2018-FEB-22
FSL version 7.6.5

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

146400 - SuSE SLES 12 SP2 SUSE-SU-2018:0482-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15129, CVE-2017-17712, CVE-2017-17862, CVE-2017-17864, CVE-2017-18017, CVE-2017-5715, CVE-2018-1000004, CVE-2018-5332, CVE-2018-5333

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0482-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003742.html

SuSE SLES 12 SP2
x86_64
kernel-rt-devel-4.4.114-27.1
dlm-kmp-rt-4.4.114-27.1
kernel-syms-rt-4.4.114-27.1
cluster-md-kmp-rt-debuginfo-4.4.114-27.1
kernel-rt-debuginfo-4.4.114-27.1
ocfs2-kmp-rt-debuginfo-4.4.114-27.1
kernel-rt-4.4.114-27.1
kernel-rt_debug-debugsource-4.4.114-27.1
gfs2-kmp-rt-4.4.114-27.1
dlm-kmp-rt-debuginfo-4.4.114-27.1
cluster-network-kmp-rt-4.4.114-27.1
ocfs2-kmp-rt-4.4.114-27.1
kernel-rt-base-4.4.114-27.1
kernel-rt_debug-devel-debuginfo-4.4.114-27.1
kernel-rt-debugsource-4.4.114-27.1
cluster-network-kmp-rt-debuginfo-4.4.114-27.1
cluster-md-kmp-rt-4.4.114-27.1
kernel-rt_debug-debuginfo-4.4.114-27.1
kernel-rt_debug-devel-4.4.114-27.1
kernel-rt-base-debuginfo-4.4.114-27.1
gfs2-kmp-rt-debuginfo-4.4.114-27.1

noarch
kernel-devel-rt-4.4.114-27.1
kernel-source-rt-4.4.114-27.1

193289 - Fedora Linux 26 FEDORA-2018-a6b59d8f78 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4658, CVE-2016-5131, CVE-2017-8872, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050

Description

The scan detected that the host is missing the following update:
FEDORA-2018-a6b59d8f78

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/2018/2/?count=200&page=4

Fedora Core 26

libxml2-2.9.7-1.fc26

23136 - 3S CODESYS Web Server Vulnerability (ICSA-18-032-02)

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

Risk Level: High

CVE: CVE-2018-5440

Description

A vulnerability is present in some versions of 3S Software CODESYS Web Server.

Observation

3S CODESYS is used for programming and creating controller applications that are used across the energy, critical manufacturing, and industrial automation industries.

A vulnerability is present in some versions of 3S Software CODESYS Web Server. The flaw lies in an undetermined component. Successful exploitation could allow an attacker to cause a denial of service condition or execute remote code on the vulnerable system.

23143 - (HPESBHF03811) HPE Intelligent Management Center Multiple Remote Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-8984

Description

Multiple vulnerabilities are present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

Multiple vulnerabilities are present in some versions of HPE Intelligent Management Center. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22999 - (VMSA-2018-0005) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4949, CVE-2017-4950

Description

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

Observation

VMware Workstation is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Pro. The flaws lie in NAT service when IPv6 mode is enabled. Successful exploitation could allow an attacker to execute code in the targeted system.

23064 - Mozilla Firefox Multiple Vulnerabilities Prior To 58.0.1

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

Risk Level: High

CVE: CVE-2018-5124

Description

A vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox. The flaw lies in unsanitized output in the browser UI. Successful exploitation could allow an attacker to execute arbitrary code in the context of the user running the affected application

23065 - Mozilla Firefox Multiple Vulnerabilities Prior To 58.0.1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-5124

Description

A vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox. The flaw lies in unsanitized output in the browser UI. Successful exploitation could allow an attacker to execute arbitrary code in the context of the user running the affected application

23066 - Google Chrome Multiple Vulnerabilities Prior To 64.0.3282.140

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

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 cause unspecified attacks.

23067 - Google Chrome Multiple Vulnerabilities Prior To 64.0.3282.140

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

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 cause unspecified attacks.

23099 - (HPESBHF03797) HPE Integrated Lights-Out Multiple Remote Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-8979

Description

Multiple vulnerabilities are present in some versions of HPE Integrated Lights-Out.

Observation

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

Multiple vulnerabilities are present in some versions of HPE Integrated Lights-Out. The flaw lies in unknown components. Successful exploitation could allow a remote attacker to execute arbitrary code, cause a denial of service or bypass authentication security measure.

23120 - Apache Tomcat Vulnerability Prior To 8.0.48

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

Risk Level: High

CVE: CVE-2017-15706

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

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

A vulnerability is present in some versions of Apache Tomcat. The flaw lies in the search algorithm used by CGI Servlet. Successful exploitation could allow an attacker to execute scripts unexpectedly.

23124 - Apache Tomcat Vulnerability Prior To 8.5.24

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

Risk Level: High

CVE: CVE-2017-15706

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

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

A vulnerability is present in some versions of Apache Tomcat. The flaw lies in the CGI Servlet component. Successful exploitation could allow an attacker to cause undermined impact on the target system.

23138 - LibreOffice Remote Arbitrary File Disclosure Vulnerability

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

Risk Level: High

CVE: CVE-2018-6871

Description

An Arbitrary file disclosure vulnerability is present in some versions of LibreOffice.

Observation

LibreOffice is an open source office suite.

An Arbitrary file disclosure vulnerability is present in some versions of LibreOffice.The flaw lies in the WEBSERVICE function. Successful exploitation by an attacker could result in the disclosure of sensitive information.

23139 - LibreOffice Remote Arbitrary File Disclosure Vulnerability

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

Risk Level: High

CVE: CVE-2018-6871

Description

An Arbitrary file disclosure vulnerability is present in some versions of LibreOffice.

Observation

LibreOffice is an open source office suite.

An Arbitrary file disclosure vulnerability is present in some versions of LibreOffice.The flaw lies in the WEBSERVICE function. Successful exploitation by an attacker could result in the disclosure of sensitive information.

131021 - Debian Linux 9.0 DSA-4113-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14632, CVE-2017-14633

Description

The scan detected that the host is missing the following update:
DSA-4113-1

Observation

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

http://www.debian.org/security/2018/dsa-4113

Debian 9.0
all
libvorbis0a_1.3.5-4+deb9u1
libvorbis-dev_1.3.5-4+deb9u1
libvorbisfile3_1.3.5-4+deb9u1
libvorbis-dbg_1.3.5-4+deb9u1
libvorbisenc2_1.3.5-4+deb9u1

131023 - Debian Linux 8.0, 9.0 DSA-4114-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17485, CVE-2018-5968

Description

The scan detected that the host is missing the following update:
DSA-4114-1

Observation

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

http://www.debian.org/security/2018/dsa-4114

Debian 8.0
all
libjackson2-databind-java-doc_2.4.2-2+deb8u3
libjackson2-databind-java_2.4.2-2+deb8u3

Debian 9.0
all
libjackson2-databind-java-doc_2.8.6-1+deb9u3
libjackson2-databind-java_2.8.6-1+deb9u3

141871 - Red Hat Enterprise Linux RHSA-2018-0334 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6056

Description

The scan detected that the host is missing the following update:
RHSA-2018-0334

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-February/msg00020.html

RHEL6D
x86_64
chromium-browser-64.0.3282.167-1.el6_9
chromium-browser-debuginfo-64.0.3282.167-1.el6_9

i386
chromium-browser-64.0.3282.167-1.el6_9
chromium-browser-debuginfo-64.0.3282.167-1.el6_9

RHEL6S
x86_64
chromium-browser-64.0.3282.167-1.el6_9
chromium-browser-debuginfo-64.0.3282.167-1.el6_9

i386
chromium-browser-64.0.3282.167-1.el6_9
chromium-browser-debuginfo-64.0.3282.167-1.el6_9

RHEL6WS
x86_64
chromium-browser-64.0.3282.167-1.el6_9
chromium-browser-debuginfo-64.0.3282.167-1.el6_9

i386
chromium-browser-64.0.3282.167-1.el6_9
chromium-browser-debuginfo-64.0.3282.167-1.el6_9

146382 - SuSE Linux 42.3 openSUSE-SU-2018:0496-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11637, CVE-2017-11638, CVE-2017-11642, CVE-2017-14060, CVE-2017-17503

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0496-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00079.html

SuSE Linux 42.3
x86_64
perl-GraphicsMagick-1.3.25-71.1
libGraphicsMagickWand-Q16-2-1.3.25-71.1
GraphicsMagick-debuginfo-1.3.25-71.1
GraphicsMagick-devel-1.3.25-71.1
libGraphicsMagick++-Q16-12-1.3.25-71.1
libGraphicsMagick-Q16-3-1.3.25-71.1

libGraphicsMagick++-devel-1.3.25-71.1
GraphicsMagick-1.3.25-71.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-71.1
GraphicsMagick-debugsource-1.3.25-71.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-71.1
libGraphicsMagick3-config-1.3.25-71.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-71.1
perl-GraphicsMagick-debuginfo-1.3.25-71.1

i586
perl-GraphicsMagick-1.3.25-71.1
libGraphicsMagickWand-Q16-2-1.3.25-71.1
GraphicsMagick-debuginfo-1.3.25-71.1
GraphicsMagick-devel-1.3.25-71.1
libGraphicsMagick++-Q16-12-1.3.25-71.1
libGraphicsMagick-Q16-3-1.3.25-71.1
libGraphicsMagick++-devel-1.3.25-71.1
GraphicsMagick-1.3.25-71.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-71.1
GraphicsMagick-debugsource-1.3.25-71.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-71.1
libGraphicsMagick3-config-1.3.25-71.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-71.1
perl-GraphicsMagick-debuginfo-1.3.25-71.1

146383 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0507-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1053

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0507-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003746.html

SuSE SLES 12 SP2
noarch
postgresql96-docs-9.6.7-3.13.1

x86_64
postgresql96-debuginfo-9.6.7-3.13.1
libpq5-debuginfo-32bit-9.6.7-3.13.1
postgresql96-server-debuginfo-9.6.7-3.13.1
postgresql96-server-9.6.7-3.13.1
postgresql96-contrib-debuginfo-9.6.7-3.13.1
libpq5-debuginfo-9.6.7-3.13.1
libpq5-32bit-9.6.7-3.13.1
postgresql96-contrib-9.6.7-3.13.1
postgresql96-debugsource-9.6.7-3.13.1
postgresql96-9.6.7-3.13.1
postgresql96-libs-debugsource-9.6.7-3.13.1
libpq5-9.6.7-3.13.1

libecpg6-debuginfo-9.6.7-3.13.1
libecpg6-9.6.7-3.13.1

SuSE SLED 12 SP3
x86_64
libpq5-debuginfo-9.6.7-3.13.1
postgresql96-debugsource-9.6.7-3.13.1
libpq5-32bit-9.6.7-3.13.1
postgresql96-9.6.7-3.13.1
libpq5-9.6.7-3.13.1
postgresql96-libs-debugsource-9.6.7-3.13.1
postgresql96-debuginfo-9.6.7-3.13.1
libecpg6-9.6.7-3.13.1
libecpg6-debuginfo-9.6.7-3.13.1
libpq5-debuginfo-32bit-9.6.7-3.13.1

SuSE SLED 12 SP2
x86_64
libpq5-debuginfo-9.6.7-3.13.1
postgresql96-debugsource-9.6.7-3.13.1
libpq5-32bit-9.6.7-3.13.1
postgresql96-9.6.7-3.13.1
libpq5-9.6.7-3.13.1
postgresql96-libs-debugsource-9.6.7-3.13.1
postgresql96-debuginfo-9.6.7-3.13.1
libecpg6-9.6.7-3.13.1
libecpg6-debuginfo-9.6.7-3.13.1
libpq5-debuginfo-32bit-9.6.7-3.13.1

SuSE SLES 12 SP3
noarch
postgresql96-docs-9.6.7-3.13.1

x86_64
postgresql96-debuginfo-9.6.7-3.13.1
libpq5-debuginfo-32bit-9.6.7-3.13.1
postgresql96-server-debuginfo-9.6.7-3.13.1
postgresql96-server-9.6.7-3.13.1
postgresql96-contrib-debuginfo-9.6.7-3.13.1
libpq5-debuginfo-9.6.7-3.13.1
libpq5-32bit-9.6.7-3.13.1
postgresql96-contrib-9.6.7-3.13.1
postgresql96-debugsource-9.6.7-3.13.1
postgresql96-9.6.7-3.13.1
postgresql96-libs-debugsource-9.6.7-3.13.1
libpq5-9.6.7-3.13.1
libecpg6-debuginfo-9.6.7-3.13.1
libecpg6-9.6.7-3.13.1

146386 - SuSE Linux 42.3 openSUSE-SU-2018:0460-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11140, CVE-2017-11450, CVE-2017-11722, CVE-2017-14224, CVE-2017-17502, CVE-2017-17912, CVE-2017-18028

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0460-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00053.html

SuSE Linux 42.3
x86_64
libGraphicsMagick-Q16-3-1.3.25-68.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-68.1
libGraphicsMagick3-config-1.3.25-68.1
GraphicsMagick-1.3.25-68.1
GraphicsMagick-debugsource-1.3.25-68.1
GraphicsMagick-devel-1.3.25-68.1
perl-GraphicsMagick-debuginfo-1.3.25-68.1
libGraphicsMagickWand-Q16-2-1.3.25-68.1
libGraphicsMagick++-Q16-12-1.3.25-68.1
perl-GraphicsMagick-1.3.25-68.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-68.1
libGraphicsMagick++-devel-1.3.25-68.1
GraphicsMagick-debuginfo-1.3.25-68.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-68.1

i586
libGraphicsMagick-Q16-3-1.3.25-68.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-68.1
libGraphicsMagick3-config-1.3.25-68.1
GraphicsMagick-1.3.25-68.1
GraphicsMagick-debugsource-1.3.25-68.1
GraphicsMagick-devel-1.3.25-68.1
perl-GraphicsMagick-debuginfo-1.3.25-68.1
libGraphicsMagickWand-Q16-2-1.3.25-68.1
libGraphicsMagick++-Q16-12-1.3.25-68.1
perl-GraphicsMagick-1.3.25-68.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-68.1
libGraphicsMagick++-devel-1.3.25-68.1
GraphicsMagick-debuginfo-1.3.25-68.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-68.1

146387 - SuSE Linux 42.3 openSUSE-SU-2018:0471-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10689

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0471-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00058.html

SuSE Linux 42.3
i586

ruby2.3-rubygem-puppet-3.8.7-23.1
ruby2.3-rubygem-puppet-doc-3.8.7-23.1
rubygem-puppet-3.8.7-23.1
ruby2.1-rubygem-puppet-3.8.7-23.1
ruby2.4-rubygem-puppet-testsuite-3.8.7-23.1
rubygem-puppet-master-3.8.7-23.1
ruby2.4-rubygem-puppet-3.8.7-23.1
ruby2.3-rubygem-puppet-testsuite-3.8.7-23.1
ruby2.4-rubygem-puppet-doc-3.8.7-23.1
ruby2.1-rubygem-puppet-doc-3.8.7-23.1
ruby2.1-rubygem-puppet-testsuite-3.8.7-23.1
ruby2.2-rubygem-puppet-testsuite-3.8.7-23.1
ruby2.2-rubygem-puppet-doc-3.8.7-23.1
ruby2.2-rubygem-puppet-3.8.7-23.1

noarch
rubygem-puppet-emacs-3.8.7-23.1
rubygem-puppet-master-unicorn-3.8.7-23.1
rubygem-puppet-vim-3.8.7-23.1

x86_64
ruby2.3-rubygem-puppet-3.8.7-23.1
ruby2.3-rubygem-puppet-doc-3.8.7-23.1
rubygem-puppet-3.8.7-23.1
ruby2.1-rubygem-puppet-3.8.7-23.1
ruby2.4-rubygem-puppet-testsuite-3.8.7-23.1
rubygem-puppet-master-3.8.7-23.1
ruby2.4-rubygem-puppet-3.8.7-23.1
ruby2.3-rubygem-puppet-testsuite-3.8.7-23.1
ruby2.4-rubygem-puppet-doc-3.8.7-23.1
ruby2.1-rubygem-puppet-doc-3.8.7-23.1
ruby2.1-rubygem-puppet-testsuite-3.8.7-23.1
ruby2.2-rubygem-puppet-testsuite-3.8.7-23.1
ruby2.2-rubygem-puppet-doc-3.8.7-23.1
ruby2.2-rubygem-puppet-3.8.7-23.1

146389 - SuSE SLES 11 SP4 SUSE-SU-2018:0486-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11166, CVE-2017-11448, CVE-2017-11450, CVE-2017-11537, CVE-2017-11637, CVE-2017-11638, CVE-2017-11642, CVE-2017-12418, CVE-2017-12427, CVE-2017-12429, CVE-2017-12432, CVE-2017-12566, CVE-2017-12654, CVE-2017-12664, CVE-2017-12665, CVE-2017-12668, CVE-2017-12674, CVE-2017-13058, CVE-2017-13131, CVE-2017-14224, CVE-2017-17885, CVE-2017-18028, CVE-2017-9407, CVE-2018-6405

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0486-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003743.html

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.78.34.1

x86_64
libMagickCore1-32bit-6.4.3.6-7.78.34.1
libMagickCore1-6.4.3.6-7.78.34.1

146390 - SuSE Linux 42.3 openSUSE-SU-2018:0459-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15595, CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566, CVE-2017-18030, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-5683

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0459-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00052.html

SuSE Linux 42.3
x86_64
xen-libs-4.9.1_08-16.1
xen-devel-4.9.1_08-16.1
xen-tools-domU-debuginfo-4.9.1_08-16.1
xen-libs-debuginfo-4.9.1_08-16.1
xen-tools-debuginfo-4.9.1_08-16.1
xen-tools-4.9.1_08-16.1
xen-4.9.1_08-16.1
xen-doc-html-4.9.1_08-16.1
xen-tools-domU-4.9.1_08-16.1
xen-debugsource-4.9.1_08-16.1

146393 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0451-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12132, CVE-2017-8804, CVE-2018-1000001, CVE-2018-6485, CVE-2018-6551

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0451-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003732.html

SuSE SLES 12 SP2
noarch
glibc-html-2.22-62.6.2
glibc-info-2.22-62.6.2
glibc-i18ndata-2.22-62.6.2

x86_64
glibc-devel-debuginfo-32bit-2.22-62.6.2
nscd-2.22-62.6.2
glibc-debuginfo-32bit-2.22-62.6.2
glibc-32bit-2.22-62.6.2
glibc-devel-32bit-2.22-62.6.2
glibc-locale-32bit-2.22-62.6.2
glibc-debuginfo-2.22-62.6.2
glibc-devel-debuginfo-2.22-62.6.2
glibc-profile-2.22-62.6.2
nscd-debuginfo-2.22-62.6.2
glibc-locale-debuginfo-32bit-2.22-62.6.2
glibc-profile-32bit-2.22-62.6.2
glibc-2.22-62.6.2
glibc-devel-2.22-62.6.2
glibc-locale-debuginfo-2.22-62.6.2
glibc-debugsource-2.22-62.6.2
glibc-locale-2.22-62.6.2

SuSE SLED 12 SP3
x86_64
nscd-2.22-62.6.2
glibc-debuginfo-32bit-2.22-62.6.2
glibc-32bit-2.22-62.6.2
glibc-devel-32bit-2.22-62.6.2
glibc-locale-32bit-2.22-62.6.2
glibc-debuginfo-2.22-62.6.2
glibc-devel-debuginfo-2.22-62.6.2
nscd-debuginfo-2.22-62.6.2
glibc-devel-debuginfo-32bit-2.22-62.6.2
glibc-locale-debuginfo-32bit-2.22-62.6.2
glibc-2.22-62.6.2
glibc-devel-2.22-62.6.2
glibc-locale-debuginfo-2.22-62.6.2
glibc-debugsource-2.22-62.6.2
glibc-locale-2.22-62.6.2

noarch
glibc-i18ndata-2.22-62.6.2

SuSE SLED 12 SP2
x86_64
nscd-2.22-62.6.2
glibc-debuginfo-32bit-2.22-62.6.2
glibc-32bit-2.22-62.6.2
glibc-devel-32bit-2.22-62.6.2
glibc-locale-32bit-2.22-62.6.2
glibc-debuginfo-2.22-62.6.2
glibc-devel-debuginfo-2.22-62.6.2
nscd-debuginfo-2.22-62.6.2
glibc-devel-debuginfo-32bit-2.22-62.6.2
glibc-locale-debuginfo-32bit-2.22-62.6.2
glibc-2.22-62.6.2
glibc-devel-2.22-62.6.2
glibc-locale-debuginfo-2.22-62.6.2
glibc-debugsource-2.22-62.6.2
glibc-locale-2.22-62.6.2

noarch

glibc-i18ndata-2.22-62.6.2

SuSE SLES 12 SP3
noarch
glibc-html-2.22-62.6.2
glibc-info-2.22-62.6.2
glibc-i18ndata-2.22-62.6.2

x86_64
glibc-devel-debuginfo-32bit-2.22-62.6.2
nscd-2.22-62.6.2
glibc-debuginfo-32bit-2.22-62.6.2
glibc-32bit-2.22-62.6.2
glibc-devel-32bit-2.22-62.6.2
glibc-locale-32bit-2.22-62.6.2
glibc-debuginfo-2.22-62.6.2
glibc-devel-debuginfo-2.22-62.6.2
glibc-profile-2.22-62.6.2
nscd-debuginfo-2.22-62.6.2
glibc-locale-debuginfo-32bit-2.22-62.6.2
glibc-profile-32bit-2.22-62.6.2
glibc-2.22-62.6.2
glibc-devel-2.22-62.6.2
glibc-locale-debuginfo-2.22-62.6.2
glibc-debugsource-2.22-62.6.2
glibc-locale-2.22-62.6.2

146396 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0438-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15595, CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566, CVE-2017-18030, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-5683

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0438-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003729.html

SuSE SLED 12 SP3
x86_64
xen-libs-32bit-4.9.1_08-3.26.1
xen-libs-4.9.1_08-3.26.1
xen-libs-debuginfo-4.9.1_08-3.26.1
xen-libs-debuginfo-32bit-4.9.1_08-3.26.1
xen-4.9.1_08-3.26.1
xen-debugsource-4.9.1_08-3.26.1

SuSE SLES 12 SP3
x86_64
xen-libs-32bit-4.9.1_08-3.26.1
xen-libs-4.9.1_08-3.26.1
xen-doc-html-4.9.1_08-3.26.1

xen-libs-debuginfo-32bit-4.9.1_08-3.26.1
xen-tools-debuginfo-4.9.1_08-3.26.1
xen-tools-4.9.1_08-3.26.1
xen-4.9.1_08-3.26.1
xen-libs-debuginfo-4.9.1_08-3.26.1
xen-debugsource-4.9.1_08-3.26.1
xen-tools-domU-4.9.1_08-3.26.1
xen-tools-domU-debuginfo-4.9.1_08-3.26.1

146397 - SuSE Linux 42.3 openSUSE-SU-2018:0458-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306, CVE-2016-7052, CVE-2016-7055, CVE-2016-7056, CVE-2017-3731, CVE-2017-3732

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0458-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00051.html

SuSE Linux 42.3
x86_64
libopenssl1_0_0-steam-1.0.2k-4.3.1
libopenssl1_0_0-steam-32bit-1.0.2k-4.3.1
libopenssl1_0_0-steam-debuginfo-1.0.2k-4.3.1
openssl-steam-debugsource-1.0.2k-4.3.1
libopenssl1_0_0-steam-debuginfo-32bit-1.0.2k-4.3.1

i586
libopenssl1_0_0-steam-1.0.2k-4.3.1
libopenssl1_0_0-steam-debuginfo-1.0.2k-4.3.1
openssl-steam-debugsource-1.0.2k-4.3.1

146401 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0472-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15595, CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566, CVE-2017-18030, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-5683

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0472-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003741.html

SuSE SLED 12 SP2
x86_64
xen-libs-4.7.4_06-43.24.1
xen-debugsource-4.7.4_06-43.24.1
xen-libs-debuginfo-4.7.4_06-43.24.1
xen-libs-32bit-4.7.4_06-43.24.1
xen-libs-debuginfo-32bit-4.7.4_06-43.24.1
xen-4.7.4_06-43.24.1

SuSE SLES 12 SP2
x86_64
xen-tools-4.7.4_06-43.24.1
xen-libs-4.7.4_06-43.24.1
xen-doc-html-4.7.4_06-43.24.1
xen-debugsource-4.7.4_06-43.24.1
xen-tools-debuginfo-4.7.4_06-43.24.1
xen-libs-debuginfo-4.7.4_06-43.24.1
xen-libs-32bit-4.7.4_06-43.24.1
xen-tools-domU-4.7.4_06-43.24.1
xen-tools-domU-debuginfo-4.7.4_06-43.24.1
xen-libs-debuginfo-32bit-4.7.4_06-43.24.1
xen-4.7.4_06-43.24.1

146402 - SuSE SLES 11 SP4 SUSE-SU-2018:0465-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000035

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0465-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003738.html

SuSE SLES 11 SP4
i586
unzip-6.00-11.18.3.1

x86_64
unzip-6.00-11.18.3.1

146404 - SuSE SLES 11 SP4 SUSE-SU-2018:0462-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10244, CVE-2017-8105, CVE-2017-8287

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0462-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003736.html

SuSE SLES 11 SP4
i586
ft2demos-2.3.7-25.45.5.1
freetype2-2.3.7-25.45.5.1

x86_64
freetype2-32bit-2.3.7-25.45.5.1
ft2demos-2.3.7-25.45.5.1
freetype2-2.3.7-25.45.5.1

146405 - SuSE SLES 11 SP4 SUSE-SU-2018:0444-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3144

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0444-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003731.html

SuSE SLES 11 SP4
i586
dhcp-client-4.2.4.P2-0.28.5.3
dhcp-4.2.4.P2-0.28.5.3
dhcp-server-4.2.4.P2-0.28.5.3
dhcp-relay-4.2.4.P2-0.28.5.3

x86_64
dhcp-client-4.2.4.P2-0.28.5.3
dhcp-4.2.4.P2-0.28.5.3
dhcp-server-4.2.4.P2-0.28.5.3
dhcp-relay-4.2.4.P2-0.28.5.3

146406 - SuSE Linux 42.3 openSUSE-SU-2018:0468-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6789

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0468-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00055.html

SuSE Linux 42.3
x86_64
exim-debuginfo-4.86.2-20.1
eximon-4.86.2-20.1
eximon-debuginfo-4.86.2-20.1
exim-4.86.2-20.1
eximstats-html-4.86.2-20.1
exim-debugsource-4.86.2-20.1

146407 - SuSE Linux 42.3 openSUSE-SU-2018:0453-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6056

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0453-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00049.html

SuSE Linux 42.3
x86_64
chromium-64.0.3282.167-141.1
chromedriver-64.0.3282.167-141.1
chromedriver-debuginfo-64.0.3282.167-141.1
chromium-debugsource-64.0.3282.167-141.1
chromium-debuginfo-64.0.3282.167-141.1

146408 - SuSE Linux 42.3 openSUSE-SU-2018:0446-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6871

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0446-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00045.html

SuSE Linux 42.3
x86_64
libreoffice-base-5.4.5.1-15.1
libreoffice-writer-extensions-5.4.5.1-15.1
libreoffice-calc-5.4.5.1-15.1
libreoffice-base-drivers-postgresql-debuginfo-5.4.5.1-15.1
libreoffice-writer-5.4.5.1-15.1
libreoffice-impress-debuginfo-5.4.5.1-15.1
libreoffice-base-drivers-mysql-debuginfo-5.4.5.1-15.1
libreoffice-kde4-debuginfo-5.4.5.1-15.1
libreoffice-math-5.4.5.1-15.1
libreoffice-sdk-debuginfo-5.4.5.1-15.1
libreoffice-officebean-5.4.5.1-15.1
libreoffice-filters-optional-5.4.5.1-15.1
libreofficekit-5.4.5.1-15.1
libreoffice-5.4.5.1-15.1
libreoffice-gtk3-debuginfo-5.4.5.1-15.1
libreoffice-math-debuginfo-5.4.5.1-15.1
libreoffice-officebean-debuginfo-5.4.5.1-15.1
libreoffice-base-drivers-postgresql-5.4.5.1-15.1
libreoffice-kde4-5.4.5.1-15.1
libreoffice-impress-5.4.5.1-15.1
libreoffice-draw-5.4.5.1-15.1
libreoffice-mailmerge-5.4.5.1-15.1
libreoffice-debuginfo-5.4.5.1-15.1
libreoffice-gnome-5.4.5.1-15.1
libreoffice-base-drivers-mysql-5.4.5.1-15.1
libreoffice-pyuno-debuginfo-5.4.5.1-15.1
libreoffice-sdk-doc-5.4.5.1-15.1
libreoffice-gnome-debuginfo-5.4.5.1-15.1
libreoffice-debugsource-5.4.5.1-15.1
libreoffice-pyuno-5.4.5.1-15.1
libreoffice-base-debuginfo-5.4.5.1-15.1
libreofficekit-devel-5.4.5.1-15.1
libreoffice-draw-debuginfo-5.4.5.1-15.1
libreoffice-calc-extensions-5.4.5.1-15.1
libreoffice-sdk-5.4.5.1-15.1
libreoffice-calc-debuginfo-5.4.5.1-15.1
libreoffice-writer-debuginfo-5.4.5.1-15.1
libreoffice-gtk3-5.4.5.1-15.1

noarch
libreoffice-l10n-ro-5.4.5.1-15.1
libreoffice-l10n-sk-5.4.5.1-15.1
libreoffice-l10n-zh_CN-5.4.5.1-15.1
libreoffice-l10n-nl-5.4.5.1-15.1
libreoffice-l10n-zh_TW-5.4.5.1-15.1
libreoffice-l10n-sl-5.4.5.1-15.1
libreoffice-l10n-sr-5.4.5.1-15.1
libreoffice-l10n-ca-5.4.5.1-15.1
libreoffice-l10n-xh-5.4.5.1-15.1
libreoffice-l10n-eu-5.4.5.1-15.1
libreoffice-l10n-lv-5.4.5.1-15.1
libreoffice-l10n-hr-5.4.5.1-15.1
libreoffice-l10n-fi-5.4.5.1-15.1
libreoffice-l10n-hu-5.4.5.1-15.1
libreoffice-l10n-pt_PT-5.4.5.1-15.1
libreoffice-l10n-or-5.4.5.1-15.1
libreoffice-l10n-de-5.4.5.1-15.1
libreoffice-l10n-pt_BR-5.4.5.1-15.1

libreoffice-l10n-ko-5.4.5.1-15.1
libreoffice-l10n-bn-5.4.5.1-15.1
libreoffice-l10n-ga-5.4.5.1-15.1
libreoffice-l10n-nb-5.4.5.1-15.1
libreoffice-branding-upstream-5.4.5.1-15.1
libreoffice-l10n-nn-5.4.5.1-15.1
libreoffice-l10n-nso-5.4.5.1-15.1
libreoffice-l10n-af-5.4.5.1-15.1
libreoffice-l10n-br-5.4.5.1-15.1
libreoffice-l10n-ja-5.4.5.1-15.1
libreoffice-l10n-te-5.4.5.1-15.1
libreoffice-gdb-pretty-printers-5.4.5.1-15.1
libreoffice-l10n-bg-5.4.5.1-15.1
libreoffice-l10n-zu-5.4.5.1-15.1
libreoffice-l10n-gu-5.4.5.1-15.1
libreoffice-l10n-as-5.4.5.1-15.1
libreoffice-l10n-da-5.4.5.1-15.1
libreoffice-glade-5.4.5.1-15.1
libreoffice-l10n-th-5.4.5.1-15.1
libreoffice-l10n-si-5.4.5.1-15.1
libreoffice-icon-theme-sifr-5.4.5.1-15.1
libreoffice-l10n-ru-5.4.5.1-15.1
libreoffice-l10n-hi-5.4.5.1-15.1
libreoffice-l10n-ml-5.4.5.1-15.1
libreoffice-l10n-eo-5.4.5.1-15.1
libreoffice-l10n-et-5.4.5.1-15.1
libreoffice-l10n-tn-5.4.5.1-15.1
libreoffice-l10n-st-5.4.5.1-15.1
libreoffice-l10n-ta-5.4.5.1-15.1
libreoffice-icon-theme-hicontrast-5.4.5.1-15.1
libreoffice-l10n-ts-5.4.5.1-15.1
libreoffice-icon-theme-breeze-5.4.5.1-15.1
libreoffice-l10n-es-5.4.5.1-15.1
libreoffice-l10n-nr-5.4.5.1-15.1
libreoffice-l10n-tr-5.4.5.1-15.1
libreoffice-l10n-en-5.4.5.1-15.1
libreoffice-l10n-ve-5.4.5.1-15.1
libreoffice-l10n-pa-5.4.5.1-15.1
libreoffice-l10n-el-5.4.5.1-15.1
libreoffice-l10n-kk-5.4.5.1-15.1
libreoffice-l10n-kn-5.4.5.1-15.1
libreoffice-l10n-cy-5.4.5.1-15.1
libreoffice-l10n-cs-5.4.5.1-15.1
libreoffice-l10n-fa-5.4.5.1-15.1
libreoffice-l10n-gl-5.4.5.1-15.1
libreoffice-l10n-fr-5.4.5.1-15.1
libreoffice-l10n-he-5.4.5.1-15.1
libreoffice-l10n-lt-5.4.5.1-15.1
libreoffice-l10n-pl-5.4.5.1-15.1
libreoffice-l10n-ar-5.4.5.1-15.1
libreoffice-l10n-ss-5.4.5.1-15.1
libreoffice-l10n-sv-5.4.5.1-15.1
libreoffice-icon-theme-galaxy-5.4.5.1-15.1
libreoffice-l10n-uk-5.4.5.1-15.1
libreoffice-l10n-mr-5.4.5.1-15.1
libreoffice-icon-theme-tango-5.4.5.1-15.1
libreoffice-l10n-dz-5.4.5.1-15.1
libreoffice-l10n-mai-5.4.5.1-15.1
libreoffice-l10n-it-5.4.5.1-15.1

146410 - SuSE SLES 11 SP4 SUSE-SU-2018:0467-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0467-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003740.html

SuSE SLES 11 SP4
i586
gtk2-2.18.9-0.45.3.1
gtk2-lang-2.18.9-0.45.3.1
gtk2-doc-2.18.9-0.45.3.1

x86_64
gtk2-2.18.9-0.45.3.1
gtk2-32bit-2.18.9-0.45.3.1
gtk2-lang-2.18.9-0.45.3.1
gtk2-doc-2.18.9-0.45.3.1

146413 - SuSE Linux 42.3 openSUSE-SU-2018:0476-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15186, CVE-2017-15672, CVE-2017-16840, CVE-2017-17081, CVE-2017-17555, CVE-2018-6392, CVE-2018-6621

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0476-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00062.html

SuSE Linux 42.3
x86_64
libavresample-devel-3.4.2-10.1
libavcodec-devel-3.4.2-10.1
libavformat57-debuginfo-32bit-3.4.2-10.1
libavcodec57-debuginfo-32bit-3.4.2-10.1
libpostproc54-debuginfo-3.4.2-10.1
ffmpeg-debuginfo-3.4.2-10.1
libavformat57-32bit-3.4.2-10.1
libswscale4-3.4.2-10.1
libpostproc54-3.4.2-10.1

libswscale-devel-3.4.2-10.1
libavcodec57-32bit-3.4.2-10.1
libavresample3-32bit-3.4.2-10.1
libavdevice-devel-3.4.2-10.1
libswresample-devel-3.4.2-10.1
libavdevice57-3.4.2-10.1
libavresample3-3.4.2-10.1
libswscale4-32bit-3.4.2-10.1
libswresample2-3.4.2-10.1
libavutil55-3.4.2-10.1
libavcodec57-debuginfo-3.4.2-10.1
libavutil55-debuginfo-3.4.2-10.1
libavutil-devel-3.4.2-10.1
libavfilter6-debuginfo-32bit-3.4.2-10.1
libswscale4-debuginfo-32bit-3.4.2-10.1
libswresample2-debuginfo-3.4.2-10.1
libavdevice57-32bit-3.4.2-10.1
libavfilter-devel-3.4.2-10.1
libavresample3-debuginfo-3.4.2-10.1
libswresample2-debuginfo-32bit-3.4.2-10.1
libavcodec57-3.4.2-10.1
libpostproc-devel-3.4.2-10.1
libavutil55-debuginfo-32bit-3.4.2-10.1
libavformat57-debuginfo-3.4.2-10.1
libswscale4-debuginfo-3.4.2-10.1
libavfilter6-32bit-3.4.2-10.1
libpostproc54-debuginfo-32bit-3.4.2-10.1
libswresample2-32bit-3.4.2-10.1
ffmpeg-debugsource-3.4.2-10.1
libavdevice57-debuginfo-3.4.2-10.1
libavutil55-32bit-3.4.2-10.1
libpostproc54-32bit-3.4.2-10.1
libavformat57-3.4.2-10.1
libavfilter6-3.4.2-10.1
libavformat-devel-3.4.2-10.1
ffmpeg-3.4.2-10.1
libavdevice57-debuginfo-32bit-3.4.2-10.1
libavresample3-debuginfo-32bit-3.4.2-10.1
libavfilter6-debuginfo-3.4.2-10.1

i586
libavresample-devel-3.4.2-10.1
libavcodec-devel-3.4.2-10.1
libpostproc54-debuginfo-3.4.2-10.1
ffmpeg-debuginfo-3.4.2-10.1
libswscale4-3.4.2-10.1
libpostproc54-3.4.2-10.1
libswscale-devel-3.4.2-10.1
libavdevice-devel-3.4.2-10.1
libswresample-devel-3.4.2-10.1
libavdevice57-3.4.2-10.1
libavresample3-3.4.2-10.1
libswresample2-3.4.2-10.1
libavutil55-3.4.2-10.1
libavcodec57-debuginfo-3.4.2-10.1
libavutil55-debuginfo-3.4.2-10.1
libavutil-devel-3.4.2-10.1
libswresample2-debuginfo-3.4.2-10.1
libavfilter-devel-3.4.2-10.1
libavresample3-debuginfo-3.4.2-10.1

libavcodec57-3.4.2-10.1
libpostproc-devel-3.4.2-10.1
libavformat57-debuginfo-3.4.2-10.1
libswscale4-debuginfo-3.4.2-10.1
ffmpeg-debugsource-3.4.2-10.1
libavdevice57-debuginfo-3.4.2-10.1
libavformat57-3.4.2-10.1
libavfilter6-3.4.2-10.1
libavformat-devel-3.4.2-10.1
ffmpeg-3.4.2-10.1
libavfilter6-debuginfo-3.4.2-10.1

146414 - SuSE SLES 11 SP4 SUSE-SU-2018:0457-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16227, CVE-2017-5495, CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0457-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003735.html

SuSE SLES 11 SP4
i586
quagga-0.99.15-0.30.3.1

x86_64
quagga-0.99.15-0.30.3.1

146415 - SuSE Linux 42.3 openSUSE-SU-2018:0475-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7050, CVE-2018-7051, CVE-2018-7052, CVE-2018-7053, CVE-2018-7054

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0475-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00061.html

SuSE Linux 42.3
x86_64
irssi-1.0.7-25.1
irssi-devel-1.0.7-25.1
irssi-debuginfo-1.0.7-25.1

irssi-debugsource-1.0.7-25.1

i586
irssi-1.0.7-25.1
irssi-devel-1.0.7-25.1
irssi-debuginfo-1.0.7-25.1
irssi-debugsource-1.0.7-25.1

146416 - SuSE Linux 42.3 openSUSE-SU-2018:0494-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12132, CVE-2017-8804, CVE-2018-1000001, CVE-2018-6485, CVE-2018-6551

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0494-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00078.html

SuSE Linux 42.3
i586
nscd-debuginfo-2.22-13.2
glibc-extra-debuginfo-2.22-13.2
glibc-profile-2.22-13.2
glibc-utils-2.22-13.2
glibc-obsolete-debuginfo-2.22-13.2
nscd-2.22-13.2
glibc-2.22-13.2
glibc-obsolete-2.22-13.2
glibc-utils-debugsource-2.22-13.2
glibc-extra-2.22-13.2
glibc-devel-2.22-13.2
glibc-locale-debuginfo-2.22-13.2
glibc-devel-debuginfo-2.22-13.2
glibc-debuginfo-2.22-13.2
glibc-devel-static-2.22-13.2
glibc-debugsource-2.22-13.2
glibc-utils-debuginfo-2.22-13.2
glibc-locale-2.22-13.2

i686
glibc-debugsource-2.22-13.2
glibc-2.22-13.2
glibc-locale-debuginfo-2.22-13.2
glibc-profile-2.22-13.2
glibc-debuginfo-2.22-13.2
glibc-locale-2.22-13.2
glibc-devel-static-2.22-13.2
glibc-devel-debuginfo-2.22-13.2
glibc-devel-2.22-13.2

noarch
glibc-i18ndata-2.22-13.2

glibc-info-2.22-13.2
glibc-html-2.22-13.2

x86_64
nscd-debuginfo-2.22-13.2
glibc-extra-debuginfo-2.22-13.2
glibc-profile-2.22-13.2
glibc-utils-2.22-13.2
glibc-32bit-2.22-13.2
glibc-utils-32bit-2.22-13.2
glibc-profile-32bit-2.22-13.2
nscd-2.22-13.2
glibc-2.22-13.2
glibc-utils-debuginfo-32bit-2.22-13.2
glibc-utils-debugsource-2.22-13.2
glibc-extra-2.22-13.2
glibc-devel-debuginfo-32bit-2.22-13.2
glibc-locale-32bit-2.22-13.2
glibc-devel-2.22-13.2
glibc-locale-debuginfo-2.22-13.2
glibc-devel-32bit-2.22-13.2
glibc-devel-debuginfo-2.22-13.2
glibc-debuginfo-2.22-13.2
glibc-devel-static-2.22-13.2
glibc-debugsource-2.22-13.2
glibc-debuginfo-32bit-2.22-13.2
glibc-locale-debuginfo-32bit-2.22-13.2
glibc-devel-static-32bit-2.22-13.2
glibc-utils-debuginfo-2.22-13.2
glibc-locale-2.22-13.2

146417 - SuSE SLED 12 SP3 SUSE-SU-2018:0443-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6871

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0443-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003730.html

SuSE SLED 12 SP3
x86_64
libreoffice-impress-5.4.5.1-43.19.1
libreoffice-pyuno-debuginfo-5.4.5.1-43.19.1
libreoffice-draw-5.4.5.1-43.19.1
libreoffice-calc-extensions-5.4.5.1-43.19.1
libreoffice-5.4.5.1-43.19.1
libreoffice-base-drivers-mysql-5.4.5.1-43.19.1
libreoffice-officebean-5.4.5.1-43.19.1
libreoffice-writer-extensions-5.4.5.1-43.19.1
libreoffice-base-debuginfo-5.4.5.1-43.19.1

libreoffice-impress-debuginfo-5.4.5.1-43.19.1
libreoffice-calc-5.4.5.1-43.19.1
libreoffice-base-drivers-mysql-debuginfo-5.4.5.1-43.19.1
libreoffice-math-5.4.5.1-43.19.1
libreoffice-debuginfo-5.4.5.1-43.19.1
libreoffice-draw-debuginfo-5.4.5.1-43.19.1
libreoffice-math-debuginfo-5.4.5.1-43.19.1
libreofficekit-5.4.5.1-43.19.1
libreoffice-base-drivers-postgresql-5.4.5.1-43.19.1
libreoffice-calc-debuginfo-5.4.5.1-43.19.1
libreoffice-base-5.4.5.1-43.19.1
libreoffice-writer-5.4.5.1-43.19.1
libreoffice-pyuno-5.4.5.1-43.19.1
libreoffice-officebean-debuginfo-5.4.5.1-43.19.1
libreoffice-gnome-debuginfo-5.4.5.1-43.19.1
libreoffice-debugsource-5.4.5.1-43.19.1
libreoffice-filters-optional-5.4.5.1-43.19.1
libreoffice-writer-debuginfo-5.4.5.1-43.19.1
libreoffice-base-drivers-postgresql-debuginfo-5.4.5.1-43.19.1
libreoffice-gnome-5.4.5.1-43.19.1
libreoffice-mailmerge-5.4.5.1-43.19.1

noarch
libreoffice-l10n-uk-5.4.5.1-43.19.1
libreoffice-l10n-pt_PT-5.4.5.1-43.19.1
libreoffice-l10n-it-5.4.5.1-43.19.1
libreoffice-l10n-sk-5.4.5.1-43.19.1
libreoffice-l10n-fr-5.4.5.1-43.19.1
libreoffice-l10n-de-5.4.5.1-43.19.1
libreoffice-l10n-es-5.4.5.1-43.19.1
libreoffice-l10n-zh_TW-5.4.5.1-43.19.1
libreoffice-l10n-hr-5.4.5.1-43.19.1
libreoffice-l10n-da-5.4.5.1-43.19.1
libreoffice-l10n-fi-5.4.5.1-43.19.1
libreoffice-l10n-xh-5.4.5.1-43.19.1
libreoffice-icon-theme-tango-5.4.5.1-43.19.1
libreoffice-l10n-cs-5.4.5.1-43.19.1
libreoffice-l10n-ro-5.4.5.1-43.19.1
libreoffice-l10n-lt-5.4.5.1-43.19.1
libreoffice-l10n-pl-5.4.5.1-43.19.1
libreoffice-l10n-sv-5.4.5.1-43.19.1
libreoffice-l10n-gu-5.4.5.1-43.19.1
libreoffice-l10n-nb-5.4.5.1-43.19.1
libreoffice-icon-theme-galaxy-5.4.5.1-43.19.1
libreoffice-l10n-af-5.4.5.1-43.19.1
libreoffice-l10n-hi-5.4.5.1-43.19.1
libreoffice-l10n-zh_CN-5.4.5.1-43.19.1
libreoffice-l10n-pt_BR-5.4.5.1-43.19.1
libreoffice-l10n-ca-5.4.5.1-43.19.1
libreoffice-l10n-en-5.4.5.1-43.19.1
libreoffice-l10n-zu-5.4.5.1-43.19.1
libreoffice-l10n-ar-5.4.5.1-43.19.1
libreoffice-l10n-ja-5.4.5.1-43.19.1
libreoffice-l10n-ko-5.4.5.1-43.19.1
libreoffice-l10n-ru-5.4.5.1-43.19.1
libreoffice-l10n-nl-5.4.5.1-43.19.1
libreoffice-l10n-nn-5.4.5.1-43.19.1
libreoffice-l10n-bg-5.4.5.1-43.19.1
libreoffice-l10n-hu-5.4.5.1-43.19.1

146418 - SuSE Linux 42.3 openSUSE-SU-2018:0461-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000051

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0461-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00054.html

SuSE Linux 42.3
x86_64
mupdf-devel-static-1.12.0-31.1
mupdf-1.12.0-31.1

i586
mupdf-devel-static-1.12.0-31.1
mupdf-1.12.0-31.1

146419 - SuSE Linux 42.3 openSUSE-SU-2018:0491-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18187, CVE-2018-0487, CVE-2018-0488

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0491-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00075.html

SuSE Linux 42.3
x86_64
libmbedtls9-32bit-1.3.19-21.1
libmbedtls9-1.3.19-21.1
libmbedtls9-debuginfo-1.3.19-21.1
mbedtls-devel-1.3.19-21.1
mbedtls-debugsource-1.3.19-21.1
libmbedtls9-debuginfo-32bit-1.3.19-21.1

i586
libmbedtls9-debuginfo-1.3.19-21.1
mbedtls-devel-1.3.19-21.1
mbedtls-debugsource-1.3.19-21.1
libmbedtls9-1.3.19-21.1

146420 - SuSE SLES 11 SP4 SUSE-SU-2018:0506-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1053

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0506-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003745.html

SuSE SLES 11 SP4
i586
postgresql94-server-9.4.16-0.23.13.2
libecpg6-9.4.16-0.23.13.2
postgresql94-9.4.16-0.23.13.2
libpq5-9.4.16-0.23.13.2
postgresql94-contrib-9.4.16-0.23.13.2
postgresql94-docs-9.4.16-0.23.13.2

x86_64
postgresql94-server-9.4.16-0.23.13.2
libpq5-32bit-9.4.16-0.23.13.2
libecpg6-9.4.16-0.23.13.2
postgresql94-9.4.16-0.23.13.2
libpq5-9.4.16-0.23.13.2
postgresql94-contrib-9.4.16-0.23.13.2
postgresql94-docs-9.4.16-0.23.13.2

178584 - Gentoo Linux GLSA-201802-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201802-04

Observation

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

https://security.gentoo.org/glsa/201802-04

Affected packages:
dev-db/mysql < 5.6.39

178585 - Gentoo Linux GLSA-201802-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201802-03

Observation

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

https://security.gentoo.org/glsa/201802-03

Affected packages:
www-client/firefox < 52.6.0
www-client/firefox-bin < 52.6.0

186101 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3575-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11334, CVE-2017-13672, CVE-2017-14167, CVE-2017-15038, CVE-2017-15118, CVE-2017-15119, CVE-2017-15124, CVE-2017-15268, CVE-2017-15289, CVE-2017-16845, CVE-2017-17381, CVE-2017-18043, CVE-2018-5683

Description

The scan detected that the host is missing the following update:
USN-3575-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004284.html

Ubuntu 16.04

qemu-system_2.5+dfsg-5ubuntu10.22
qemu-system-ppc_2.5+dfsg-5ubuntu10.22
qemu-system-s390x_2.5+dfsg-5ubuntu10.22
qemu-system-misc_2.5+dfsg-5ubuntu10.22
qemu-system-mips_2.5+dfsg-5ubuntu10.22
qemu-system-aarch64_2.5+dfsg-5ubuntu10.22
qemu-system-x86_2.5+dfsg-5ubuntu10.22
qemu-system-sparc_2.5+dfsg-5ubuntu10.22
qemu-system-arm_2.5+dfsg-5ubuntu10.22

Ubuntu 14.04

qemu-system-ppc_2.0.0+dfsg-2ubuntu1.39
qemu-system-mips_2.0.0+dfsg-2ubuntu1.39
qemu-system-x86_2.0.0+dfsg-2ubuntu1.39
qemu-system-arm_2.0.0+dfsg-2ubuntu1.39
qemu-system-aarch64_2.0.0+dfsg-2ubuntu1.39
qemu-system-misc_2.0.0+dfsg-2ubuntu1.39
qemu-system-sparc_2.0.0+dfsg-2ubuntu1.39
qemu-system_2.0.0+dfsg-2ubuntu1.39

Ubuntu 17.10

qemu-system-s390x_2.10+dfsg-0ubuntu3.5
qemu-system-misc_2.10+dfsg-0ubuntu3.5
qemu-system_2.10+dfsg-0ubuntu3.5
qemu-system-aarch64_2.10+dfsg-0ubuntu3.5
qemu-system-arm_2.10+dfsg-0ubuntu3.5
qemu-system-sparc_2.10+dfsg-0ubuntu3.5
qemu-system-x86_2.10+dfsg-0ubuntu3.5
qemu-system-ppc_2.10+dfsg-0ubuntu3.5
qemu-system-mips_2.10+dfsg-0ubuntu3.5

186104 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3571-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1693, CVE-2015-2774, CVE-2016-10253, CVE-2017-1000385

Description

The scan detected that the host is missing the following update:
USN-3571-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004279.html

Ubuntu 16.04

erlang_18.3-dfsg-1ubuntu3.1

Ubuntu 14.04

erlang_16.b.3-dfsg-1ubuntu2.2

Ubuntu 17.10

erlang_20.0.4+dfsg-1ubuntu1.1

193283 - Fedora Linux 26 FEDORA-2018-0db545e976 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0903

Description

The scan detected that the host is missing the following update:
FEDORA-2018-0db545e976

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/2018/2/?count=200&page=2

Fedora Core 26

ruby-2.4.3-86.fc26

23121 - Apache Tomcat Vulnerability Prior To 9.0.2

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

Risk Level: Medium

CVE: CVE-2017-15706

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

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

A vulnerability is present in some versions of Apache Tomcat. The flaw lies in the search algorithm used by CGI Servlet. Successful exploitation could allow an attacker to execute scripts unexpectedly.

23140 - IBM WebSphere Portal Cross-Site Scripting Vulnerability (swg22012416)

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

Risk Level: Medium

CVE: CVE-2017-1761

Description

A cross-site-scripting vulnerability is present in some versions of IBM WebSphere Portal.

Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

A cross-site-scripting vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in Web UI. Successful exploitation could allow an attacker to obtain sensitive information.

23141 - IBM WebSphere Portal Cross-Site Scripting Vulnerability (swg22013097)

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

Risk Level: Medium

CVE: CVE-2018-1401

Description

A cross-site-scripting vulnerability is present in some versions of IBM WebSphere Portal.

Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

A cross-site-scripting vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in Web UI. Successful exploitation could allow an attacker to obtain sensitive information.

131027 - Debian Linux 9.0 DSA-4112-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566

Description

The scan detected that the host is missing the following update:
DSA-4112-1

Observation

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

http://www.debian.org/security/2018/dsa-4112

Debian 9.0
all
xen-utils-4.8_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
libxenstore3.0_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
libxen-4.8_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
xenstore-utils_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
xen-hypervisor-4.8-arm64_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
xen-hypervisor-4.8-armhf_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
xen-system-arm64_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
xen-hypervisor-4.8-amd64_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
libxen-dev_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
xen-system-amd64_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
xen-system-armhf_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1
xen-utils-common_4.8.3+comet2+shim4.10.0+comet3-1+deb9u4.1

146388 - SuSE Linux 42.3 openSUSE-SU-2018:0490-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2887

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0490-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00074.html

SuSE Linux 42.3
x86_64
libSDL2_image-2_0-0-debuginfo-32bit-2.0.0-13.7.1
SDL_image-debugsource-1.2.12-16.3.1
libSDL_image-1_2-0-debuginfo-32bit-1.2.12-16.3.1
libSDL_image-1_2-0-1.2.12-16.3.1
libSDL2_image-2_0-0-32bit-2.0.0-13.7.1
libSDL2_image-2_0-0-2.0.0-13.7.1
libSDL2_image-devel-32bit-2.0.0-13.7.1
SDL2_image-debugsource-2.0.0-13.7.1
libSDL2_image-devel-2.0.0-13.7.1

libSDL_image-devel-1.2.12-16.3.1
libSDL_image-1_2-0-debuginfo-1.2.12-16.3.1
libSDL_image-1_2-0-32bit-1.2.12-16.3.1
libSDL_image-devel-32bit-1.2.12-16.3.1
libSDL2_image-2_0-0-debuginfo-2.0.0-13.7.1

i586
libSDL2_image-2_0-0-2.0.0-13.7.1
libSDL_image-1_2-0-1.2.12-16.3.1
libSDL2_image-devel-2.0.0-13.7.1
SDL_image-debugsource-1.2.12-16.3.1
SDL2_image-debugsource-2.0.0-13.7.1
libSDL2_image-2_0-0-debuginfo-2.0.0-13.7.1
libSDL_image-1_2-0-debuginfo-1.2.12-16.3.1
libSDL_image-devel-1.2.12-16.3.1

146398 - SuSE Linux 42.3 openSUSE-SU-2018:0497-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1372, CVE-2017-17969, CVE-2018-5996

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0497-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00080.html

SuSE Linux 42.3
x86_64
p7zip-9.20.1-18.3.1
p7zip-debuginfo-9.20.1-18.3.1
p7zip-debugsource-9.20.1-18.3.1

i586
p7zip-9.20.1-18.3.1
p7zip-debuginfo-9.20.1-18.3.1
p7zip-debugsource-9.20.1-18.3.1

146399 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0464-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1372, CVE-2017-17969, CVE-2018-5996

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0464-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003737.html

SuSE SLES 12 SP2
x86_64
p7zip-debuginfo-9.20.1-7.3.1
p7zip-debugsource-9.20.1-7.3.1
p7zip-9.20.1-7.3.1

SuSE SLED 12 SP3
x86_64
p7zip-debuginfo-9.20.1-7.3.1
p7zip-debugsource-9.20.1-7.3.1
p7zip-9.20.1-7.3.1

SuSE SLED 12 SP2
x86_64
p7zip-debuginfo-9.20.1-7.3.1
p7zip-debugsource-9.20.1-7.3.1
p7zip-9.20.1-7.3.1

SuSE SLES 12 SP3
x86_64
p7zip-debuginfo-9.20.1-7.3.1
p7zip-debugsource-9.20.1-7.3.1
p7zip-9.20.1-7.3.1

146403 - SuSE Linux 42.3 openSUSE-SU-2018:0469-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11624, CVE-2017-11625, CVE-2017-11626, CVE-2017-11627, CVE-2017-12595, CVE-2017-9208, CVE-2017-9209, CVE-2017-9210

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0469-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00056.html

SuSE Linux 42.3
x86_64
qpdf-debugsource-7.1.1-6.3.1
cups-filters-cups-browsed-1.8.2-4.2.1
qpdf-7.1.1-6.3.1
cups-filters-foomatic-rip-debuginfo-1.8.2-4.2.1
cups-filters-devel-1.8.2-4.2.1
cups-filters-debugsource-1.8.2-4.2.1
qpdf-debuginfo-7.1.1-6.3.1
libqpdf18-7.1.1-6.3.1
cups-filters-ghostscript-1.8.2-4.2.1
cups-filters-1.8.2-4.2.1
cups-filters-foomatic-rip-1.8.2-4.2.1
cups-filters-ghostscript-debuginfo-1.8.2-4.2.1

cups-filters-cups-browsed-debuginfo-1.8.2-4.2.1
libqpdf18-debuginfo-7.1.1-6.3.1
cups-filters-debuginfo-1.8.2-4.2.1
qpdf-devel-7.1.1-6.3.1

i586
qpdf-debugsource-7.1.1-6.3.1
qpdf-debuginfo-7.1.1-6.3.1
libqpdf18-7.1.1-6.3.1
qpdf-7.1.1-6.3.1
qpdf-devel-7.1.1-6.3.1
libqpdf18-debuginfo-7.1.1-6.3.1

146411 - SuSE Linux 42.3 openSUSE-SU-2018:0479-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6360

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0479-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00065.html

SuSE Linux 42.3
i586
libmpv1-0.27.2-13.5.1
libmpv1-debuginfo-0.27.2-13.5.1
mpv-devel-0.27.2-13.5.1
mpv-debuginfo-0.27.2-13.5.1
mpv-0.27.2-13.5.1

noarch
mpv-bash-completion-3.3.16-13.5.1
mpv-zsh-completion-0.27.2-13.5.1

x86_64
libmpv1-0.27.2-13.5.1
libmpv1-debuginfo-0.27.2-13.5.1
mpv-devel-0.27.2-13.5.1
mpv-debuginfo-0.27.2-13.5.1
mpv-0.27.2-13.5.1

186105 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3576-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5008, CVE-2017-1000256, CVE-2018-5748, CVE-2018-6764

Description

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

USN-3576-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004285.html

Ubuntu 16.04

libvirt-bin_1.3.1-1ubuntu10.19
libvirt0_1.3.1-1ubuntu10.19

Ubuntu 14.04

libvirt-bin_1.2.2-0ubuntu13.1.26
libvirt0_1.2.2-0ubuntu13.1.26

Ubuntu 17.10

libvirt-bin_3.6.0-1ubuntu6.3
libvirt0_3.6.0-1ubuntu6.3

193285 - Fedora Linux 27 FEDORA-2018-29232aa760 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17969

Description

The scan detected that the host is missing the following update:
FEDORA-2018-29232aa760

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/2018/2/?count=200&page=3

Fedora Core 27

p7zip-16.02-10.fc27

193292 - Fedora Linux 26 FEDORA-2018-7edc48be11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17969

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7edc48be11

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/2018/2/?count=200&page=2

Fedora Core 26

p7zip-16.02-10.fc26

23131 - (HPESBHF03814) HPE Intelligent Management Center Remote Unauthorized Modification Vulnerability

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

Risk Level: Medium

CVE: CVE-2004-2761

Description

A vulnerability is present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A vulnerability is present in some versions of HPE Intelligent Management Center. The flaw is related with an issue with the MD5 Message-Digest algorithm. Successful exploitation could allow an attacker to bypass security access restrictions in the target system.

23132 - (K45432295) F5 BIG-IP APM Logging Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6139

Description

A vulnerability is present in some versions of F5 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 BIG-IP APM logging. Successful exploitation could allow an attacker to obtain potentially sensitive information on the target system.

23133 - (K12044607) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6132

Description

A denial of service vulnerability is present in some versions of F5 BIG-IP systems.

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in TMM. Successful exploitation

could allow an attacker to cause a denial of service condition.

23142 - (VMSA-2018-0007) VMware vSphere Integrated Containers Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

Multiple vulnerabilities are present in some versions of VMware vSphere Integrated Containers.

Observation

VMware vSphere Integrated Container (VIC) is a platform that helps to deploy and manage containers within virtual machines.

Multiple vulnerabilities are present in some versions of VMware vSphere Integrated Containers. The flaws occurs due to abuse of CPU data cache timing. Successful exploitation could allow an attacker to retrieve sensitive data.

23144 - (HPESBHF03810) HPE Intelligent Management Center Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-8980

Description

A vulnerability is present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A vulnerability is present in some versions of HPE Intelligent Management Center. The flaw lies in an unknown component. Successful exploitation could allow an attacker to disclose information.

131022 - Debian Linux 8.0 DSA-4119-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16803

Description

The scan detected that the host is missing the following update:
DSA-4119-1

Observation

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

http://www.debian.org/security/2018/dsa-4119

Debian 8.0
all
libavdevice55_6:11.12-1~deb8u1
libavcodec-dev_6:11.12-1~deb8u1

libavfilter5_6:11.12-1~deb8u1
libswscale-dev_6:11.12-1~deb8u1
libavcodec-extra-56_6:11.12-1~deb8u1
libav-dbg_6:11.12-1~deb8u1
libavformat-dev_6:11.12-1~deb8u1
libavcodec-extra_6:11.12-1~deb8u1
libavdevice-dev_6:11.12-1~deb8u1
libavcodec56_6:11.12-1~deb8u1
libavutil54_6:11.12-1~deb8u1
libavresample2_6:11.12-1~deb8u1
libav-tools_6:11.12-1~deb8u1
libavformat56_6:11.12-1~deb8u1
libavutil-dev_6:11.12-1~deb8u1
libavfilter-dev_6:11.12-1~deb8u1
libswscale3_6:11.12-1~deb8u1
libav-doc_6:11.12-1~deb8u1
libavresample-dev_6:11.12-1~deb8u1

146384 - SuSE Linux 42.3 openSUSE-SU-2018:0474-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2131

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0474-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00060.html

SuSE Linux 42.3
x86_64
python-rrdtool-1.4.7-26.3.1
tcl-rrdtool-debuginfo-1.4.7-26.3.1
python-rrdtool-debuginfo-1.4.7-26.3.1
ruby-rrdtool-1.4.7-26.3.1
rrdtool-devel-1.4.7-26.3.1
lua-rrdtool-debuginfo-1.4.7-26.3.1
tcl-rrdtool-1.4.7-26.3.1
rrdtool-cached-1.4.7-26.3.1
rrdtool-debuginfo-1.4.7-26.3.1
lua-rrdtool-1.4.7-26.3.1
ruby-rrdtool-debuginfo-1.4.7-26.3.1
rrdtool-1.4.7-26.3.1
rrdtool-cached-debuginfo-1.4.7-26.3.1
rrdtool-debugsource-1.4.7-26.3.1

i586
python-rrdtool-1.4.7-26.3.1
tcl-rrdtool-debuginfo-1.4.7-26.3.1
python-rrdtool-debuginfo-1.4.7-26.3.1
ruby-rrdtool-1.4.7-26.3.1
rrdtool-devel-1.4.7-26.3.1
lua-rrdtool-debuginfo-1.4.7-26.3.1

tcl-rrdtool-1.4.7-26.3.1
rrdtool-cached-1.4.7-26.3.1
rrdtool-debuginfo-1.4.7-26.3.1
lua-rrdtool-1.4.7-26.3.1
ruby-rrdtool-debuginfo-1.4.7-26.3.1
rrdtool-1.4.7-26.3.1
rrdtool-cached-debuginfo-1.4.7-26.3.1
rrdtool-debugsource-1.4.7-26.3.1

146391 - SuSE Linux 42.3 openSUSE-SU-2018:0504-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16612

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0504-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00087.html

SuSE Linux 42.3
x86_64
libXcursor1-debuginfo-32bit-1.1.14-10.3.1
libXcursor1-32bit-1.1.14-10.3.1
libXcursor1-1.1.14-10.3.1
libXcursor-devel-32bit-1.1.14-10.3.1
libXcursor1-debuginfo-1.1.14-10.3.1
libXcursor-debugsource-1.1.14-10.3.1
libXcursor-devel-1.1.14-10.3.1

i586
libXcursor-devel-1.1.14-10.3.1
libXcursor-debugsource-1.1.14-10.3.1
libXcursor1-debuginfo-1.1.14-10.3.1
libXcursor1-1.1.14-10.3.1

146392 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2018:0466-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15132

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0466-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003739.html

SuSE SLES 12 SP3
x86_64
dovecot22-backend-sqlite-debuginfo-2.2.31-19.5.1
dovecot22-debuginfo-2.2.31-19.5.1
dovecot22-backend-pgsql-debuginfo-2.2.31-19.5.1
dovecot22-backend-mysql-2.2.31-19.5.1
dovecot22-backend-pgsql-2.2.31-19.5.1
dovecot22-backend-sqlite-2.2.31-19.5.1
dovecot22-backend-mysql-debuginfo-2.2.31-19.5.1
dovecot22-2.2.31-19.5.1
dovecot22-debugsource-2.2.31-19.5.1

SuSE SLES 12 SP2
x86_64
dovecot22-backend-sqlite-debuginfo-2.2.31-19.5.1
dovecot22-debuginfo-2.2.31-19.5.1
dovecot22-backend-pgsql-debuginfo-2.2.31-19.5.1
dovecot22-backend-mysql-2.2.31-19.5.1
dovecot22-backend-pgsql-2.2.31-19.5.1
dovecot22-backend-sqlite-2.2.31-19.5.1
dovecot22-backend-mysql-debuginfo-2.2.31-19.5.1
dovecot22-2.2.31-19.5.1
dovecot22-debugsource-2.2.31-19.5.1

146394 - SuSE Linux 42.3 openSUSE-SU-2018:0473-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16227, CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0473-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00059.html

SuSE Linux 42.3
x86_64
quagga-debugsource-1.1.1-18.3.1
libfpm_pb0-debuginfo-1.1.1-18.3.1
quagga-1.1.1-18.3.1
libospf0-debuginfo-1.1.1-18.3.1
quagga-debuginfo-1.1.1-18.3.1
libquagga_pb0-debuginfo-1.1.1-18.3.1
libzebra1-debuginfo-1.1.1-18.3.1
libospfapiclient0-1.1.1-18.3.1
libquagga_pb0-1.1.1-18.3.1
quagga-devel-1.1.1-18.3.1
libfpm_pb0-1.1.1-18.3.1
libzebra1-1.1.1-18.3.1
libospfapiclient0-debuginfo-1.1.1-18.3.1
libospf0-1.1.1-18.3.1

i586
quagga-debugsource-1.1.1-18.3.1
libfpm_pb0-debuginfo-1.1.1-18.3.1
quagga-1.1.1-18.3.1
libospf0-debuginfo-1.1.1-18.3.1
quagga-debuginfo-1.1.1-18.3.1
libquagga_pb0-debuginfo-1.1.1-18.3.1
libzebra1-debuginfo-1.1.1-18.3.1
libospfapiclient0-1.1.1-18.3.1
libquagga_pb0-1.1.1-18.3.1
quagga-devel-1.1.1-18.3.1
libfpm_pb0-1.1.1-18.3.1
libzebra1-1.1.1-18.3.1
libospfapiclient0-debuginfo-1.1.1-18.3.1
libospf0-1.1.1-18.3.1

146395 - SuSE Linux 42.3 openSUSE-SU-2018:0492-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15132

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0492-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00076.html

SuSE Linux 42.3
x86_64
dovecot22-fts-2.2.31-2.3.1
dovecot22-fts-solr-debuginfo-2.2.31-2.3.1
dovecot22-devel-2.2.31-2.3.1
dovecot22-fts-debuginfo-2.2.31-2.3.1
dovecot22-backend-mysql-2.2.31-2.3.1
dovecot22-debugsource-2.2.31-2.3.1
dovecot22-fts-lucene-debuginfo-2.2.31-2.3.1
dovecot22-fts-squat-2.2.31-2.3.1
dovecot22-backend-sqlite-2.2.31-2.3.1
dovecot22-debuginfo-2.2.31-2.3.1
dovecot22-backend-pgsql-2.2.31-2.3.1
dovecot22-backend-pgsql-debuginfo-2.2.31-2.3.1
dovecot22-backend-mysql-debuginfo-2.2.31-2.3.1
dovecot22-2.2.31-2.3.1
dovecot22-fts-solr-2.2.31-2.3.1
dovecot22-fts-squat-debuginfo-2.2.31-2.3.1
dovecot22-fts-lucene-2.2.31-2.3.1
dovecot22-backend-sqlite-debuginfo-2.2.31-2.3.1

i586
dovecot22-fts-2.2.31-2.3.1
dovecot22-fts-solr-debuginfo-2.2.31-2.3.1
dovecot22-devel-2.2.31-2.3.1
dovecot22-fts-debuginfo-2.2.31-2.3.1

dovecot22-backend-mysql-2.2.31-2.3.1
dovecot22-debugsource-2.2.31-2.3.1
dovecot22-fts-lucene-debuginfo-2.2.31-2.3.1
dovecot22-fts-squat-2.2.31-2.3.1
dovecot22-backend-sqlite-2.2.31-2.3.1
dovecot22-debuginfo-2.2.31-2.3.1
dovecot22-backend-pgsql-2.2.31-2.3.1
dovecot22-backend-pgsql-debuginfo-2.2.31-2.3.1
dovecot22-backend-mysql-debuginfo-2.2.31-2.3.1
dovecot22-2.2.31-2.3.1
dovecot22-fts-solr-2.2.31-2.3.1
dovecot22-fts-squat-debuginfo-2.2.31-2.3.1
dovecot22-fts-lucene-2.2.31-2.3.1
dovecot22-backend-sqlite-debuginfo-2.2.31-2.3.1

146409 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2018:0456-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16227, CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0456-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003734.html

SuSE SLES 12 SP3
x86_64
libzebra1-1.1.1-17.7.1
libfpm_pb0-1.1.1-17.7.1
libospf0-debuginfo-1.1.1-17.7.1
libospfapiclient0-debuginfo-1.1.1-17.7.1
libospf0-1.1.1-17.7.1
quagga-debugsource-1.1.1-17.7.1
libospfapiclient0-1.1.1-17.7.1
libzebra1-debuginfo-1.1.1-17.7.1
libquagga_pb0-1.1.1-17.7.1
libquagga_pb0-debuginfo-1.1.1-17.7.1
quagga-1.1.1-17.7.1
libfpm_pb0-debuginfo-1.1.1-17.7.1
quagga-debuginfo-1.1.1-17.7.1

SuSE SLES 12 SP2
x86_64
libzebra1-1.1.1-17.7.1
libfpm_pb0-1.1.1-17.7.1
libospf0-debuginfo-1.1.1-17.7.1
libospfapiclient0-debuginfo-1.1.1-17.7.1
libospf0-1.1.1-17.7.1
quagga-debugsource-1.1.1-17.7.1
libospfapiclient0-1.1.1-17.7.1
libzebra1-debuginfo-1.1.1-17.7.1
libquagga_pb0-1.1.1-17.7.1

libquagga_pb0-debuginfo-1.1.1-17.7.1
quagga-1.1.1-17.7.1
libfpm_pb0-debuginfo-1.1.1-17.7.1
quagga-debuginfo-1.1.1-17.7.1

146412 - SuSE Linux 42.3 openSUSE-SU-2018:0498-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16899

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0498-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00081.html

SuSE Linux 42.3
x86_64
transfig-3.2.5e-7.3.1
transfig-debuginfo-3.2.5e-7.3.1
transfig-debugsource-3.2.5e-7.3.1

i586
transfig-3.2.5e-7.3.1
transfig-debuginfo-3.2.5e-7.3.1
transfig-debugsource-3.2.5e-7.3.1

178586 - Gentoo Linux GLSA-201802-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201802-02

Observation

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

https://security.gentoo.org/glsa/201802-02

Affected packages:
www-client/chromium < 64.0.3282.167
www-client/google-chrome < 64.0.3282.167

178587 - Gentoo Linux GLSA-201802-05 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201802-05

Observation

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

https://security.gentoo.org/glsa/201802-05

Affected packages:
dev-lang/ruby < 2.2.9

178588 - Gentoo Linux GLSA-201802-06 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-201802-06

Observation

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

https://security.gentoo.org/glsa/201802-06

Affected packages:
app-office/libreoffice < 5.4.5.1
app-office/libreoffice-bin < 5.4.5.1

182612 - FreeBSD consul Vulnerability In Embedded DNS Library (ad2eeab6-ca68-4f06-9325-1937b237df60)

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

Risk Level: Medium

CVE: CVE-2017-15133

Description

The scan detected that the host is missing the following update:
consul -- vulnerability in embedded DNS library (ad2eeab6-ca68-4f06-9325-1937b237df60)

Observation

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

http://www.vuxml.org/freebsd/ad2eeab6-ca68-4f06-9325-1937b237df60.html

Affected packages:
consul < 1.0.5

23034 - Cisco AnyConnect Secure Mobility Client XML External Entity Injection Vulnerability (cisco-sa-20180117-acpe)

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

Risk Level: Medium

CVE: CVE-2018-0100

Description

An XML External Entity Injection vulnerability is present in some versions of Cisco AnyConnect Secure Mobility Client.

Observation

Cisco AnyConnect Secure Mobility Client is a VPN client software.

An XML External Entity Injection vulnerability is present in some versions of Cisco AnyConnect Secure Mobility Client. The flaw lies in the profile editor component. Successful exploitation could allow an attacker to retrieve or modify data in the target system.

146385 - SuSE Linux 42.3 openSUSE-SU-2018:0493-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11332, CVE-2017-11358, CVE-2017-11359, CVE-2017-15370, CVE-2017-15371, CVE-2017-15372, CVE-2017-15642, CVE-2017-18189

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0493-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00077.html

SuSE Linux 42.3
x86_64
libsox3-debuginfo-14.4.2-5.3.1
sox-debugsource-14.4.2-5.3.1
libsox3-14.4.2-5.3.1
sox-debuginfo-14.4.2-5.3.1
sox-devel-14.4.2-5.3.1
sox-14.4.2-5.3.1

i586
libsox3-debuginfo-14.4.2-5.3.1
sox-debugsource-14.4.2-5.3.1
libsox3-14.4.2-5.3.1
sox-debuginfo-14.4.2-5.3.1
sox-devel-14.4.2-5.3.1
sox-14.4.2-5.3.1

193274 - Fedora Linux 27 FEDORA-2018-ec93095a73 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15372, CVE-2017-15642

Description

The scan detected that the host is missing the following update:
FEDORA-2018-ec93095a73

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/2018/2/?count=200&page=3

Fedora Core 27

sox-14.4.2.0-16.fc27

193276 - Fedora Linux 27 FEDORA-2018-5b2e981f14 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5759, CVE-2018-6191

Description

The scan detected that the host is missing the following update:
FEDORA-2018-5b2e981f14

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/2018/2/?count=200&page=3

Fedora Core 27

mujs-0-11.20180129git25821e6.fc27

193278 - Fedora Linux 26 FEDORA-2018-d4746c772f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5759, CVE-2018-6191

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d4746c772f

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/2018/2/?count=200&page=4

Fedora Core 26

mujs-0-11.20180129git25821e6.fc26

193288 - Fedora Linux 27 FEDORA-2018-8d544ee879 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6484, CVE-2018-6869

Description

The scan detected that the host is missing the following update:
FEDORA-2018-8d544ee879

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/2018/2/?count=200&page=1

Fedora Core 27

zziplib-0.13.68-1.fc27

193291 - Fedora Linux 26 FEDORA-2018-aa1bf1711d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15372, CVE-2017-15642

Description

The scan detected that the host is missing the following update:
FEDORA-2018-aa1bf1711d

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/2018/2/?count=200&page=2

Fedora Core 26

sox-14.4.2.0-17.fc26

23079 - IBM WebSphere Application Server Information Disclosure Vulnerability (swg22010419)

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

Risk Level: Low

CVE: CVE-2017-1681

Description

An information disclosure vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

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

An information disclosure vulnerability is present in some versions of IBM WebSphere Application Server. The flaw is due to improper handling of application requests. Successful exploitation could allow an attacker to obtain sensitive information.

88917 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-046-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-7050, CVE-2018-7051, CVE-2018-7052, CVE-2018-7053, CVE-2018-7054

Description

The scan detected that the host is missing the following update:
SSA:2018-046-01

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=2018&m=slackware-security.437110

Slackware 14.0
x86_64
irssi-1.0.7-x86_64-1

Slackware 14.2
x86_64
irssi-1.0.7-x86_64-1

i586
irssi-1.0.7-i586-1

Slackware 14.1
x86_64
irssi-1.0.7-x86_64-1

131020 - Debian Linux 8.0, 9.0 DSA-4118-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15698

Description

The scan detected that the host is missing the following update:
DSA-4118-1

Observation

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

http://www.debian.org/security/2018/dsa-4118

Debian 8.0
all
libtcnative-1_1.1.32~repack-2+deb8u1

Debian 9.0

all
libtcnative-1_1.2.12-2+deb9u1

131024 - Debian Linux 9.0 DSA-4116-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6791

Description

The scan detected that the host is missing the following update:
DSA-4116-1

Observation

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

http://www.debian.org/security/2018/dsa-4116

Debian 9.0
all
plasma-workspace_4:5.8.6-2.1+deb9u1

131025 - Debian Linux 8.0, 9.0 DSA-4115-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

Description

The scan detected that the host is missing the following update:
DSA-4115-1

Observation

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

http://www.debian.org/security/2018/dsa-4115

Debian 8.0
all
quagga_0.99.23.1-1+deb8u5

Debian 9.0
all
quagga_1.1.1-3+deb9u2

131026 - Debian Linux 8.0 DSA-4117-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-4117-1

Observation

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

http://www.debian.org/security/2018/dsa-4117

Debian 8.0
all
gcc-4.9_4.9.2-10+deb8u1

182608 - FreeBSD libraw Multiple DoS Vulnerabilities (c60804f1-126f-11e8-8b5b-4ccc6adda413)

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

Risk Level: Low

CVE: CVE-2017-16909, CVE-2017-16910

Description

The scan detected that the host is missing the following update:
libraw -- multiple DoS vulnerabilities (c60804f1-126f-11e8-8b5b-4ccc6adda413)

Observation

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

http://www.vuxml.org/freebsd/c60804f1-126f-11e8-8b5b-4ccc6adda413.html

Affected packages:
libraw < 0.18.6

182609 - FreeBSD libraw Multiple DoS Vulnerabilities (6f0b0cbf-1274-11e8-8b5b-4ccc6adda413)

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

Risk Level: Low

CVE: CVE-2018-5800, CVE-2018-5801, CVE-2018-5802

Description

The scan detected that the host is missing the following update:
libraw -- multiple DoS vulnerabilities (6f0b0cbf-1274-11e8-8b5b-4ccc6adda413)

Observation

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

http://www.vuxml.org/freebsd/6f0b0cbf-1274-11e8-8b5b-4ccc6adda413.html

Affected packages:
libraw < 0.18.7

182610 - FreeBSD Bugzilla Security Issues (22283b8c-13c5-11e8-a861-20cf30e32f6d)

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

Risk Level: Low

CVE: CVE-2018-5123

Description

The scan detected that the host is missing the following update:
Bugzilla security issues (22283b8c-13c5-11e8-a861-20cf30e32f6d)

Observation

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

http://www.vuxml.org/freebsd/22283b8c-13c5-11e8-a861-20cf30e32f6d.html

Affected packages:
bugzilla44 < 4.4.13
bugzilla50 < 5.0.4

182611 - FreeBSD jenkins Path Traversal Vulnerability Allows Access To Files Outside Plugin Resources (5d374fbb-bae3-45db-afc0-795684ac73

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

Risk Level: Low

CVE: CVE-2018-6356

Description

The scan detected that the host is missing the following update:
jenkins -- Path traversal vulnerability allows access to files outside plugin resources (5d374fbb-bae3-45db-afc0-795684ac7353)

Observation

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

http://www.vuxml.org/freebsd/5d374fbb-bae3-45db-afc0-795684ac7353.html

Affected packages:
jenkins <= 2.106
jenkins-lts <= 2.89.3

182613 - FreeBSD p5-Mojolicious Cookie-handling Vulnerability (a183acb5-1414-11e8-9542-002590acae31)

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:
p5-Mojolicious -- cookie-handling vulnerability (a183acb5-1414-11e8-9542-002590acae31)

Observation

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

http://www.vuxml.org/freebsd/a183acb5-1414-11e8-9542-002590acae31.html

Affected packages:
p5-Mojolicious < 7.66

182614 - FreeBSD irssi Multiple Vulnerabilities (7afc5e56-156d-11e8-95f2-005056925db4)

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

Risk Level: Low

CVE: CVE-2018-7050, CVE-2018-7051, CVE-2018-7052, CVE-2018-7053, CVE-2018-7054

Description

The scan detected that the host is missing the following update:
irssi -- multiple vulnerabilities (7afc5e56-156d-11e8-95f2-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/7afc5e56-156d-11e8-95f2-005056925db4.html

Affected packages:
irssi < 1.1.1,1

182615 - FreeBSD bro Integer Overflow Allows Remote DOS (044cff62-ed8b-4e72-b102-18a7d58a669f)

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:
bro -- integer overflow allows remote DOS (044cff62-ed8b-4e72-b102-18a7d58a669f)

Observation

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

http://www.vuxml.org/freebsd/044cff62-ed8b-4e72-b102-18a7d58a669f.html

Affected packages:
bro < 2.5.3

182616 - FreeBSD bitmessage Remote Code Execution Vulnerability (1a75c84a-11c8-11e8-83e7-485b3931c969)

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:
bitmessage -- remote code execution vulnerability (1a75c84a-11c8-11e8-83e7-485b3931c969)

Observation

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

For more information see:

http://www.vuxml.org/freebsd/1a75c84a-11c8-11e8-83e7-485b3931c969.html

Affected packages:
bitmessage <= 0.6.2

182617 - FreeBSD bro Out Of Bounds Write Allows Remote DOS (746d04dc-507e-4450-911f-4c41e48bb07a)

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:
bro -- out of bounds write allows remote DOS (746d04dc-507e-4450-911f-4c41e48bb07a)

Observation

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

http://www.vuxml.org/freebsd/746d04dc-507e-4450-911f-4c41e48bb07a.html

Affected packages:
bro < 2.5.2

182618 - FreeBSD quagga Several Security Issues (e15a22ce-f16f-446b-9ca7-6859350c2e75)

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

Risk Level: Low

CVE: CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

Description

The scan detected that the host is missing the following update:
quagga -- several security issues (e15a22ce-f16f-446b-9ca7-6859350c2e75)

Observation

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

http://www.vuxml.org/freebsd/e15a22ce-f16f-446b-9ca7-6859350c2e75.html

Affected packages:
quagga < 1.2.3

182619 - FreeBSD GitLab Multiple Vulnerabilities (86291013-16e6-11e8-ae9f-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 (86291013-16e6-11e8-ae9f-d43d7e971a1b)

Observation

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

http://www.vuxml.org/freebsd/86291013-16e6-11e8-ae9f-d43d7e971a1b.html

Affected packages:
6.1.0 <= gitlab <= 10.2.7
10.3.0 <= gitlab <= 10.3.6
10.4.0 <= gitlab <= 10.4.2

186102 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3570-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1056

Description

The scan detected that the host is missing the following update:
USN-3570-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004280.html

Ubuntu 16.04

advancecomp_1.20-1ubuntu0.1

Ubuntu 14.04

advancecomp_1.18-1ubuntu0.1

Ubuntu 17.10

advancecomp_2.0-1ubuntu0.1

186103 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3573-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

Description

The scan detected that the host is missing the following update:
USN-3573-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004282.html

Ubuntu 16.04

quagga_0.99.24.1-2ubuntu1.4

Ubuntu 14.04

quagga_0.99.22.4-3ubuntu1.5

Ubuntu 17.10

quagga_1.1.1-3ubuntu0.2
quagga-bgpd_1.1.1-3ubuntu0.2

186107 - Ubuntu Linux 14.04, 16.04 USN-3577-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-18190

Description

The scan detected that the host is missing the following update:
USN-3577-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004286.html

Ubuntu 14.04

cups_1.7.2-0ubuntu1.9

Ubuntu 16.04

cups_2.1.3-4ubuntu0.4

193271 - Fedora Linux 27 FEDORA-2018-391a1f3e61 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5729, CVE-2018-5730

Description

The scan detected that the host is missing the following update:
FEDORA-2018-391a1f3e61

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/2018/2/?count=200&page=1

Fedora Core 27

krb5-1.15.2-7.fc27

193272 - Fedora Linux 27 FEDORA-2018-07a3e36499 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6942

Description

The scan detected that the host is missing the following update:
FEDORA-2018-07a3e36499

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/2018/2/?count=200&page=1

Fedora Core 27

freetype-2.8-8.fc27

193273 - Fedora Linux 26 FEDORA-2018-337757e11f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6790, CVE-2018-6791

Description

The scan detected that the host is missing the following update:
FEDORA-2018-337757e11f

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/2018/2/?count=200&page=1

Fedora Core 26

plasma-workspace-5.10.5-6.fc26

193275 - Fedora Linux 27 FEDORA-2017-2d4c9a6e37 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7067

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2d4c9a6e37

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/2018/2/?count=200&page=1

Fedora Core 27

monit-5.25.1-1.fc27

193277 - Fedora Linux 26 FEDORA-2018-ac2e276c76 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15706

Description

The scan detected that the host is missing the following update:
FEDORA-2018-ac2e276c76

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/2018/2/?count=200&page=2

Fedora Core 26

tomcat-8.0.49-1.fc26

193279 - Fedora Linux 27 FEDORA-2018-80b55ca071 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-2018-80b55ca071

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/2018/2/?count=200&page=3

Fedora Core 27

torbrowser-launcher-0.2.9-1.fc27

193280 - Fedora Linux 27 FEDORA-2018-b127e58641 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-10713, CVE-2018-6951, CVE-2018-6952

Description

The scan detected that the host is missing the following update:
FEDORA-2018-b127e58641

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/2018/2/?count=200&page=1

Fedora Core 27

patch-2.7.6-3.fc27

193281 - Fedora Linux 27 FEDORA-2018-a0d72435aa 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-2018-a0d72435aa

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/2018/2/?count=200&page=3

Fedora Core 27

ca-certificates-2018.2.22-1.0.fc27

193282 - Fedora Linux 27 FEDORA-2018-5562b6e2c0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6574

Description

The scan detected that the host is missing the following update:
FEDORA-2018-5562b6e2c0

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/2018/2/?count=200&page=1

Fedora Core 27

golang-1.9.4-1.fc27

193284 - Fedora Linux 26 FEDORA-2018-0a3b07a003 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1055

Description

The scan detected that the host is missing the following update:
FEDORA-2018-0a3b07a003

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/2018/2/?count=200&page=1

Fedora Core 26

libreoffice-5.3.7.2-8.fc26

193286 - Fedora Linux 26 FEDORA-2017-d75a88f263 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7067

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d75a88f263

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/2018/2/?count=200&page=2

Fedora Core 26

monit-5.25.1-1.fc26

193287 - Fedora Linux 26 FEDORA-2018-60613721f6 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-2018-60613721f6

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/2018/2/?count=200&page=2

Fedora Core 26

ca-certificates-2018.2.22-1.0.fc26

193290 - Fedora Linux 27 FEDORA-2018-3eb4d8e4c4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1055, CVE-2018-6871

Description

The scan detected that the host is missing the following update:
FEDORA-2018-3eb4d8e4c4

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/2018/2/?count=200&page=3

Fedora Core 27

libreoffice-5.4.5.1-1.fc27

193293 - Fedora Linux 27 FEDORA-2018-2c612c6d92 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6188

Description

The scan detected that the host is missing the following update:
FEDORA-2018-2c612c6d92

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/2018/2/?count=200&page=3

Fedora Core 27

python-django-1.11.10-1.fc27

193294 - Fedora Linux 27 FEDORA-2018-8fb4a6185e 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-2018-8fb4a6185e

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/2018/2/?count=200&page=1

Fedora Core 27

firefox-58.0.2-1.fc27

193295 - Fedora Linux 26 FEDORA-2018-48d385a6fd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1294

Description

The scan detected that the host is missing the following update:
FEDORA-2018-48d385a6fd

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/2018/2/?count=200&page=3

Fedora Core 26

apache-commons-email-1.5-1.fc26

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

23047 - (HT208465) Apple macOS Multiple Vulnerabilities Prior To 10.13.3

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

Risk Level: High

CVE: CVE-2017- 5705, CVE-2017- 5708, CVE-2017-5754, CVE-2017-8817, CVE-2018-4082, CVE-2018-4083, CVE-2018-4084, CVE-2018-4085, CVE-2018-4086, CVE-2018-4088, CVE-2018-4089, CVE-2018-4090, CVE-2018-4091, CVE-2018-4092, CVE-2018-4093, CVE-2018-4094, CVE-2018-4096, CVE-2018-4097, CVE-2018-4098, CVE-2018-4100

Update Details

Risk is updated

182343 - FreeBSD jenkins Multiple Vulnerabilities (631c4710-9be5-4a80-9310-eb2847fe24dd)

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

Risk Level: High

CVE: CVE-2017-1000353, CVE-2017-1000354, CVE-2017-1000355, CVE-2017-1000356

Update Details
Risk is updated

182607 - FreeBSD electrum JSONRPC Vulnerability (aa743ee4-0f16-11e8-8fd2-10bf48e1088e)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-6353

Update Details
Risk is updated

185973 - Ubuntu Linux 16.04, 17.04, 17.10 USN-3480-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14177, CVE-2017-14180

Update Details
Risk is updated

185981 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3480-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14177, CVE-2017-14180

Update Details
Risk is updated

186056 - Ubuntu Linux 12.04 USN-3536-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-1000001

Update Details
Risk is updated

188039 - Fedora Linux 19 FEDORA-2014-7603 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-3005

Update Details
Risk is updated

188042 - Fedora Linux 20 FEDORA-2014-7594 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2014-3005

Update Details
Risk is updated

193135 - Fedora Linux 27 FEDORA-2017-828f8a8fc6 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1000408, CVE-2017-1000409

Update Details
Risk is updated

130994 - Debian Linux 8.0 DSA-4085-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-0486

Update Details
Risk is updated

131011 - Debian Linux 8.0, 9.0 DSA-4104-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17969

Update Details
Risk is updated

131014 - Debian Linux 9.0 DSA-4105-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-6360

Update Details
Risk is updated

146273 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2018:0140-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-0486

Update Details
Risk is updated

146275 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0158-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-0486

Update Details
Risk is updated

182571 - FreeBSD shibboleth-sp Vulnerable To Forged User Attribute Data (3dbe9492-f7b8-11e7-a12d-6cc21735f730)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-0486

Update Details
Risk is updated

182598 - FreeBSD mpv Arbitrary Code Execution Via Crafted Website (3ee6e521-0d32-11e8-99b0-d017c2987f9a)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-6360

Update Details
Risk is updated

182600 - FreeBSD p7zip-codec-rar Insufficient Error Handling (7a2e0063-0e4e-11e8-94c0-5453ed2e2b49)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5996

Update Details
Risk is updated

182603 - FreeBSD p7zip Heap-based Buffer Overflow (6d337396-0e4a-11e8-94c0-5453ed2e2b49)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17969

Update Details
Risk is updated

193241 - Fedora Linux 26 FEDORA-2018-cd4311d4d6 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17969

Update Details

Risk is updated

193246 - Fedora Linux 27 FEDORA-2018-f8ad787538 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17969

Update Details

Risk is updated

146124 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3221-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15091

Update Details

Risk is updated

193252 - Fedora Linux 27 FEDORA-2017-d7c0748c1b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15091

Update Details

Risk is updated

193239 - Fedora Linux 27 FEDORA-2018-a24be2586d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6381

Update Details

Risk is updated

70050 - vmware.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly

urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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