-3.el7_4
tomcat-7.0.76-3.el7_4
tomcat-webapps-7.0.76-3.el7_4
tomcat-servlet-3.0-api-7.0.76-3.el7_4
tomcat-el-2.2-api-7.0.76-3.el7_4
tomcat-javadoc-7.0.76-3.el7_4
tomcat-admin-webapps-7.0.76-3.el7_4
tomcat-jsvc-7.0.76-3.el7_4
tomcat-docs-webapp-7.0.76-3.el7_4

RHEL7WS
noarch
tomcat-lib-7.0.76-3.el7_4
tomcat-jsp-2.2-api-7.0.76-3.el7_4
tomcat-7.0.76-3.el7_4
tomcat-webapps-7.0.76-3.el7_4
tomcat-servlet-3.0-api-7.0.76-3.el7_4
tomcat-el-2.2-api-7.0.76-3.el7_4
tomcat-javadoc-7.0.76-3.el7_4
tomcat-admin-webapps-7.0.76-3.el7_4
tomcat-jsvc-7.0.76-3.el7_4
tomcat-docs-webapp-7.0.76-3.el7_4

146018 - SuSE Linux 42.3 openSUSE-SU-2017:2846-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13080, CVE-2017-15265, CVE-2017-15649

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2846-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00088.html

SuSE Linux 42.3
x86_64
kernel-debug-debugsource-4.4.92-31.1
kernel-obs-build-4.4.92-31.1
kernel-debug-base-4.4.92-31.1
kernel-obs-qa-4.4.92-31.1
kernel-vanilla-base-4.4.92-31.1
kernel-vanilla-devel-4.4.92-31.1
kernel-default-base-4.4.92-31.1
kernel-debug-devel-debuginfo-4.4.92-31.1
kernel-default-base-debuginfo-4.4.92-31.1
kernel-vanilla-4.4.92-31.1
kernel-debug-base-debuginfo-4.4.92-31.1
kernel-debug-devel-4.4.92-31.1
kernel-default-4.4.92-31.1
kernel-syms-4.4.92-31.1
kernel-vanilla-base-debuginfo-4.4.92-31.1
kernel-debug-debuginfo-4.4.92-31.1
kernel-vanilla-debugsource-4.4.92-31.1
kernel-default-devel-4.4.92-31.1
kernel-obs-build-debugsource-4.4.92-31.1
kernel-default-debuginfo-4.4.92-31.1
kernel-default-debugsource-4.4.92-31.1
kernel-debug-4.4.92-31.1
kernel-vanilla-debuginfo-4.4.92-31.1

noarch
kernel-docs-html-4.4.92-31.2
kernel-devel-4.4.92-31.1
kernel-docs-pdf-4.4.92-31.2
kernel-source-4.4.92-31.1
kernel-docs-4.4.92-31.2
kernel-source-vanilla-4.4.92-31.1
kernel-macros-4.4.92-31.1

146028 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2892-1 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:
openSUSE-SU-2017:2892-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00110.html

SuSE Linux 42.2
x86_64
openvpn-2.3.8-8.13.1
openvpn-devel-2.3.8-8.13.1
openvpn-auth-pam-plugin-debuginfo-2.3.8-8.13.1

openvpn-down-root-plugin-debuginfo-2.3.8-8.13.1
openvpn-debuginfo-2.3.8-8.13.1
openvpn-auth-pam-plugin-2.3.8-8.13.1
openvpn-down-root-plugin-2.3.8-8.13.1
openvpn-debugsource-2.3.8-8.13.1

i586
openvpn-2.3.8-8.13.1
openvpn-devel-2.3.8-8.13.1
openvpn-auth-pam-plugin-debuginfo-2.3.8-8.13.1
openvpn-down-root-plugin-debuginfo-2.3.8-8.13.1
openvpn-debuginfo-2.3.8-8.13.1
openvpn-auth-pam-plugin-2.3.8-8.13.1
openvpn-down-root-plugin-2.3.8-8.13.1
openvpn-debugsource-2.3.8-8.13.1

SuSE Linux 42.3
x86_64
openvpn-down-root-plugin-debuginfo-2.3.8-14.1
openvpn-debuginfo-2.3.8-14.1
openvpn-auth-pam-plugin-2.3.8-14.1
openvpn-down-root-plugin-2.3.8-14.1
openvpn-2.3.8-14.1
openvpn-devel-2.3.8-14.1
openvpn-debugsource-2.3.8-14.1
openvpn-auth-pam-plugin-debuginfo-2.3.8-14.1

i586
openvpn-down-root-plugin-debuginfo-2.3.8-14.1
openvpn-debuginfo-2.3.8-14.1
openvpn-auth-pam-plugin-2.3.8-14.1
openvpn-down-root-plugin-2.3.8-14.1
openvpn-2.3.8-14.1
openvpn-devel-2.3.8-14.1
openvpn-debugsource-2.3.8-14.1
openvpn-auth-pam-plugin-debuginfo-2.3.8-14.1

146030 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2848-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14608

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2848-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00089.html

SuSE Linux 42.2
x86_64
libraw15-debuginfo-0.17.1-2.14.1
libraw-tools-0.17.1-2.14.1
libraw-devel-static-0.17.1-2.14.1

libraw-debugsource-0.17.1-2.14.1
libraw15-0.17.1-2.14.1
libraw-tools-debuginfo-0.17.1-2.14.1
libraw-devel-0.17.1-2.14.1

i586
libraw15-debuginfo-0.17.1-2.14.1
libraw-tools-0.17.1-2.14.1
libraw-devel-static-0.17.1-2.14.1
libraw-debugsource-0.17.1-2.14.1
libraw15-0.17.1-2.14.1
libraw-tools-debuginfo-0.17.1-2.14.1
libraw-devel-0.17.1-2.14.1

SuSE Linux 42.3
x86_64
libraw15-0.17.1-14.1
libraw-tools-debuginfo-0.17.1-14.1
libraw-devel-0.17.1-14.1
libraw15-debuginfo-0.17.1-14.1
libraw-debugsource-0.17.1-14.1
libraw-tools-0.17.1-14.1
libraw-devel-static-0.17.1-14.1

i586
libraw15-0.17.1-14.1
libraw-tools-debuginfo-0.17.1-14.1
libraw-devel-0.17.1-14.1
libraw15-debuginfo-0.17.1-14.1
libraw-debugsource-0.17.1-14.1
libraw-tools-0.17.1-14.1
libraw-devel-static-0.17.1-14.1

146036 - SuSE Linux 42.2 openSUSE-SU-2017:2905-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13080, CVE-2017-15265, CVE-2017-15649

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2905-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00121.html

SuSE Linux 42.2
x86_64
kernel-debug-base-4.4.92-18.36.1
kernel-vanilla-debugsource-4.4.92-18.36.1
kernel-syms-4.4.92-18.36.1
kernel-default-debugsource-4.4.92-18.36.1
kernel-default-base-debuginfo-4.4.92-18.36.1
kernel-default-debuginfo-4.4.92-18.36.1
kernel-vanilla-devel-4.4.92-18.36.1

kernel-debug-devel-debuginfo-4.4.92-18.36.1
kernel-default-base-4.4.92-18.36.1
kernel-debug-debugsource-4.4.92-18.36.1
kernel-vanilla-base-debuginfo-4.4.92-18.36.1
kernel-debug-4.4.92-18.36.1
kernel-obs-build-debugsource-4.4.92-18.36.1
kernel-debug-base-debuginfo-4.4.92-18.36.1
kernel-default-devel-4.4.92-18.36.1
kernel-obs-qa-4.4.92-18.36.1
kernel-obs-build-4.4.92-18.36.1
kernel-vanilla-base-4.4.92-18.36.1
kernel-default-4.4.92-18.36.1
kernel-debug-devel-4.4.92-18.36.1
kernel-debug-debuginfo-4.4.92-18.36.1
kernel-vanilla-debuginfo-4.4.92-18.36.1
kernel-vanilla-4.4.92-18.36.1

noarch
kernel-docs-html-4.4.92-18.36.2
kernel-macros-4.4.92-18.36.1
kernel-source-4.4.92-18.36.1
kernel-docs-pdf-4.4.92-18.36.2
kernel-devel-4.4.92-18.36.1
kernel-docs-4.4.92-18.36.2
kernel-source-vanilla-4.4.92-18.36.1

160318 - CentOS 6 CESA-2017-3080 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617, CVE-2017-5647, CVE-2017-5664

Description

The scan detected that the host is missing the following update:
CESA-2017-3080

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/022610.html

CentOS 6
noarch
tomcat6-webapps-6.0.24-111.el6_9
tomcat6-lib-6.0.24-111.el6_9
tomcat6-docs-webapp-6.0.24-111.el6_9
tomcat6-6.0.24-111.el6_9
tomcat6-admin-webapps-6.0.24-111.el6_9
tomcat6-jsp-2.1-api-6.0.24-111.el6_9
tomcat6-javadoc-6.0.24-111.el6_9
tomcat6-el-2.1-api-6.0.24-111.el6_9
tomcat6-servlet-2.5-api-6.0.24-111.el6_9

160321 - CentOS 7 CESA-2017-3081 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617, CVE-2017-5647, CVE-2017-7674

Description

The scan detected that the host is missing the following update:
CESA-2017-3081

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/022611.html

CentOS 7
noarch
tomcat-javadoc-7.0.76-3.el7_4
tomcat-jsp-2.2-api-7.0.76-3.el7_4
tomcat-lib-7.0.76-3.el7_4
tomcat-7.0.76-3.el7_4
tomcat-docs-webapp-7.0.76-3.el7_4
tomcat-servlet-3.0-api-7.0.76-3.el7_4
tomcat-el-2.2-api-7.0.76-3.el7_4
tomcat-admin-webapps-7.0.76-3.el7_4
tomcat-jsvc-7.0.76-3.el7_4
tomcat-webapps-7.0.76-3.el7_4

163483 - Oracle Enterprise Linux ELSA-2017-3631 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000112, CVE-2017-7542

Description

The scan detected that the host is missing the following update:
ELSA-2017-3631

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/007302.html
http://oss.oracle.com/pipermail/el-errata/2017-October/007303.html

OEL7
x86_64
kernel-uek-debug-4.1.12-103.7.4.el7uek
kernel-uek-doc-4.1.12-103.7.4.el7uek
kernel-uek-4.1.12-103.7.4.el7uek
kernel-uek-firmware-4.1.12-103.7.4.el7uek
kernel-uek-devel-4.1.12-103.7.4.el7uek
kernel-uek-debug-devel-4.1.12-103.7.4.el7uek

OEL6
x86_64
kernel-uek-doc-4.1.12-103.7.4.el6uek
kernel-uek-4.1.12-103.7.4.el6uek
kernel-uek-devel-4.1.12-103.7.4.el6uek

kernel-uek-debug-4.1.12-103.7.4.el6uek
kernel-uek-debug-devel-4.1.12-103.7.4.el6uek
kernel-uek-firmware-4.1.12-103.7.4.el6uek

163485 - Oracle Enterprise Linux ELSA-2017-3080 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617, CVE-2017-5647, CVE-2017-5664

Description

The scan detected that the host is missing the following update:
ELSA-2017-3080

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/007315.html

OEL6
x86_64
tomcat6-webapps-6.0.24-111.el6_9
tomcat6-lib-6.0.24-111.el6_9
tomcat6-docs-webapp-6.0.24-111.el6_9
tomcat6-6.0.24-111.el6_9
tomcat6-admin-webapps-6.0.24-111.el6_9
tomcat6-jsp-2.1-api-6.0.24-111.el6_9
tomcat6-javadoc-6.0.24-111.el6_9
tomcat6-el-2.1-api-6.0.24-111.el6_9
tomcat6-servlet-2.5-api-6.0.24-111.el6_9

i386
tomcat6-webapps-6.0.24-111.el6_9
tomcat6-lib-6.0.24-111.el6_9
tomcat6-docs-webapp-6.0.24-111.el6_9
tomcat6-6.0.24-111.el6_9
tomcat6-admin-webapps-6.0.24-111.el6_9
tomcat6-jsp-2.1-api-6.0.24-111.el6_9
tomcat6-javadoc-6.0.24-111.el6_9
tomcat6-el-2.1-api-6.0.24-111.el6_9
tomcat6-servlet-2.5-api-6.0.24-111.el6_9

163488 - Oracle Enterprise Linux ELSA-2017-3081 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617, CVE-2017-5647, CVE-2017-7674

Description

The scan detected that the host is missing the following update:
ELSA-2017-3081

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/007316.html

OEL7
x86_64
tomcat-javadoc-7.0.76-3.el7_4
tomcat-jsp-2.2-api-7.0.76-3.el7_4
tomcat-lib-7.0.76-3.el7_4
tomcat-7.0.76-3.el7_4
tomcat-docs-webapp-7.0.76-3.el7_4
tomcat-servlet-3.0-api-7.0.76-3.el7_4
tomcat-el-2.2-api-7.0.76-3.el7_4
tomcat-admin-webapps-7.0.76-3.el7_4
tomcat-jsvc-7.0.76-3.el7_4
tomcat-webapps-7.0.76-3.el7_4

170890 - Amazon Linux AMI ALAS-2017-913 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12617

Description

The scan detected that the host is missing the following update:
ALAS-2017-913

Observation

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

https://alas.aws.amazon.com/ALAS-2017-913.html

Amazon Linux AMI
noarch
tomcat8-8.5.23-1.75.amzn1
tomcat7-admin-webapps-7.0.82-1.30.amzn1
tomcat7-servlet-3.0-api-7.0.82-1.30.amzn1
tomcat7-7.0.82-1.30.amzn1
tomcat8-el-3.0-api-8.5.23-1.75.amzn1
tomcat8-servlet-3.1-api-8.5.23-1.75.amzn1
tomcat8-webapps-8.5.23-1.75.amzn1
tomcat80-webapps-8.0.47-1.78.amzn1
tomcat80-javadoc-8.0.47-1.78.amzn1
tomcat80-admin-webapps-8.0.47-1.78.amzn1
tomcat7-el-2.2-api-7.0.82-1.30.amzn1
tomcat8-admin-webapps-8.5.23-1.75.amzn1
tomcat80-log4j-8.0.47-1.78.amzn1
tomcat8-log4j-8.5.23-1.75.amzn1
tomcat7-log4j-7.0.82-1.30.amzn1
tomcat8-javadoc-8.5.23-1.75.amzn1
tomcat80-lib-8.0.47-1.78.amzn1
tomcat7-jsp-2.2-api-7.0.82-1.30.amzn1
tomcat80-docs-webapp-8.0.47-1.78.amzn1
tomcat7-docs-webapp-7.0.82-1.30.amzn1
tomcat80-jsp-2.3-api-8.0.47-1.78.amzn1
tomcat7-webapps-7.0.82-1.30.amzn1
tomcat80-servlet-3.1-api-8.0.47-1.78.amzn1
tomcat8-lib-8.5.23-1.75.amzn1

tomcat80-8.0.47-1.78.amzn1
tomcat7-lib-7.0.82-1.30.amzn1
tomcat8-docs-webapp-8.5.23-1.75.amzn1
tomcat8-jsp-2.3-api-8.5.23-1.75.amzn1
tomcat7-javadoc-7.0.82-1.30.amzn1
tomcat80-el-3.0-api-8.0.47-1.78.amzn1

170893 - Amazon Linux AMI ALAS-2017-917 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon 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:
ALAS-2017-917

Observation

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

https://alas.aws.amazon.com/ALAS-2017-917.html

Amazon Linux AMI
i686
java-1.8.0-openjdk-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-src-1.8.0.151-1.b12.35.amzn1

noarch
java-1.8.0-openjdk-javadoc-zip-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-javadoc-1.8.0.151-1.b12.35.amzn1

x86_64
java-1.8.0-openjdk-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-demo-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-devel-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-debuginfo-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-headless-1.8.0.151-1.b12.35.amzn1
java-1.8.0-openjdk-src-1.8.0.151-1.b12.35.amzn1

175280 - Scientific Linux Security ERRATA Important: tomcat6 on SL6.x (noarch) (1710-19140)

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617, CVE-2017-5647, CVE-2017-5664

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: tomcat6 on SL6.x (noarch) (1710-19140)

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=19140

SL6
noarch
tomcat6-webapps-6.0.24-111.el6_9
tomcat6-lib-6.0.24-111.el6_9
tomcat6-docs-webapp-6.0.24-111.el6_9
tomcat6-6.0.24-111.el6_9
tomcat6-admin-webapps-6.0.24-111.el6_9
tomcat6-jsp-2.1-api-6.0.24-111.el6_9
tomcat6-javadoc-6.0.24-111.el6_9
tomcat6-el-2.1-api-6.0.24-111.el6_9
tomcat6-servlet-2.5-api-6.0.24-111.el6_9

175281 - Scientific Linux Security ERRATA Important: tomcat on SL7.x (noarch) (1710-18759)

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617, CVE-2017-5647, CVE-2017-7674

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: tomcat on SL7.x (noarch) (1710-18759)

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=18759

SL7
noarch
tomcat-javadoc-7.0.76-3.el7_4
tomcat-jsp-2.2-api-7.0.76-3.el7_4
tomcat-lib-7.0.76-3.el7_4
tomcat-7.0.76-3.el7_4
tomcat-docs-webapp-7.0.76-3.el7_4
tomcat-servlet-3.0-api-7.0.76-3.el7_4
tomcat-el-2.2-api-7.0.76-3.el7_4
tomcat-admin-webapps-7.0.76-3.el7_4
tomcat-jsvc-7.0.76-3.el7_4
tomcat-webapps-7.0.76-3.el7_4

185947 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3464-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7098, CVE-2017-13089, CVE-2017-13090, CVE-2017-6508

Description

The scan detected that the host is missing the following update:
USN-3464-1

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/004114.html

Ubuntu 16.04

wget_1.17.1-1ubuntu1.3

Ubuntu 14.04

wget_1.15-1ubuntu1.14.04.3

Ubuntu 17.04

wget_1.18-2ubuntu1.1

Ubuntu 17.10

wget_1.19.1-3ubuntu1.1

192818 - Fedora Linux 26 FEDORA-2017-a0ffdf1fbd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14517, CVE-2017-14518, CVE-2017-14519, CVE-2017-14617, CVE-2017-14926, CVE-2017-14927, CVE-2017-14928, CVE-2017-14929, CVE-2017-14975, CVE-2017-14976, CVE-2017-14977

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a0ffdf1fbd

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

mingw-poppler-0.52.0-5.fc26

192822 - Fedora Linux 25 FEDORA-2017-6127ddb036 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14517, CVE-2017-14518, CVE-2017-14519, CVE-2017-14617, CVE-2017-14926, CVE-2017-14927, CVE-2017-14928, CVE-2017-14929, CVE-2017-14975, CVE-2017-14976, CVE-2017-14977

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6127ddb036

Observation

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

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

Fedora Core 25

mingw-poppler-0.45.0-5.fc25

192823 - Fedora Linux 25 FEDORA-2017-cafcdbdde5 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-cafcdbdde5

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

kernel-4.13.8-100.fc25

192831 - Fedora Linux 26 FEDORA-2017-c110ac0eb1 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-c110ac0eb1

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

kernel-4.13.8-200.fc26

22624 - (JSA10827) Juniper Junos 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 Junos.

Observation

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

Multiple vulnerabilities are present in some versions of Juniper Junos. 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.

22633 - (JSA10809) Juniper SRX Series Cryptographic Weakness Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10606

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in TPM Firmware. Successful exploitation could allow an attacker to decrypt sensitive information.

22636 - Oracle MySQL Server Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10165, CVE-2017-10167, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, 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-2017-10378, CVE-2017-10379, CVE-2017-10384, CVE-2017-3731

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL Server.

Observation

Oracle MySQL Server is a popular open source database.

Multiple vulnerabilities are present in some versions of Oracle MySQL Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or have unauthorized access to the target system.

22637 - (JSA10817) Juniper Junos OS Telnetd Denial of Service Vulnerabilities (CVE-2017-10614)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10614

Description

Multiple denial-of-service vulnerabilities are present in some versions of Juniper Junos OS.

Observation

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

Multiple denial-of-service vulnerabilities are present in some versions of Juniper Junos OS. The flaw lies in the telnet daemon. Successful exploitation could allow a remote attacker to cause a denial-of-service.

22642 - Oracle VM VirtualBox Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2017-10392, CVE-2017-10407, CVE-2017-10408, CVE-2017-10428, CVE-2017-3733

Description

Multiple vulnerabilities are present in some versions of Oracle VM VirtualBox.

Observation

Oracle VM VirtualBox is a virtualization software.

Multiple vulnerabilities are present in some versions of Oracle VM VirtualBox. The flaws exist in core component. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or do unauthorized modifications on the target system.

22644 - Oracle WebCenter Content Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2017-10360

Description

A vulnerability is present in Oracle WebCenter Content.

Observation

Oracle WebCenter Content is a complete Enterprise Content Management Software that provides a unified repository to the content.

A vulnerability is present in Oracle WebCenter Content. The flaw lies in the WebCenter Content component. Successful exploitation could allow an attacker to gain unauthorized access to critical data and or disclose sensitive information.

22645 - (JSA10817) Juniper Junos OS Telnetd Denial of Service Vulnerabilities (CVE-2017-10621)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10621

Description

Multiple denial-of-service vulnerabilities are present in some versions of Juniper Junos OS.

Observation

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

Multiple denial-of-service vulnerabilities are present in some versions of Juniper Junos OS. The flaw lies in the telnet daemon. Successful exploitation could allow a remote attacker to cause a denial-of-service.

22655 - IBM WebSphere Application Server Liberty Multiple JSF Vulnerabilities (swg22008707)

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

Risk Level: Medium

CVE: CVE-2011-4343, CVE-2017-1583

Description

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

Observation

IBM WebSphere Application Server Liberty is a Java application server.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server Liberty. The flaws lie in the Java Server Faces component. Successful exploitation could allow an attacker to obtain sensitive information.

88893 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-298-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware 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:
SSA:2017-298-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.439610

Slackware 14.0
x86_64
irssi-1.0.5-x86_64-1

Slackware 14.2
x86_64
irssi-1.0.5-x86_64-1

i586
irssi-1.0.5-i586-1

Slackware 14.1
x86_64
irssi-1.0.5-x86_64-1

146019 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2868-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10279, CVE-2017-10283, CVE-2017-10286, CVE-2017-10294, CVE-2017-10314, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384, CVE-2017-3731

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2868-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00091.html

SuSE Linux 42.2
i586
mysql-community-server-test-5.6.38-24.12.1
mysql-community-server-debugsource-5.6.38-24.12.1
mysql-community-server-5.6.38-24.12.1
mysql-community-server-test-debuginfo-5.6.38-24.12.1
libmysql56client18-debuginfo-5.6.38-24.12.1
libmysql56client_r18-5.6.38-24.12.1
mysql-community-server-tools-debuginfo-5.6.38-24.12.1
mysql-community-server-tools-5.6.38-24.12.1
mysql-community-server-client-5.6.38-24.12.1
mysql-community-server-bench-5.6.38-24.12.1
mysql-community-server-debuginfo-5.6.38-24.12.1
libmysql56client18-5.6.38-24.12.1
mysql-community-server-bench-debuginfo-5.6.38-24.12.1
mysql-community-server-client-debuginfo-5.6.38-24.12.1

noarch
mysql-community-server-errormessages-5.6.38-24.12.1

x86_64
mysql-community-server-test-5.6.38-24.12.1
mysql-community-server-debugsource-5.6.38-24.12.1
mysql-community-server-5.6.38-24.12.1
mysql-community-server-test-debuginfo-5.6.38-24.12.1
libmysql56client18-32bit-5.6.38-24.12.1
libmysql56client18-debuginfo-5.6.38-24.12.1
libmysql56client_r18-5.6.38-24.12.1
mysql-community-server-tools-debuginfo-5.6.38-24.12.1
mysql-community-server-tools-5.6.38-24.12.1
mysql-community-server-client-5.6.38-24.12.1
libmysql56client_r18-32bit-5.6.38-24.12.1
mysql-community-server-bench-5.6.38-24.12.1
libmysql56client18-debuginfo-32bit-5.6.38-24.12.1
mysql-community-server-debuginfo-5.6.38-24.12.1
libmysql56client18-5.6.38-24.12.1
mysql-community-server-bench-debuginfo-5.6.38-24.12.1
mysql-community-server-client-debuginfo-5.6.38-24.12.1

SuSE Linux 42.3
i586
mysql-community-server-client-debuginfo-5.6.38-30.1
mysql-community-server-bench-5.6.38-30.1
libmysql56client18-5.6.38-30.1
mysql-community-server-test-5.6.38-30.1
mysql-community-server-client-5.6.38-30.1
mysql-community-server-bench-debuginfo-5.6.38-30.1
libmysql56client_r18-5.6.38-30.1
mysql-community-server-tools-5.6.38-30.1

mysql-community-server-5.6.38-30.1
mysql-community-server-debuginfo-5.6.38-30.1
libmysql56client18-debuginfo-5.6.38-30.1
mysql-community-server-debugsource-5.6.38-30.1
mysql-community-server-tools-debuginfo-5.6.38-30.1
mysql-community-server-test-debuginfo-5.6.38-30.1

noarch
mysql-community-server-errormessages-5.6.38-30.1

x86_64
libmysql56client18-32bit-5.6.38-30.1
libmysql56client18-debuginfo-32bit-5.6.38-30.1
mysql-community-server-client-debuginfo-5.6.38-30.1
libmysql56client_r18-32bit-5.6.38-30.1
mysql-community-server-bench-5.6.38-30.1
libmysql56client18-5.6.38-30.1
mysql-community-server-test-5.6.38-30.1
mysql-community-server-client-5.6.38-30.1
mysql-community-server-bench-debuginfo-5.6.38-30.1
libmysql56client_r18-5.6.38-30.1
mysql-community-server-tools-5.6.38-30.1
mysql-community-server-5.6.38-30.1
mysql-community-server-debuginfo-5.6.38-30.1
libmysql56client18-debuginfo-5.6.38-30.1
mysql-community-server-debugsource-5.6.38-30.1
mysql-community-server-tools-debuginfo-5.6.38-30.1
mysql-community-server-test-debuginfo-5.6.38-30.1

146033 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2896-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1863, CVE-2015-4141, CVE-2015-4142, CVE-2015-4143, CVE-2015-4144, CVE-2015-4145, CVE-2015-5314, CVE-2016-4476, 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-2017:2896-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00114.html

SuSE Linux 42.2
x86_64
hostapd-debuginfo-2.6-5.3.1
hostapd-debugsource-2.6-5.3.1
hostapd-2.6-5.3.1

i586
hostapd-debuginfo-2.6-5.3.1
hostapd-debugsource-2.6-5.3.1
hostapd-2.6-5.3.1

SuSE Linux 42.3

x86_64
hostapd-debuginfo-2.6-8.1
hostapd-debugsource-2.6-8.1
hostapd-2.6-8.1

i586
hostapd-debuginfo-2.6-8.1
hostapd-debugsource-2.6-8.1
hostapd-2.6-8.1

146039 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2880-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2880-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00098.html

SuSE Linux 42.2
x86_64
curl-debuginfo-7.37.0-16.9.1
libcurl4-debuginfo-32bit-7.37.0-16.9.1
libcurl4-7.37.0-16.9.1
curl-debugsource-7.37.0-16.9.1
libcurl-devel-32bit-7.37.0-16.9.1
libcurl4-debuginfo-7.37.0-16.9.1
libcurl4-32bit-7.37.0-16.9.1
curl-7.37.0-16.9.1
libcurl-devel-7.37.0-16.9.1

i586
curl-debuginfo-7.37.0-16.9.1
libcurl4-7.37.0-16.9.1
curl-debugsource-7.37.0-16.9.1
libcurl4-debuginfo-7.37.0-16.9.1
curl-7.37.0-16.9.1
libcurl-devel-7.37.0-16.9.1

SuSE Linux 42.3
x86_64
curl-debuginfo-7.37.0-23.1
libcurl-devel-32bit-7.37.0-23.1
libcurl4-32bit-7.37.0-23.1
libcurl4-debuginfo-7.37.0-23.1
curl-7.37.0-23.1
curl-debugsource-7.37.0-23.1
libcurl-devel-7.37.0-23.1
libcurl4-debuginfo-32bit-7.37.0-23.1
libcurl4-7.37.0-23.1

i586
curl-debuginfo-7.37.0-23.1
libcurl4-debuginfo-7.37.0-23.1
curl-7.37.0-23.1
curl-debugsource-7.37.0-23.1
libcurl-devel-7.37.0-23.1
libcurl4-7.37.0-23.1

178540 - Gentoo Linux GLSA-201710-30 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-201710-30

Observation

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

https://security.gentoo.org/glsa/201710-30

Affected packages:
x11-base/xorg-server < 1.19.4

178541 - Gentoo Linux GLSA-201710-28 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-201710-28

Observation

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

https://security.gentoo.org/glsa/201710-28

Affected packages:
dev-java/jython < 2.7.0-r2

178542 - Gentoo Linux GLSA-201710-31 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-201710-31

Observation

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

https://security.gentoo.org/glsa/201710-31

Affected packages:
dev-java/oracle-jdk-bin < 1.8.0.152-r1
dev-java/oracle-jre-bin < 1.8.0.152-r1

178543 - Gentoo Linux GLSA-201710-32 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-201710-32

Observation

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

https://security.gentoo.org/glsa/201710-32

Affected packages:
www-servers/apache < 2.4.27-r1

178544 - Gentoo Linux GLSA-201710-29 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-201710-29

Observation

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

https://security.gentoo.org/glsa/201710-29

Affected packages:
net-misc/asterisk < 11.25.3

192817 - Fedora Linux 26 FEDORA-2017-2c63df4fe3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5180

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2c63df4fe3

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

glibc-2.25-12.fc26

141766 - Red Hat Enterprise Linux RHSA-2017-3071 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
RHSA-2017-3071

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/msg00037.html

RHEL6D
i386
ntpdate-4.2.6p5-12.el6_9.1
ntp-debuginfo-4.2.6p5-12.el6_9.1
ntp-perl-4.2.6p5-12.el6_9.1
ntp-4.2.6p5-12.el6_9.1

noarch
ntp-doc-4.2.6p5-12.el6_9.1

x86_64
ntpdate-4.2.6p5-12.el6_9.1
ntp-debuginfo-4.2.6p5-12.el6_9.1
ntp-perl-4.2.6p5-12.el6_9.1
ntp-4.2.6p5-12.el6_9.1

RHEL6S
i386
ntpdate-4.2.6p5-12.el6_9.1
ntp-debuginfo-4.2.6p5-12.el6_9.1
ntp-perl-4.2.6p5-12.el6_9.1
ntp-4.2.6p5-12.el6_9.1

noarch
ntp-doc-4.2.6p5-12.el6_9.1

x86_64
ntpdate-4.2.6p5-12.el6_9.1
ntp-debuginfo-4.2.6p5-12.el6_9.1
ntp-perl-4.2.6p5-12.el6_9.1
ntp-4.2.6p5-12.el6_9.1

RHEL6WS
x86_64
ntpdate-4.2.6p5-12.el6_9.1
ntp-debuginfo-4.2.6p5-12.el6_9.1
ntp-4.2.6p5-12.el6_9.1

i386
ntpdate-4.2.6p5-12.el6_9.1
ntp-debuginfo-4.2.6p5-12.el6_9.1
ntp-4.2.6p5-12.el6_9.1

146024 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2899-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15232

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2899-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00115.html

SuSE Linux 42.2
x86_64
libjpeg8-devel-8.1.2-35.3.1
libjpeg62-debuginfo-62.2.0-35.3.1
libjpeg8-debuginfo-32bit-8.1.2-35.3.1
libjpeg62-32bit-62.2.0-35.3.1
libjpeg62-debuginfo-32bit-62.2.0-35.3.1
libjpeg62-62.2.0-35.3.1
libturbojpeg0-debuginfo-32bit-8.1.2-35.3.1
libjpeg8-8.1.2-35.3.1
libturbojpeg0-8.1.2-35.3.1
libjpeg62-devel-62.2.0-35.3.1
libjpeg8-32bit-8.1.2-35.3.1
libjpeg62-devel-32bit-62.2.0-35.3.1
libjpeg-turbo-1.5.2-35.3.1
libturbojpeg0-32bit-8.1.2-35.3.1
libturbojpeg0-debuginfo-8.1.2-35.3.1
libjpeg62-turbo-1.5.2-35.3.1
libjpeg8-devel-32bit-8.1.2-35.3.1
libjpeg8-debuginfo-8.1.2-35.3.1
libjpeg62-turbo-debugsource-1.5.2-35.3.1
libjpeg-turbo-debugsource-1.5.2-35.3.1
libjpeg-turbo-debuginfo-1.5.2-35.3.1

i586
libjpeg8-devel-8.1.2-35.3.1
libjpeg62-debuginfo-62.2.0-35.3.1
libjpeg62-62.2.0-35.3.1
libjpeg8-8.1.2-35.3.1
libturbojpeg0-8.1.2-35.3.1
libjpeg62-devel-62.2.0-35.3.1
libjpeg-turbo-1.5.2-35.3.1
libturbojpeg0-debuginfo-8.1.2-35.3.1
libjpeg62-turbo-1.5.2-35.3.1
libjpeg8-debuginfo-8.1.2-35.3.1
libjpeg62-turbo-debugsource-1.5.2-35.3.1
libjpeg-turbo-debugsource-1.5.2-35.3.1
libjpeg-turbo-debuginfo-1.5.2-35.3.1

SuSE Linux 42.3
x86_64
libjpeg62-32bit-62.2.0-38.1
libjpeg62-debuginfo-62.2.0-38.1
libjpeg62-debuginfo-32bit-62.2.0-38.1
libjpeg-turbo-1.5.2-38.1
libjpeg8-debuginfo-32bit-8.1.2-38.1
libjpeg8-debuginfo-8.1.2-38.1
libjpeg8-8.1.2-38.1
libturbojpeg0-debuginfo-32bit-8.1.2-38.1
libturbojpeg0-8.1.2-38.1
libjpeg62-devel-32bit-62.2.0-38.1
libjpeg-turbo-debugsource-1.5.2-38.1
libjpeg-turbo-debuginfo-1.5.2-38.1
libturbojpeg0-32bit-8.1.2-38.1
libturbojpeg0-debuginfo-8.1.2-38.1
libjpeg8-devel-8.1.2-38.1
libjpeg62-turbo-debugsource-1.5.2-38.1
libjpeg62-devel-62.2.0-38.1
libjpeg8-devel-32bit-8.1.2-38.1
libjpeg62-62.2.0-38.1
libjpeg62-turbo-1.5.2-38.1
libjpeg8-32bit-8.1.2-38.1

i586
libjpeg62-debuginfo-62.2.0-38.1
libjpeg-turbo-1.5.2-38.1
libjpeg8-debuginfo-8.1.2-38.1
libjpeg8-8.1.2-38.1
libturbojpeg0-8.1.2-38.1
libjpeg-turbo-debugsource-1.5.2-38.1
libjpeg-turbo-debuginfo-1.5.2-38.1
libturbojpeg0-debuginfo-8.1.2-38.1
libjpeg8-devel-8.1.2-38.1
libjpeg62-turbo-debugsource-1.5.2-38.1
libjpeg62-devel-62.2.0-38.1
libjpeg62-62.2.0-38.1
libjpeg62-turbo-1.5.2-38.1

160319 - CentOS 6 CESA-2017-3071 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
CESA-2017-3071

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/022608.html

CentOS 6
i686
ntp-perl-4.2.6p5-12.el6.centos.1
ntpdate-4.2.6p5-12.el6.centos.1
ntp-4.2.6p5-12.el6.centos.1

noarch
ntp-doc-4.2.6p5-12.el6.centos.1

x86_64
ntp-perl-4.2.6p5-12.el6.centos.1
ntpdate-4.2.6p5-12.el6.centos.1
ntp-4.2.6p5-12.el6.centos.1

175282 - Scientific Linux Security ERRATA Moderate: ntp on SL6.x i386/x86_64 (1710-18062)

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

Risk Level: Medium

CVE: CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ntp on SL6.x i386/x86_64 (1710-18062)

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=18062

SL6
i386
ntpdate-4.2.6p5-12.el6_9.1
ntp-debuginfo-4.2.6p5-12.el6_9.1
ntp-perl-4.2.6p5-12.el6_9.1
ntp-4.2.6p5-12.el6_9.1

noarch
ntp-doc-4.2.6p5-12.el6_9.1

x86_64
ntpdate-4.2.6p5-12.el6_9.1
ntp-debuginfo-4.2.6p5-12.el6_9.1
ntp-perl-4.2.6p5-12.el6_9.1
ntp-4.2.6p5-12.el6_9.1

192815 - Fedora Linux 25 FEDORA-2017-8761075ffd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15194

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8761075ffd

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

cacti-1.1.26-1.fc25

192837 - Fedora Linux 26 FEDORA-2017-ac20492c3e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15194

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ac20492c3e

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

cacti-1.1.26-1.fc26

22639 - (K74759095) F5 BIG-IP SafeNet External Network HSM Script Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2017-6165

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 safenet-sync.sc script. Successful exploitation could allow a local attacker to cause disclosure of information.

37586 - IBM AIX IV97811 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV97811

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV97811

7200-01
bos.acct < 7.2.1.1

37587 - IBM AIX IV97810 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV97810

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV97810

7200-00
bos.acct < 7.2.0.3

37588 - IBM AIX IV97356 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV97356

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV97356

6.1
bos.net.tcp.client < 6.1.9.300

37589 - IBM AIX IV97305 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV97305

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV97305

7.2
bos.net.tcp.client_core < 7.2.2.0

37590 - IBM AIX IV97396 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV97396

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV97396

7.1
bos.net.tcp.client < 7.1.5.0

37591 - IBM AIX IV96306 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV96306

Observation

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

For more information see:

http://www-01.ibm.com/support/docview.wss?uid=isg1IV96306

6.1
bos.net.tcp.client < 6.1.9.300

37592 - IBM AIX IV94723 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV94723

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV94723

7200-01
bos.net.tcp.tcpdump < 7.2.1.1

37593 - IBM AIX IV94724 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV94724

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV94724

7200-00
bos.net.tcp.tcpdump < 7.2.0.3

37594 - IBM AIX IV94726 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV94726

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV94726

7100-04
bos.net.tcp.server < 7.1.4.32

37595 - IBM AIX IV94728 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
IV94728

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=isg1IV94728

6.1
bos.net.tcp.server < 6.1.9.300

88892 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-300-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
SSA:2017-300-02

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.534644

Slackware 14.0
x86_64
wget-1.19.2-x86_64-1

Slackware 13.37
x86_64
wget-1.19.2-x86_64-1

Slackware 14.1
x86_64
wget-1.19.2-x86_64-1

Slackware 13.1
x86_64
wget-1.19.2-x86_64-1

Slackware 14.2
x86_64
wget-1.19.2-x86_64-1

i586
wget-1.19.2-i586-1

Slackware 13.0
x86_64
wget-1.19.2-x86_64-1

130916 - Debian Linux 8.0, 9.0 DSA-4011-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16227

Description

The scan detected that the host is missing the following update:
DSA-4011-1

Observation

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

http://www.debian.org/security/2017/dsa-4011

Debian 8.0
all
quagga_0.99.23.1-1+deb8u4

Debian 9.0
all
quagga_1.1.1-3+deb9u1

130917 - Debian Linux 8.0, 9.0 DSA-4008-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
DSA-4008-1

Observation

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

http://www.debian.org/security/2017/dsa-4008

Debian 8.0
all
wget_1.16-1+deb8u4

Debian 9.0
all
wget_1.18-5+deb9u1

130918 - Debian Linux 9.0 DSA-4009-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15924

Description

The scan detected that the host is missing the following update:
DSA-4009-1

Observation

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

http://www.debian.org/security/2017/dsa-4009

Debian 9.0
all
shadowsocks-libev_2.6.3+ds-3+deb9u1

130919 - Debian Linux 8.0, 9.0 DSA-4007-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000257

Description

The scan detected that the host is missing the following update:
DSA-4007-1

Observation

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

http://www.debian.org/security/2017/dsa-4007

Debian 8.0
all
curl_7.38.0-4+deb8u7

Debian 9.0
all
curl_7.52.1-5+deb9u2

141762 - Red Hat Enterprise Linux RHSA-2017-3107 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-3107

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/msg00045.html

RHEL6_5S
x86_64
redhat-release-server-6Server-6.5.0.3.el6_5.3

141764 - Red Hat Enterprise Linux RHSA-2017-3108 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-3108

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/msg00044.html

RHEL7_2S
x86_64
redhat-release-server-7.2-9.el7_2.3

182501 - FreeBSD Apache OpenOffice Multiple Vulnerabilities (27229c67-b8ff-11e7-9f79-ac9e174be3af)

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

Risk Level: Low

CVE: CVE-2017-12607, CVE-2017-12608, CVE-2017-3157, CVE-2017-9806

Description

The scan detected that the host is missing the following update:
Apache OpenOffice -- multiple vulnerabilities (27229c67-b8ff-11e7-9f79-ac9e174be3af)

Observation

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

http://www.vuxml.org/freebsd/27229c67-b8ff-11e7-9f79-ac9e174be3af.html

Affected packages:

apache-openoffice < 4.1.4
apache-openoffice-devel < 4.2.1810071_1,4

182502 - FreeBSD wget Heap Overflow In HTTP Protocol Handling (d77ceb8c-bb13-11e7-8357-3065ec6f3643)

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

Risk Level: Low

CVE: CVE-2017-13090

Description

The scan detected that the host is missing the following update:
wget -- Heap overflow in HTTP protocol handling (d77ceb8c-bb13-11e7-8357-3065ec6f3643)

Observation

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

http://www.vuxml.org/freebsd/d77ceb8c-bb13-11e7-8357-3065ec6f3643.html

Affected packages:
wget < 1.19.2

182503 - FreeBSD GitLab Multiple Vulnerabilities (418c172b-b96f-11e7-b627-d43d7e971a1b)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GitLab -- multiple vulnerabilities (418c172b-b96f-11e7-b627-d43d7e971a1b)

Observation

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

http://www.vuxml.org/freebsd/418c172b-b96f-11e7-b627-d43d7e971a1b.html

Affected packages:
2.8.0 <= gitlab <= 9.4.6
9.5.0 <= gitlab <= 9.5.8
10.0.0 <= gitlab <= 10.0.3

182504 - FreeBSD wget Stack Overflow In HTTP Protocol Handling (09849e71-bb12-11e7-8357-3065ec6f3643)

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

Risk Level: Low

CVE: CVE-2017-13089

Description

The scan detected that the host is missing the following update:
wget -- Stack overflow in HTTP protocol handling (09849e71-bb12-11e7-8357-3065ec6f3643)

Observation

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

http://www.vuxml.org/freebsd/09849e71-bb12-11e7-8357-3065ec6f3643.html

Affected packages:
wget < 1.19.2

182506 - FreeBSD chromium Stack Overflow In V8 (3cd46257-bbc5-11e7-a3bc-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-15396

Description

The scan detected that the host is missing the following update:
chromium -- Stack overflow in V8 (3cd46257-bbc5-11e7-a3bc-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/3cd46257-bbc5-11e7-a3bc-e8e0b747a45a.html

Affected packages:
chromium < 62.0.3202.75

182507 - FreeBSD Node.js Remote DOS Security Vulnerability (d7d1cc94-b971-11e7-af3a-f1035dd0da62)

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

Risk Level: Low

CVE: CVE-2017-14919

Description

The scan detected that the host is missing the following update:
Node.js -- remote DOS security vulnerability (d7d1cc94-b971-11e7-af3a-f1035dd0da62)

Observation

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

http://www.vuxml.org/freebsd/d7d1cc94-b971-11e7-af3a-f1035dd0da62.html

Affected packages:
node < 8.8.0
6.10.2 <= node6 < 6.11.5
4.8.2 <= node4 < 4.8.5

185944 - Ubuntu Linux 17.04, 17.10 USN-3466-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15908

Description

The scan detected that the host is missing the following update:
USN-3466-1

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/004113.html

Ubuntu 17.10

systemd_234-2ubuntu12.1

Ubuntu 17.04

systemd_232-21ubuntu7.1

192816 - Fedora Linux 26 FEDORA-2017-36eb36ea71 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-2017-36eb36ea71

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

procmail-3.22-44.fc26

192819 - Fedora Linux 25 FEDORA-2017-88a1f4854d 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-2017-88a1f4854d

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

sssd-1.15.3-5.fc25

192820 - Fedora Linux 26 FEDORA-2017-4a42419c16 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-2017-4a42419c16

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

libextractor-1.6-1.fc26

192824 - Fedora Linux 26 FEDORA-2017-2783ef2c63 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2783ef2c63

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

libXfont-1.5.2-5.fc26

192827 - Fedora Linux 26 FEDORA-2017-afb05e0873 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-afb05e0873

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

nodejs-forwarded-0.1.2-1.fc26

192828 - Fedora Linux 25 FEDORA-2017-8cca61e2fa 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-2017-8cca61e2fa

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

libextractor-1.6-1.fc25

192829 - Fedora Linux 25 FEDORA-2017-042c59fab9 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-2017-042c59fab9

Observation

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

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

Fedora Core 25

nodejs-forwarded-0.1.2-1.fc25

192830 - Fedora Linux 26 FEDORA-2017-845c543ea4 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-2017-845c543ea4

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

thunderbird-52.4.0-2.fc26

192832 - Fedora Linux 25 FEDORA-2017-52f233a4f5 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-2017-52f233a4f5

Observation

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

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

Fedora Core 25

procmail-3.22-44.fc25

192834 - Fedora Linux 26 FEDORA-2017-f44afd1f34 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-f44afd1f34

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

libXfont2-2.0.2-1.fc26

192835 - Fedora Linux 25 FEDORA-2017-b7c4334524 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b7c4334524

Observation

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

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

Fedora Core 25

libXfont-1.5.2-5.fc25

192836 - Fedora Linux 25 FEDORA-2017-5934ecf841 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-2017-5934ecf841

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

SDL2-2.0.5-8.fc25

146032 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2901-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-11671

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2901-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-10/msg00117.html

SuSE Linux 42.2
i586
libobjc4-4.8.5-23.3.2
gcc48-c++-4.8.5-23.3.2
gcc48-4.8.5-23.3.2
gcc48-objc-4.8.5-23.3.2
cpp48-4.8.5-23.3.2
libgcj48-debugsource-4.8.5-23.3.2
gcc48-java-debuginfo-4.8.5-23.3.2
libffi4-gcc48-debuginfo-4.8.5-23.3.1
gcc48-obj-c++-4.8.5-23.3.2
libgcj48-devel-debuginfo-4.8.5-23.3.2
gcc48-c++-debuginfo-4.8.5-23.3.2
libgcj48-jar-4.8.5-23.3.2
libasan0-debuginfo-4.8.5-23.3.2
gcc48-gij-4.8.5-23.3.2
gcc48-ada-4.8.5-23.3.2
gcc48-locale-4.8.5-23.3.2
gcc48-java-4.8.5-23.3.2
gcc48-fortran-4.8.5-23.3.2
libada48-4.8.5-23.3.2
gcc48-debugsource-4.8.5-23.3.2
libffi48-devel-4.8.5-23.3.1
gcc48-testresults-4.8.5-23.3.4
gcc48-fortran-debuginfo-4.8.5-23.3.2
libgcj48-4.8.5-23.3.2
libgcj48-debuginfo-4.8.5-23.3.2
gcc48-gij-debuginfo-4.8.5-23.3.2
libobjc4-debuginfo-4.8.5-23.3.2
libgcj_bc1-gcc48-4.8.5-23.3.2
gcc48-obj-c++-debuginfo-4.8.5-23.3.2
gcc48-ada-debuginfo-4.8.5-23.3.2
libffi4-gcc48-4.8.5-23.3.1
cpp48-debuginfo-4.8.5-23.3.2
gcc48-debuginfo-4.8.5-23.3.2
libasan0-4.8.5-23.3.2
libstdc++48-devel-4.8.5-23.3.2
gcc48-objc-debuginfo-4.8.5-23.3.2
libgcj48-devel-4.8.5-23.3.2
libada48-debuginfo-4.8.5-23.3.2
libffi48-debugsource-4.8.5-23.3.1

noarch
gcc48-info-4.8.5-23.3.2
libstdc++48-doc-4.8.5-23.3.2

x86_64
libobjc4-4.8.5-23.3.2
gcc48-gij-32bit-4.8.5-23.3.2
libffi4-gcc48-4.8.5-23.3.1
libffi4-gcc48-32bit-debuginfo-4.8.5-23.3.1
libgcj48-devel-4.8.5-23.3.2
libffi4-gcc48-debuginfo-4.8.5-23.3.1
cross-ppc-gcc48-icecream-backend-4.8.5-23.3.4
libgcj_bc1-gcc48-4.8.5-23.3.2
libasan0-debuginfo-4.8.5-23.3.2
gcc48-obj-c++-4.8.5-23.3.2
libffi4-gcc48-32bit-4.8.5-23.3.1

libada48-32bit-4.8.5-23.3.2
libada48-debuginfo-4.8.5-23.3.2
libgcj48-devel-32bit-4.8.5-23.3.2
libasan0-32bit-debuginfo-4.8.5-23.3.2
gcc48-fortran-32bit-4.8.5-23.3.2
cross-aarch64-gcc48-icecream-backend-4.8.5-23.3.4
libobjc4-32bit-debuginfo-4.8.5-23.3.2
gcc48-java-4.8.5-23.3.2
cross-ppc64-gcc48-icecream-backend-4.8.5-23.3.4
libstdc++48-devel-32bit-4.8.5-23.3.2
gcc48-gij-debuginfo-32bit-4.8.5-23.3.2
libasan0-4.8.5-23.3.2
libgcj48-devel-debuginfo-32bit-4.8.5-23.3.2
gcc48-debuginfo-4.8.5-23.3.2
libgcj48-debuginfo-4.8.5-23.3.2
cross-armv6hl-gcc48-icecream-backend-4.8.5-23.3.4
cross-armv7hl-gcc48-icecream-backend-4.8.5-23.3.4
gcc48-objc-4.8.5-23.3.2
cpp48-debuginfo-4.8.5-23.3.2
cross-s390x-gcc48-icecream-backend-4.8.5-23.3.4
gcc48-obj-c++-debuginfo-4.8.5-23.3.2
gcc48-ada-32bit-4.8.5-23.3.2
libgcj48-jar-4.8.5-23.3.2
libasan0-32bit-4.8.5-23.3.2
gcc48-4.8.5-23.3.2
gcc48-gij-4.8.5-23.3.2
libgcj48-devel-debuginfo-4.8.5-23.3.2
libffi48-debugsource-4.8.5-23.3.1
cross-ppc64le-gcc48-icecream-backend-4.8.5-23.3.4
cross-ia64-gcc48-icecream-backend-4.8.5-23.3.4
libffi48-devel-4.8.5-23.3.1
cross-s390-gcc48-icecream-backend-4.8.5-23.3.4
gcc48-32bit-4.8.5-23.3.2
gcc48-ada-4.8.5-23.3.2
libffi48-devel-32bit-4.8.5-23.3.1
libgcj48-4.8.5-23.3.2
gcc48-objc-32bit-4.8.5-23.3.2
gcc48-objc-debuginfo-4.8.5-23.3.2
libobjc4-debuginfo-4.8.5-23.3.2
libstdc++48-devel-4.8.5-23.3.2
libada48-4.8.5-23.3.2
libgcj48-debugsource-4.8.5-23.3.2
cross-i386-gcc48-icecream-backend-4.8.5-23.3.4
libgcj48-debuginfo-32bit-4.8.5-23.3.2
gcc48-fortran-debuginfo-4.8.5-23.3.2
gcc48-java-debuginfo-4.8.5-23.3.2
gcc48-fortran-4.8.5-23.3.2
gcc48-gij-debuginfo-4.8.5-23.3.2
cpp48-4.8.5-23.3.2
gcc48-testresults-4.8.5-23.3.4
libobjc4-32bit-4.8.5-23.3.2
libgcj48-32bit-4.8.5-23.3.2
gcc48-c++-debuginfo-4.8.5-23.3.2
gcc48-ada-debuginfo-4.8.5-23.3.2
libada48-32bit-debuginfo-4.8.5-23.3.2
gcc48-c++-4.8.5-23.3.2
gcc48-debugsource-4.8.5-23.3.2
gcc48-locale-4.8.5-23.3.2

SuSE Linux 42.3

i586
libobjc4-4.8.5-26.2
gcc48-objc-debuginfo-4.8.5-26.2
gcc48-testresults-4.8.5-26.4
libgcj48-4.8.5-26.2
gcc48-c++-4.8.5-26.2
gcc48-obj-c++-4.8.5-26.2
gcc48-c++-debuginfo-4.8.5-26.2
libgcj48-devel-4.8.5-26.2
libffi4-gcc48-4.8.5-26.1
libffi48-devel-4.8.5-26.1
libasan0-4.8.5-26.2
libffi4-gcc48-debuginfo-4.8.5-26.1
libgcj_bc1-4.8.5-26.2
libgcj48-debugsource-4.8.5-26.2
gcc48-java-debuginfo-4.8.5-26.2
libasan0-debuginfo-4.8.5-26.2
gcc48-gij-4.8.5-26.2
gcc48-4.8.5-26.2
gcc48-fortran-4.8.5-26.2
gcc48-objc-4.8.5-26.2
gcc48-ada-debuginfo-4.8.5-26.2
gcc48-locale-4.8.5-26.2
libgcj48-jar-4.8.5-26.2
libada48-4.8.5-26.2
gcc48-debugsource-4.8.5-26.2
gcc48-fortran-debuginfo-4.8.5-26.2
libgcj48-debuginfo-4.8.5-26.2
libffi48-debugsource-4.8.5-26.1
gcc48-debuginfo-4.8.5-26.2
libstdc++48-devel-4.8.5-26.2
gcc48-gij-debuginfo-4.8.5-26.2
cpp48-4.8.5-26.2
libada48-debuginfo-4.8.5-26.2
gcc48-java-4.8.5-26.2
gcc48-ada-4.8.5-26.2
gcc48-obj-c++-debuginfo-4.8.5-26.2
libobjc4-debuginfo-4.8.5-26.2
libgcj48-devel-debuginfo-4.8.5-26.2
cpp48-debuginfo-4.8.5-26.2

noarch
gcc48-info-4.8.5-26.2
libstdc++48-doc-4.8.5-26.2

x86_64
cross-i386-gcc48-icecream-backend-4.8.5-26.4
libstdc++48-devel-32bit-4.8.5-26.2
libobjc4-4.8.5-26.2
cross-s390-gcc48-icecream-backend-4.8.5-26.4
gcc48-objc-debuginfo-4.8.5-26.2
gcc48-gij-32bit-4.8.5-26.2
gcc48-objc-32bit-4.8.5-26.2
cross-s390x-gcc48-icecream-backend-4.8.5-26.4
libffi48-devel-32bit-4.8.5-26.1
libffi4-gcc48-32bit-4.8.5-26.1
gcc48-gij-debuginfo-32bit-4.8.5-26.2
cross-ppc64le-gcc48-icecream-backend-4.8.5-26.4
libgcj48-debuginfo-4.8.5-26.2
gcc48-java-debuginfo-4.8.5-26.2

gcc48-c++-debuginfo-4.8.5-26.2
libasan0-debuginfo-4.8.5-26.2
libasan0-32bit-debuginfo-4.8.5-26.2
gcc48-ada-32bit-4.8.5-26.2
gcc48-obj-c++-debuginfo-4.8.5-26.2
libffi4-gcc48-debuginfo-4.8.5-26.1
libffi4-gcc48-32bit-debuginfo-4.8.5-26.1
gcc48-obj-c++-4.8.5-26.2
libgcj_bc1-4.8.5-26.2
libgcj48-devel-debuginfo-32bit-4.8.5-26.2
libada48-32bit-4.8.5-26.2
gcc48-debugsource-4.8.5-26.2
libgcj48-32bit-4.8.5-26.2
libobjc4-32bit-debuginfo-4.8.5-26.2
libobjc4-debuginfo-4.8.5-26.2
libffi48-debugsource-4.8.5-26.1
gcc48-4.8.5-26.2
gcc48-32bit-4.8.5-26.2
cpp48-debuginfo-4.8.5-26.2
cross-ia64-gcc48-icecream-backend-4.8.5-26.4
libgcj48-jar-4.8.5-26.2
gcc48-gij-debuginfo-4.8.5-26.2
libffi48-devel-4.8.5-26.1
libgcj48-4.8.5-26.2
libasan0-4.8.5-26.2
libffi4-gcc48-4.8.5-26.1
libgcj48-devel-4.8.5-26.2
gcc48-fortran-debuginfo-4.8.5-26.2
libada48-debuginfo-4.8.5-26.2
cross-armv7hl-gcc48-icecream-backend-4.8.5-26.4
gcc48-gij-4.8.5-26.2
cross-ppc-gcc48-icecream-backend-4.8.5-26.4
libobjc4-32bit-4.8.5-26.2
libgcj48-devel-debuginfo-4.8.5-26.2
gcc48-debuginfo-4.8.5-26.2
cross-ppc64-gcc48-icecream-backend-4.8.5-26.4
cross-aarch64-gcc48-icecream-backend-4.8.5-26.4
libgcj48-debugsource-4.8.5-26.2
gcc48-ada-debuginfo-4.8.5-26.2
libasan0-32bit-4.8.5-26.2
libstdc++48-devel-4.8.5-26.2
libgcj48-devel-32bit-4.8.5-26.2
libada48-4.8.5-26.2
gcc48-java-4.8.5-26.2
libada48-32bit-debuginfo-4.8.5-26.2
gcc48-locale-4.8.5-26.2
libgcj48-debuginfo-32bit-4.8.5-26.2
cpp48-4.8.5-26.2
gcc48-fortran-32bit-4.8.5-26.2
gcc48-fortran-4.8.5-26.2
gcc48-objc-4.8.5-26.2
gcc48-c++-4.8.5-26.2
cross-armv6hl-gcc48-icecream-backend-4.8.5-26.4
gcc48-testresults-4.8.5-26.4
gcc48-ada-4.8.5-26.2

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.

160317 - CentOS 7 CESA-2017-2930 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS 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

Update Details

Risk is updated CVE is updated

22528 - (HT208142) Apple iCloud Vulnerabilities Prior To 7.0

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

Risk Level: High

CVE: CVE-2017-7081, CVE-2017-7087, CVE-2017-7089, CVE-2017-7090, CVE-2017-7091, CVE-2017-7092, CVE-2017-7093, CVE-2017-7094, CVE-2017-7095, CVE-2017-7096, CVE-2017-7098, CVE-2017-7099, CVE-2017-7100, CVE-2017-7102, CVE-2017-7104, CVE-2017-7106, CVE-2017-7107, CVE-2017-7109, CVE-2017-7111, CVE-2017-7117, CVE-2017-7120, CVE-2017-7127

Update Details

Risk is updated

21700 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 52.1

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2016-6354, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469

Update Details

CVE is updated

21701 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 52.1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2016-6354, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469

Update Details

CVE is updated

22481 - (SB10209) Threat Intelligence Exchange Server Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112

Update Details

Risk is updated

160308 - CentOS 7 CESA-2017-2836 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS 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 CVE is updated

160309 - CentOS 6 CESA-2017-2863 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7541

Update Details

Risk is updated CVE is updated

160310 - CentOS 6 CESA-2017-2860 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546

Update Details

Risk is updated CVE is updated

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

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

Risk Level: High

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

Update Details

CVE is updated

170845 - Amazon Linux AMI ALAS-2017-868 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112

Update Details

Risk is updated

181623 - FreeBSD OpenSMTPD Multiple Vulnerabilities (ee7bdf7f-11bb-4eea-b054-c692ab848c20)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-7687

Update Details
Risk is updated

185826 - Ubuntu Linux 17.04 USN-3384-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000111, CVE-2017-1000112

Update Details
Risk is updated

185828 - Ubuntu Linux 14.04 USN-3385-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000111, CVE-2017-1000112

Update Details
Risk is updated

185829 - Ubuntu Linux 16.04 USN-3385-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000111, CVE-2017-1000112

Update Details
Risk is updated

185831 - Ubuntu Linux 16.04 USN-3384-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000111, CVE-2017-1000112

Update Details
Risk is updated

185836 - Ubuntu Linux 12.04 USN-3386-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000111, CVE-2017-1000112

Update Details

Risk is updated

185838 - Ubuntu Linux 14.04 USN-3386-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112

Update Details

Risk is updated

189842 - Fedora Linux 22 FEDORA-2015-fd133d52cc Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7687

Update Details

Risk is updated

189900 - Fedora Linux 23 FEDORA-2015-ed1c673f09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7687

Update Details

Risk is updated

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

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

Risk Level: High

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

Update Details

Risk is updated

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

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

Risk Level: High

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

Update Details

Risk is updated

192810 - Fedora Linux 25 FEDORA-2017-8f7bca960b Update Is Not Installed

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

Risk Level: High
CVE: CVE-2017-15041, CVE-2017-15042

Update Details
Risk is updated

130852 - Debian Linux 8.0, 9.0 DSA-3934-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000117

Update Details
Risk is updated

141688 - Red Hat Enterprise Linux RHSA-2017-2485 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000117

Update Details
Risk is updated

141690 - Red Hat Enterprise Linux RHSA-2017-2484 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000117

Update Details
Risk is updated

145682 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:2320-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000117

Update Details
Risk is updated

145726 - SuSE Linux 42.2 openSUSE-SU-2017:2331-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000117

Update Details
Risk is updated

145886 - SuSE Linux 42.3 openSUSE-SU-2017:2182-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000117

Update Details

Risk is updated

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: Medium

CVE: CVE-2017-15056

Update Details

Risk is updated

160316 - CentOS 6, 7 CESA-2017-2998 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS 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

Update Details

Risk is updated CVE is updated

163443 - Oracle Enterprise Linux ELSA-2017-2484 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000117

Update Details

Risk is updated

163445 - Oracle Enterprise Linux ELSA-2017-2485 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000117

Update Details

Risk is updated

170859 - Amazon Linux AMI ALAS-2017-882 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000117

Update Details

Risk is updated

175231 - Scientific Linux Security ERRATA Important: git on SL6.x i386/x86_64 (1708-1146)

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

Risk Level: Medium

CVE: CVE-2017-1000117

Update Details

Risk is updated

175244 - Scientific Linux Security ERRATA Important: git on SL7.x x86_64 (1708-1798)

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

Risk Level: Medium

CVE: CVE-2017-1000117

Update Details

Risk is updated

185833 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3387-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000117

Update Details

Risk is updated

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

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

Risk Level: Medium

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

Update Details

Risk is updated

192514 - Fedora Linux 25 FEDORA-2017-8ba7572cfd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000117

Update Details

Risk is updated

192530 - Fedora Linux 26 FEDORA-2017-b1b3ae6666 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000117

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15056

Update Details
Risk is updated

192802 - Fedora Linux 25 FEDORA-2017-caafcbd6b9 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15056

Update Details
Risk is updated

192812 - Fedora Linux 26 FEDORA-2017-d22c391318 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15056

Update Details
Risk is updated

83846 - FreeBSD mediawiki Multiple Vulnerabilities (7c0fecd6-f42f-11e1-b17b-000c2977ec30)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2012-4377, CVE-2012-4378, CVE-2012-4379, CVE-2012-4380, CVE-2012-4381, CVE-2012-4382

Update Details
Risk is updated

144015 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1825-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7384

Update Details

Risk is updated

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: Medium

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

Update Details

Risk is updated

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

Category: SSH Module -> NonIntrusive -> Cent OS 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

Update Details

Risk is updated CVE is updated

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

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

Risk Level: Medium

CVE: CVE-2017-9798

Update Details

CVE is updated

160314 - CentOS 6 CESA-2017-2972 Update Is Not Installed

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

Risk Level: Medium

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

Update Details

CVE is updated

160315 - CentOS 6 CESA-2017-2911 Update Is Not Installed

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

Risk Level: Medium

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

Update Details

Risk is updated CVE is updated

182466 - FreeBSD cURL Out Of Bounds Read (ccace707-a8d8-11e7-ac58-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-1000254

Update Details

Risk is updated

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

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

Risk Level: Medium

CVE: CVE-2017-1000254

Update Details

Risk is updated

22495 - (HT208116) Apple Safari Multiple Vulnerabilities Prior To 11

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

Risk Level: Medium

CVE: CVE-2017-7085, CVE-2017-7089, CVE-2017-7106

Update Details

Risk is updated

22578 - (MSPT-Oct2017) Vulnerability in TPM could allow Security Feature Bypass (ADV170012)

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

Risk Level: Low

CVE: CVE-2017-15361

Update Details

Observation is updated CVE is updated FASLScript is updated

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

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

Risk Level: Low

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

Update Details

Risk is updated

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

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

Risk Level: Low

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

Update Details

Risk is updated

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

Update Details
Risk is updated

189072 - Fedora Linux 20 FEDORA-2015-4332 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2015-0296

Update Details
Risk is updated

189121 - Fedora Linux 21 FEDORA-2015-4872 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2015-0296

Update Details
Risk is updated

70114 - juniper.fasl3.inc

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

Update Details
FASLScript is updated

DELETED CHECKS

32831 - Oracle Solaris 145334-37 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-2015-2616

32839 - Oracle Solaris 145333-37 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-2015-2616

ADDITIONAL NOTES

- **32831** - was flagged as obsolete by the vendor.
- **32839** - was flagged as obsolete by the vendor.

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.