2019-APR-17
FSL version 7.6.106

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

24881 - Rockwell Automation RSLinx Classic Buffer Overflow Vulnerability (ICSA-19-064-01)

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

Risk Level: High

CVE: CVE-2019-6553

Description

A vulnerability is present in some versions of Rockwell Automation RSLinx Classic.

Observation

Rockwell Automation RSLinx Classic is a software, which allows programmable controllers to connect to all Rockwell application.

A vulnerability is present in some versions of Rockwell Automation RSLinx Classic. The flaw is due to improper input validation in a .dll file. Successful exploitation could allow an attacker to execute arbitrary code in the targeted system.

24931 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 60.6.1

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

Risk Level: High

CVE: CVE-2019-9810, CVE-2019-9813

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

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

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, buffer overflow and arbitrary memory read & write on the target system.

195065 - Fedora Linux 28 FEDORA-2019-ce2933b003 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-16880, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-3882, CVE-2019-3887, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9857

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ce2933b003

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/2019/4/?count=200&page=3

Fedora Core 28

kernel-headers-5.0.7-100.fc28
kernel-5.0.7-100.fc28
kernel-tools-5.0.7-100.fc28

25008 - Apache Tomcat Vulnerability Prior To 9.0.16

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

Risk Level: High

CVE: CVE-2019-0199

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 HTTP/2 implementation. Successful exploitation could allow an attacker to block server side threads leading to thread exhaustion,which causes the denial of service condition.

25034 - Microsoft Office 365 ProPlus and Office 2019 Apr 2019 Updates

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

Risk Level: High

CVE: CVE-2019-0801, CVE-2019-0822, CVE-2019-0824, CVE-2019-0825, CVE-2019-0826, CVE-2019-0827, CVE-2019-0828

Description

Multiple issues are present in some versions of Microsoft Office 365 ProPlus and Office 2019.

Observation

Microsoft Office 365 ProPlus and Office 2019 are the industry standard productivity suites.

Multiple issues are present in some versions of Microsoft Office 365 ProPlus and Office 2019. The flaws are present in multiple components. Such defects could lead the product to software vulnerabilities, malfunction or unexpected behavior in some of its affected components.

131335 - Debian Linux 9.0 DSA-4431-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-

2019-3862, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
DSA-4431-1

Observation

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

http://www.debian.org/security/2019/dsa-4431

Debian 9.0
all
libssh2-1_1.7.0-1+deb9u1
libssh2-1-dev_1.7.0-1+deb9u1
libssh2-1-dbg_1.7.0-1+deb9u1

196289 - Red Hat Enterprise Linux RHSA-2019-0737 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-7096, CVE-2019-7108

Description

The scan detected that the host is missing the following update:
RHSA-2019-0737

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-April/msg00009.html

RHEL6D
x86_64
flash-plugin-32.0.0.171-1.el6_10

i386
flash-plugin-32.0.0.171-1.el6_10

RHEL6S
x86_64
flash-plugin-32.0.0.171-1.el6_10

i386
flash-plugin-32.0.0.171-1.el6_10

RHEL6WS
x86_64
flash-plugin-32.0.0.171-1.el6_10

i386
flash-plugin-32.0.0.171-1.el6_10

25031 - (K16365) F5 BIG-IP Glibc Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-9402

Description

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

Observation

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

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

25009 - Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1606)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1606

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the CLI of Cisco NX-OS Software. Successful exploitation could allow a local attacker to execute arbitrary commands with elevated privileges.

25010 - NVIDIA GeForce Experience Multiple Vulnerabilities 03-2019

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

Risk Level: High

CVE: CVE-2019-5674

Description

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

Observation

NVIDIA is a technology company which manufactures graphics processing units.

A Vulnerability is present in some versions of the NVIDIA GeForce Experience. The flaws occur when ShadowPlay or GameStream is enabled. Successful exploitation could allow an attacker to escalate privileges, cause a denial of service condition or execute arbitrary code.

25017 - Cisco NX-OS Software Bash Shell Role-Based Access Control Bypass Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1593

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the Bash shell implementation. Successful exploitation could allow a local attacker to gain elevated privileges.

25026 - Cisco NX-OS Software NX-API Arbitrary Code Execution Vulnerability (CVE-2019-1605)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1605

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in NX-API of Cisco NX-OS Software. Successful exploitation could allow an attacker to execute arbitrary commands with the security context of the root user.

25033 - Cisco Nexus 9000 Series Fabric Switches Application-Centric Infrastructure Mode Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1585

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the Application Policy Infrastructure Controller (APIC). Successful exploitation could allow an authenticated, local attacker to escalate privilege on the affected system.

147828 - SuSE Linux 15.0 openSUSE-SU-2019:1206-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8375

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1206-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00120.html

SuSE Linux 15.0
i586
typelib-1_0-JavaScriptCore-4_0-2.24.0-lp150.2.16.1
webkit2gtk3-debugsource-2.24.0-lp150.2.16.1
libjavascriptcoregtk-4_0-18-debuginfo-2.24.0-lp150.2.16.1
webkit2gtk-4_0-injected-bundles-2.24.0-lp150.2.16.1
libwebkit2gtk-4_0-37-debuginfo-2.24.0-lp150.2.16.1
webkit2gtk3-minibrowser-debuginfo-2.24.0-lp150.2.16.1
libjavascriptcoregtk-4_0-18-2.24.0-lp150.2.16.1
typelib-1_0-WebKit2-4_0-2.24.0-lp150.2.16.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.24.0-lp150.2.16.1
webkit2gtk3-devel-2.24.0-lp150.2.16.1
typelib-1_0-WebKit2WebExtension-4_0-2.24.0-lp150.2.16.1
webkit-jsc-4-2.24.0-lp150.2.16.1
webkit-jsc-4-debuginfo-2.24.0-lp150.2.16.1
libwebkit2gtk-4_0-37-2.24.0-lp150.2.16.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.0-lp150.2.16.1
webkit2gtk3-minibrowser-2.24.0-lp150.2.16.1
webkit2gtk3-plugin-process-gtk2-2.24.0-lp150.2.16.1

noarch
libwebkit2gtk3-lang-2.24.0-lp150.2.16.1

x86_64
libjavascriptcoregtk-4_0-18-32bit-debuginfo-2.24.0-lp150.2.16.1
typelib-1_0-JavaScriptCore-4_0-2.24.0-lp150.2.16.1
libjavascriptcoregtk-4_0-18-32bit-2.24.0-lp150.2.16.1
webkit2gtk3-debugsource-2.24.0-lp150.2.16.1
libjavascriptcoregtk-4_0-18-debuginfo-2.24.0-lp150.2.16.1
webkit2gtk-4_0-injected-bundles-2.24.0-lp150.2.16.1
libwebkit2gtk-4_0-37-debuginfo-2.24.0-lp150.2.16.1
webkit2gtk3-minibrowser-debuginfo-2.24.0-lp150.2.16.1
libjavascriptcoregtk-4_0-18-2.24.0-lp150.2.16.1
typelib-1_0-WebKit2-4_0-2.24.0-lp150.2.16.1
libwebkit2gtk-4_0-37-32bit-debuginfo-2.24.0-lp150.2.16.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.24.0-lp150.2.16.1
webkit2gtk3-devel-2.24.0-lp150.2.16.1
typelib-1_0-WebKit2WebExtension-4_0-2.24.0-lp150.2.16.1
webkit-jsc-4-2.24.0-lp150.2.16.1
webkit-jsc-4-debuginfo-2.24.0-lp150.2.16.1
libwebkit2gtk-4_0-37-2.24.0-lp150.2.16.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.0-lp150.2.16.1
libwebkit2gtk-4_0-37-32bit-2.24.0-lp150.2.16.1
webkit2gtk3-minibrowser-2.24.0-lp150.2.16.1
webkit2gtk3-plugin-process-gtk2-2.24.0-lp150.2.16.1

147829 - SuSE Linux 42.3 openSUSE-SU-2019:1190-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-0196, CVE-2019-0197, CVE-2019-0211, CVE-2019-0217, CVE-2019-0220

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1190-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00102.html

SuSE Linux 42.3
i586
apache2-event-debuginfo-2.4.23-45.1
apache2-debuginfo-2.4.23-45.1
apache2-utils-2.4.23-45.1
apache2-example-pages-2.4.23-45.1
apache2-debugsource-2.4.23-45.1
apache2-prefork-debuginfo-2.4.23-45.1
apache2-devel-2.4.23-45.1
apache2-prefork-2.4.23-45.1
apache2-2.4.23-45.1
apache2-worker-debuginfo-2.4.23-45.1
apache2-worker-2.4.23-45.1
apache2-event-2.4.23-45.1
apache2-utils-debuginfo-2.4.23-45.1

noarch
apache2-doc-2.4.23-45.1

x86_64
apache2-event-debuginfo-2.4.23-45.1
apache2-debuginfo-2.4.23-45.1
apache2-utils-2.4.23-45.1
apache2-example-pages-2.4.23-45.1
apache2-debugsource-2.4.23-45.1
apache2-prefork-debuginfo-2.4.23-45.1
apache2-devel-2.4.23-45.1
apache2-prefork-2.4.23-45.1
apache2-2.4.23-45.1
apache2-worker-debuginfo-2.4.23-45.1
apache2-worker-2.4.23-45.1
apache2-event-2.4.23-45.1
apache2-utils-debuginfo-2.4.23-45.1

147830 - SuSE Linux 15.0 openSUSE-SU-2019:1209-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-0196, CVE-2019-0197, CVE-2019-0211, CVE-2019-0217, CVE-2019-0220

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1209-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00124.html

SuSE Linux 15.0
i586

apache2-devel-2.4.33-lp150.2.17.1
apache2-utils-debuginfo-2.4.33-lp150.2.17.1
apache2-debugsource-2.4.33-lp150.2.17.1
apache2-debuginfo-2.4.33-lp150.2.17.1
apache2-prefork-debuginfo-2.4.33-lp150.2.17.1
apache2-2.4.33-lp150.2.17.1
apache2-event-debuginfo-2.4.33-lp150.2.17.1
apache2-prefork-2.4.33-lp150.2.17.1
apache2-worker-2.4.33-lp150.2.17.1
apache2-utils-2.4.33-lp150.2.17.1
apache2-event-2.4.33-lp150.2.17.1
apache2-example-pages-2.4.33-lp150.2.17.1
apache2-worker-debuginfo-2.4.33-lp150.2.17.1

noarch
apache2-doc-2.4.33-lp150.2.17.1

x86_64
apache2-devel-2.4.33-lp150.2.17.1
apache2-utils-debuginfo-2.4.33-lp150.2.17.1
apache2-debugsource-2.4.33-lp150.2.17.1
apache2-debuginfo-2.4.33-lp150.2.17.1
apache2-prefork-debuginfo-2.4.33-lp150.2.17.1
apache2-2.4.33-lp150.2.17.1
apache2-event-debuginfo-2.4.33-lp150.2.17.1
apache2-prefork-2.4.33-lp150.2.17.1
apache2-worker-2.4.33-lp150.2.17.1
apache2-utils-2.4.33-lp150.2.17.1
apache2-event-2.4.33-lp150.2.17.1
apache2-example-pages-2.4.33-lp150.2.17.1
apache2-worker-debuginfo-2.4.33-lp150.2.17.1

147831 - SuSE Linux 15.0 openSUSE-SU-2019:1193-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-2024, CVE-2019-3819, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1193-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00109.html

SuSE Linux 15.0
x86_64
kernel-vanilla-debugsource-4.12.14-lp150.12.58.1
kernel-obs-build-debugsource-4.12.14-lp150.12.58.1
kernel-kvmsmall-4.12.14-lp150.12.58.1
kernel-syms-4.12.14-lp150.12.58.1
kernel-vanilla-devel-4.12.14-lp150.12.58.1
kernel-obs-qa-4.12.14-lp150.12.58.1
kernel-default-base-4.12.14-lp150.12.58.1
kernel-debug-devel-debuginfo-4.12.14-lp150.12.58.1

kernel-default-base-debuginfo-4.12.14-lp150.12.58.1
kernel-default-devel-debuginfo-4.12.14-lp150.12.58.1
kernel-kvmsmall-devel-4.12.14-lp150.12.58.1
kernel-debug-devel-4.12.14-lp150.12.58.1
kernel-debug-base-debuginfo-4.12.14-lp150.12.58.1
kernel-debug-4.12.14-lp150.12.58.1
kernel-vanilla-4.12.14-lp150.12.58.1
kernel-default-debuginfo-4.12.14-lp150.12.58.1
kernel-kvmsmall-devel-debuginfo-4.12.14-lp150.12.58.1
kernel-debug-debugsource-4.12.14-lp150.12.58.1
kernel-default-debugsource-4.12.14-lp150.12.58.1
kernel-obs-build-4.12.14-lp150.12.58.1
kernel-debug-base-4.12.14-lp150.12.58.1
kernel-default-devel-4.12.14-lp150.12.58.1
kernel-kvmsmall-base-debuginfo-4.12.14-lp150.12.58.1
kernel-vanilla-devel-debuginfo-4.12.14-lp150.12.58.1
kernel-kvmsmall-debugsource-4.12.14-lp150.12.58.1
kernel-default-4.12.14-lp150.12.58.1
kernel-vanilla-debuginfo-4.12.14-lp150.12.58.1
kernel-vanilla-base-debuginfo-4.12.14-lp150.12.58.1
kernel-vanilla-base-4.12.14-lp150.12.58.1
kernel-debug-debuginfo-4.12.14-lp150.12.58.1
kernel-kvmsmall-base-4.12.14-lp150.12.58.1
kernel-kvmsmall-debuginfo-4.12.14-lp150.12.58.1

noarch
kernel-source-4.12.14-lp150.12.58.1
kernel-macros-4.12.14-lp150.12.58.1
kernel-docs-html-4.12.14-lp150.12.58.1
kernel-docs-4.12.14-lp150.12.58.1
kernel-source-vanilla-4.12.14-lp150.12.58.1
kernel-devel-4.12.14-lp150.12.58.1

147846 - SuSE Linux 15.0 openSUSE-SU-2019:1212-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-7524

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1212-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00123.html

SuSE Linux 15.0
x86_64
dovecot23-backend-mysql-debuginfo-2.3.3-lp150.8.2
dovecot23-backend-pgsql-2.3.3-lp150.8.2
dovecot23-devel-2.3.3-lp150.8.2
dovecot23-fts-debuginfo-2.3.3-lp150.8.2
dovecot23-backend-sqlite-2.3.3-lp150.8.2
dovecot23-debugsource-2.3.3-lp150.8.2
dovecot23-fts-solr-2.3.3-lp150.8.2

dovecot23-backend-pgsql-debuginfo-2.3.3-lp150.8.2
dovecot23-debuginfo-2.3.3-lp150.8.2
dovecot23-2.3.3-lp150.8.2
dovecot23-fts-lucene-debuginfo-2.3.3-lp150.8.2
dovecot23-backend-mysql-2.3.3-lp150.8.2
dovecot23-fts-2.3.3-lp150.8.2
dovecot23-fts-squat-debuginfo-2.3.3-lp150.8.2
dovecot23-fts-lucene-2.3.3-lp150.8.2
dovecot23-fts-solr-debuginfo-2.3.3-lp150.8.2
dovecot23-fts-squat-2.3.3-lp150.8.2
dovecot23-backend-sqlite-debuginfo-2.3.3-lp150.8.2

147847 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0956-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5953

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0956-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005343.html

SuSE SLED 12 SP3
x86_64
wget-debugsource-1.14-21.10.1
wget-debuginfo-1.14-21.10.1
wget-1.14-21.10.1

SuSE SLED 12 SP4
x86_64
wget-debugsource-1.14-21.10.1
wget-debuginfo-1.14-21.10.1
wget-1.14-21.10.1

SuSE SLES 12 SP4
x86_64
wget-debugsource-1.14-21.10.1
wget-debuginfo-1.14-21.10.1
wget-1.14-21.10.1

SuSE SLES 12 SP3
x86_64
wget-debugsource-1.14-21.10.1
wget-debuginfo-1.14-21.10.1
wget-1.14-21.10.1

160543 - CentOS 7 CESA-2019-0697 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-8786, CVE-2018-8787, CVE-2018-8788

Description

The scan detected that the host is missing the following update:
CESA-2019-0697

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-April/023267.html

CentOS 7
x86_64
freerdp-devel-1.0.2-15.el7_6.1
freerdp-libs-1.0.2-15.el7_6.1
freerdp-plugins-1.0.2-15.el7_6.1
freerdp-1.0.2-15.el7_6.1

i686
freerdp-devel-1.0.2-15.el7_6.1
freerdp-libs-1.0.2-15.el7_6.1

163845 - Oracle Enterprise Linux ELSA-2019-4612 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3701, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
ELSA-2019-4612

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-April/008648.html

OEL7
x86_64
kernel-uek-devel-4.14.35-1844.4.5.el7uek
kernel-uek-4.14.35-1844.4.5.el7uek
kernel-uek-debug-4.14.35-1844.4.5.el7uek
kernel-uek-tools-4.14.35-1844.4.5.el7uek
kernel-uek-doc-4.14.35-1844.4.5.el7uek
kernel-uek-debug-devel-4.14.35-1844.4.5.el7uek

186654 - Ubuntu Linux 18.04, 18.10 USN-3948-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11070, CVE-2019-6251, CVE-2019-8375, CVE-2019-8506, CVE-2019-8518, CVE-2019-8523, CVE-2019-8524, CVE-2019-8535, CVE-2019-8536, CVE-2019-8544, CVE-2019-8551, CVE-2019-8558, CVE-2019-8559, CVE-2019-8563

Description

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

USN-3948-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004853.html

Ubuntu 18.10

libwebkit2gtk-4.0-37_2.24.1-0ubuntu0.18.10.2
libjavascriptcoregtk-4.0-18_2.24.1-0ubuntu0.18.10.2

Ubuntu 18.04

libjavascriptcoregtk-4.0-18_2.24.1-0ubuntu0.18.04.1
libwebkit2gtk-4.0-37_2.24.1-0ubuntu0.18.04.1

186658 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3946-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-1000018, CVE-2019-3463, CVE-2019-3464

Description

The scan detected that the host is missing the following update:
USN-3946-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004850.html

Ubuntu 16.04

rssh_2.3.4-4+deb8u2ubuntu0.16.04.2

Ubuntu 18.10

rssh_2.3.4-8ubuntu0.2

Ubuntu 14.04

rssh_2.3.4-4+deb8u2ubuntu0.14.04.2

Ubuntu 18.04

rssh_2.3.4-7ubuntu0.1

195048 - Fedora Linux 29 FEDORA-2019-94dc902948 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16862, CVE-2018-16880, CVE-2018-18710, CVE-2018-19407, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-3882, CVE-2019-3887, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-

8980, CVE-2019-9857

Description

The scan detected that the host is missing the following update:
FEDORA-2019-94dc902948

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/2019/4/?count=200&page=2

Fedora Core 29

kernel-headers-5.0.7-200.fc29
kernel-5.0.7-200.fc29
kernel-tools-5.0.7-200.fc29

195049 - Fedora Linux 30 FEDORA-2019-c3627a0e7a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19974, CVE-2018-19975, CVE-2018-19976

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c3627a0e7a

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/2019/4/?count=200&page=4

Fedora Core 30

yara-3.9.0-1.fc30
python-yara-3.9.0-2.fc30

195062 - Fedora Linux 29 FEDORA-2019-d05bc7e3df Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16873, CVE-2018-16874, CVE-2018-16875, CVE-2019-6486, CVE-2019-9741

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d05bc7e3df

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/2019/4/?count=200&page=4

Fedora Core 29

golang-1.11.6-1.fc29

196292 - Red Hat Enterprise Linux RHSA-2019-0746 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-0211, CVE-2019-3878

Description

The scan detected that the host is missing the following update:
RHSA-2019-0746

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-April/msg00012.html

RHEL6S
x86_64
httpd24-httpd-debuginfo-2.4.34-7.el6.1
httpd24-httpd-tools-2.4.34-7.el6.1
httpd24-mod_ldap-2.4.34-7.el6.1
httpd24-mod_proxy_html-2.4.34-7.el6.1
httpd24-httpd-devel-2.4.34-7.el6.1
httpd24-mod_session-2.4.34-7.el6.1
httpd24-httpd-2.4.34-7.el6.1
httpd24-mod_ssl-2.4.34-7.el6.1

noarch
httpd24-httpd-manual-2.4.34-7.el6.1

RHEL6WS
x86_64
httpd24-httpd-debuginfo-2.4.34-7.el6.1
httpd24-httpd-tools-2.4.34-7.el6.1
httpd24-mod_ldap-2.4.34-7.el6.1
httpd24-mod_proxy_html-2.4.34-7.el6.1
httpd24-httpd-devel-2.4.34-7.el6.1
httpd24-mod_session-2.4.34-7.el6.1
httpd24-httpd-2.4.34-7.el6.1
httpd24-mod_ssl-2.4.34-7.el6.1

noarch
httpd24-httpd-manual-2.4.34-7.el6.1

RHEL7S
noarch
httpd24-httpd-manual-2.4.34-7.el7.1

RHEL7WS
x86_64
httpd24-httpd-debuginfo-2.4.34-7.el7.1
httpd24-mod_auth_mellon-0.13.1-2.el7.1
httpd24-httpd-2.4.34-7.el7.1
httpd24-mod_ldap-2.4.34-7.el7.1

httpd24-mod_ssl-2.4.34-7.el7.1
httpd24-httpd-devel-2.4.34-7.el7.1
httpd24-httpd-tools-2.4.34-7.el7.1
httpd24-mod_session-2.4.34-7.el7.1
httpd24-mod_proxy_html-2.4.34-7.el7.1
httpd24-mod_auth_mellon-debuginfo-0.13.1-2.el7.1
httpd24-mod_md-2.4.34-7.el7.1

noarch
httpd24-httpd-manual-2.4.34-7.el7.1

24979 - (VMSA-2019-0002) VMware Workstation Pro Multiple Elevation Of Privilege Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2019-5511, CVE-2019-5512

Description

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

Observation

VMware Workstation Pro is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Pro. The flaws lie in multiple components. Successful exploitation could allow an attacker to gain elevated privileges on the host operating system

25018 - (HT209605) Apple iCloud Multiple Vulnerabilities Prior To 7.11

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

Risk Level: Medium

CVE: CVE-2019-6201, CVE-2019-6232, CVE-2019-6236, CVE-2019-7285, CVE-2019-7292, CVE-2019-8503, CVE-2019-8506, CVE-2019-8515, CVE-2019-8518, CVE-2019-8523, CVE-2019-8524, CVE-2019-8535, CVE-2019-8536, CVE-2019-8542, CVE-2019-8544, CVE-2019-8551, CVE-2019-8556, CVE-2019-8558, CVE-2019-8559, CVE-2019-8563

Description

Multiple vulnerabilities are present in some versions of Apple iCloud.

Observation

Apple iCloud is a manager for the Apple's cloud-based storage service.

Multiple vulnerabilities are present in some versions of Apple iCloud. The flaws lie in several components. Successful exploitation could allow an attacker to execute arbitrary code or retrieve sensitive information.

25025 - Cisco NX-OS Software 802.1X Extensible Authentication Protocol Over LAN Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-1594

Description

A vulnerability is present in Cisco NX-OS Software 802.1X protocol.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in Cisco NX-OS Software 802.1X protocol. Successful exploitation could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device.

131334 - Debian Linux 9.0 DSA-4429-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11071

Description

The scan detected that the host is missing the following update:
DSA-4429-1

Observation

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

http://www.debian.org/security/2019/dsa-4429

Debian 9.0
all
spip_3.1.4-4~deb9u2

147833 - SuSE Linux 42.3 openSUSE-SU-2019:1197-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10360, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1197-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00110.html

SuSE Linux 42.3
x86_64
libmagic1-debuginfo-5.22-16.1
file-5.22-16.1
libmagic1-32bit-5.22-16.1
libmagic1-5.22-16.1
file-debuginfo-5.22-16.1
libmagic1-debuginfo-32bit-5.22-16.1
file-devel-5.22-16.1
python-magic-5.22-16.1
file-debugsource-5.22-16.1
file-magic-5.22-16.1

i586
libmagic1-debuginfo-5.22-16.1
file-5.22-16.1
libmagic1-5.22-16.1
file-debuginfo-5.22-16.1
file-devel-5.22-16.1
python-magic-5.22-16.1
file-debugsource-5.22-16.1
file-magic-5.22-16.1

147834 - SuSE Linux 42.3 openSUSE-SU-2019:1213-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7572, CVE-2019-7573, CVE-2019-7574, CVE-2019-7575, CVE-2019-7576, CVE-2019-7577, CVE-2019-7578, CVE-2019-7635, CVE-2019-7636, CVE-2019-7637, CVE-2019-7638

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1213-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00126.html

SuSE Linux 42.3
x86_64
libSDL-1_2-0-32bit-1.2.15-20.3.1
libSDL-1_2-0-debuginfo-1.2.15-20.3.1
libSDL-devel-1.2.15-20.3.1
libSDL-1_2-0-1.2.15-20.3.1
libSDL-devel-32bit-1.2.15-20.3.1
SDL-debugsource-1.2.15-20.3.1
libSDL-1_2-0-debuginfo-32bit-1.2.15-20.3.1

i586
libSDL-1_2-0-debuginfo-1.2.15-20.3.1
libSDL-devel-1.2.15-20.3.1
libSDL-1_2-0-1.2.15-20.3.1
SDL-debugsource-1.2.15-20.3.1

147835 - SuSE Linux 15.0 openSUSE-SU-2019:1196-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000877, CVE-2018-1000878, CVE-2018-1000879, CVE-2018-1000880, CVE-2019-1000019, CVE-2019-1000020

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1196-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00112.html

SuSE Linux 15.0
x86_64
libarchive13-32bit-3.3.2-lp150.7.1
libarchive13-3.3.2-lp150.7.1
libarchive13-32bit-debuginfo-3.3.2-lp150.7.1
libarchive-devel-3.3.2-lp150.7.1
bsdtar-3.3.2-lp150.7.1
libarchive-debugsource-3.3.2-lp150.7.1
bsdtar-debuginfo-3.3.2-lp150.7.1
libarchive13-debuginfo-3.3.2-lp150.7.1

i586
libarchive13-3.3.2-lp150.7.1
libarchive-devel-3.3.2-lp150.7.1
bsdtar-3.3.2-lp150.7.1
libarchive-debugsource-3.3.2-lp150.7.1
bsdtar-debuginfo-3.3.2-lp150.7.1
libarchive13-debuginfo-3.3.2-lp150.7.1

147845 - SuSE Linux 15.0 openSUSE-SU-2019:1216-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19490, CVE-2018-19491, CVE-2018-19492

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1216-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00130.html

SuSE Linux 15.0
i586
gnuplot-debugsource-5.2.2-lp150.3.3.1
gnuplot-5.2.2-lp150.3.3.1
gnuplot-debuginfo-5.2.2-lp150.3.3.1

noarch
gnuplot-doc-5.2.2-lp150.3.3.1

x86_64
gnuplot-debugsource-5.2.2-lp150.3.3.1
gnuplot-5.2.2-lp150.3.3.1
gnuplot-debuginfo-5.2.2-lp150.3.3.1

160546 - CentOS 7 CESA-2019-0766 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3877, CVE-2019-3878

Description

The scan detected that the host is missing the following update:
CESA-2019-0766

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-April/023270.html

CentOS 7
x86_64
mod_auth_mellon-diagnostics-0.14.0-2.el7_6.4
mod_auth_mellon-0.14.0-2.el7_6.4

163844 - Oracle Enterprise Linux ELSA-2019-0766 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3877, CVE-2019-3878

Description

The scan detected that the host is missing the following update:
ELSA-2019-0766

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-April/008652.html

OEL7
x86_64
mod_auth_mellon-diagnostics-0.14.0-2.el7_6.4
mod_auth_mellon-0.14.0-2.el7_6.4

195043 - Fedora Linux 30 FEDORA-2019-2d8ee47f61 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3877, CVE-2019-3878

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2d8ee47f61

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/2019/4/?count=200&page=4

Fedora Core 30

mod_auth_mellon-0.14.2-1.fc30

195060 - Fedora Linux 30 FEDORA-2019-833466697f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1098, CVE-2018-1099, CVE-2018-16886

Description

The scan detected that the host is missing the following update:
FEDORA-2019-833466697f

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/2019/4/?count=200&page=3

Fedora Core 30

etcd-3.3.12-1.20190314gite1ca3b4.fc30

196291 - Red Hat Enterprise Linux RHSA-2019-0766 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3877, CVE-2019-3878

Description

The scan detected that the host is missing the following update:
RHSA-2019-0766

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-April/msg00015.html

RHEL7S
x86_64
mod_auth_mellon-debuginfo-0.14.0-2.el7_6.4
mod_auth_mellon-diagnostics-0.14.0-2.el7_6.4
mod_auth_mellon-0.14.0-2.el7_6.4

RHEL7WS
x86_64
mod_auth_mellon-debuginfo-0.14.0-2.el7_6.4
mod_auth_mellon-diagnostics-0.14.0-2.el7_6.4
mod_auth_mellon-0.14.0-2.el7_6.4

24924 - (K91026261) F5 BIG-IP BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2019-6594

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the TMM software Multi-Path TCP (MPTCP) component. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

24981 - Mozilla Firefox Vulnerabilities Prior To 66.0.1

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

Risk Level: Medium

CVE: CVE-2019-9810, CVE-2019-9813

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

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

25011 - (K94735334) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2018-10883

Description

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

Observation

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

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

25015 - Cisco IOS Software Short Message Service Denial of Service Vulnerability (cisco-sa-20190327-sms-dos)

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

Risk Level: Medium

CVE: CVE-2019-1747

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw lies in the Sierra Wireless WWAN Cellular Interface Module. Successful exploitation could allow an attacker to cause a denial of service.

132500 - Oracle VM OVMSA-2019-0013 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-15473

Description

The scan detected that the host is missing the following update:
OVMSA-2019-0013

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2019-April/000935.html
http://oss.oracle.com/pipermail/oraclevm-errata/2019-April/000934.html

OVM3.3
x86_64
openssh-server-5.3p1-124.el6_10
openssh-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10

OVM3.4
x86_64
openssh-server-5.3p1-124.el6_10
openssh-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10

147837 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:0928-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9628

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0928-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005324.html

SuSE SLES 12 SP3
x86_64
libxmltooling6-debuginfo-1.5.6-3.9.1
xmltooling-schemas-1.5.6-3.9.1
xmltooling-debugsource-1.5.6-3.9.1
libxmltooling6-1.5.6-3.9.1

SuSE SLES 12 SP4

x86_64
libxmltooling6-debuginfo-1.5.6-3.9.1
xmltooling-schemas-1.5.6-3.9.1
xmltooling-debugsource-1.5.6-3.9.1
libxmltooling6-1.5.6-3.9.1

147838 - SuSE Linux 42.3 openSUSE-SU-2019:1211-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5737

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1211-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00122.html

SuSE Linux 42.3
i586
nodejs10-10.15.2-5.2
nodejs10-debuginfo-10.15.2-5.2
nodejs10-debugsource-10.15.2-5.2
nodejs10-devel-10.15.2-5.2
npm10-10.15.2-5.2

noarch
nodejs10-docs-10.15.2-5.2

x86_64
nodejs10-10.15.2-5.2
nodejs10-debuginfo-10.15.2-5.2
nodejs10-debugsource-10.15.2-5.2
nodejs10-devel-10.15.2-5.2
npm10-10.15.2-5.2

147839 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0961-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0961-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005344.html

SuSE SLED 12 SP3
x86_64
python3-base-3.4.6-25.24.1
libpython3_4m1_0-3.4.6-25.24.1
python3-base-debugsource-3.4.6-25.24.1
python3-3.4.6-25.24.1
libpython3_4m1_0-debuginfo-3.4.6-25.24.1
python3-base-debuginfo-3.4.6-25.24.1
python3-debuginfo-3.4.6-25.24.1
python3-debugsource-3.4.6-25.24.1
python3-curses-3.4.6-25.24.1
python3-curses-debuginfo-3.4.6-25.24.1

SuSE SLED 12 SP4
x86_64
python3-base-3.4.6-25.24.1
libpython3_4m1_0-3.4.6-25.24.1
python3-base-debugsource-3.4.6-25.24.1
python3-3.4.6-25.24.1
libpython3_4m1_0-debuginfo-3.4.6-25.24.1
python3-base-debuginfo-3.4.6-25.24.1
python3-debuginfo-3.4.6-25.24.1
python3-debugsource-3.4.6-25.24.1
python3-curses-3.4.6-25.24.1
python3-curses-debuginfo-3.4.6-25.24.1

SuSE SLES 12 SP4
x86_64
python3-base-3.4.6-25.24.1
libpython3_4m1_0-3.4.6-25.24.1
python3-base-debugsource-3.4.6-25.24.1
python3-3.4.6-25.24.1
libpython3_4m1_0-debuginfo-3.4.6-25.24.1
python3-base-debuginfo-3.4.6-25.24.1
python3-debuginfo-3.4.6-25.24.1
python3-debugsource-3.4.6-25.24.1
python3-curses-3.4.6-25.24.1
python3-curses-debuginfo-3.4.6-25.24.1

SuSE SLES 12 SP3
x86_64
python3-base-3.4.6-25.24.1
libpython3_4m1_0-3.4.6-25.24.1
python3-base-debugsource-3.4.6-25.24.1
python3-3.4.6-25.24.1
libpython3_4m1_0-debuginfo-3.4.6-25.24.1
python3-base-debuginfo-3.4.6-25.24.1
python3-debuginfo-3.4.6-25.24.1
python3-debugsource-3.4.6-25.24.1
python3-curses-3.4.6-25.24.1
python3-curses-debuginfo-3.4.6-25.24.1

147840 - SuSE Linux 15.0 openSUSE-SU-2019:1198-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9918

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1198-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00111.html

SuSE Linux 15.0
i586
bluez-cups-debuginfo-5.48-lp150.4.10.1
bluez-test-debuginfo-5.48-lp150.4.10.1
bluez-5.48-lp150.4.10.1
bluez-test-5.48-lp150.4.10.1
bluez-debuginfo-5.48-lp150.4.10.1
bluez-debugsource-5.48-lp150.4.10.1
libbluetooth3-5.48-lp150.4.10.1
bluez-devel-5.48-lp150.4.10.1
libbluetooth3-debuginfo-5.48-lp150.4.10.1
bluez-cups-5.48-lp150.4.10.1

noarch
bluez-auto-enable-devices-5.48-lp150.4.10.1

x86_64
bluez-devel-32bit-5.48-lp150.4.10.1
bluez-debuginfo-5.48-lp150.4.10.1
bluez-test-debuginfo-5.48-lp150.4.10.1
bluez-cups-debuginfo-5.48-lp150.4.10.1
libbluetooth3-32bit-5.48-lp150.4.10.1
libbluetooth3-debuginfo-5.48-lp150.4.10.1
libbluetooth3-32bit-debuginfo-5.48-lp150.4.10.1
bluez-test-5.48-lp150.4.10.1
bluez-cups-5.48-lp150.4.10.1
bluez-devel-5.48-lp150.4.10.1
bluez-debugsource-5.48-lp150.4.10.1
bluez-5.48-lp150.4.10.1
libbluetooth3-5.48-lp150.4.10.1

147841 - SuSE Linux 42.3 openSUSE-SU-2019:1217-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3816, CVE-2019-3833

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1217-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00129.html

SuSE Linux 42.3

x86_64
libwsman3-debuginfo-2.6.7-4.3.1
openwsman-server-2.6.7-4.3.1
openwsman-ruby-docs-2.6.7-4.3.1
openwsman-debugsource-2.6.7-4.3.1
openwsman-java-2.6.7-4.3.1
openwsman-ruby-debuginfo-2.6.7-4.3.1
openwsman-python-debuginfo-2.6.7-4.3.1
winrs-2.6.7-4.3.1
openwsman-perl-debuginfo-2.6.7-4.3.1
openwsman-server-plugin-ruby-debuginfo-2.6.7-4.3.1
libwsman3-2.6.7-4.3.1
openwsman-server-debuginfo-2.6.7-4.3.1
libwsman_clientpp1-2.6.7-4.3.1
libwsman_clientpp-devel-2.6.7-4.3.1
libwsman-devel-2.6.7-4.3.1
openwsman-python-2.6.7-4.3.1
openwsman-server-plugin-ruby-2.6.7-4.3.1
libwsman_clientpp1-debuginfo-2.6.7-4.3.1
openwsman-ruby-2.6.7-4.3.1
openwsman-perl-2.6.7-4.3.1

147843 - SuSE Linux 15.0 openSUSE-SU-2019:1180-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3880

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1180-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00095.html

SuSE Linux 15.0
i586
samba-python-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-errors0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-winbind-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-policy0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
ctdb-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-errors-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-krb5pac0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
ldb-tools-debuginfo-1.2.4-lp150.10.1
libnetapi0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-nbt-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbldap-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbconf-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbconf0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-credentials0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-client-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
python-ldb-devel-1.2.4-lp150.10.1
ctdb-tests-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbconf0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1

ctdb-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libldb1-1.2.4-lp150.10.1
libwbclient0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc-samr0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-dsdb-modules-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-policy0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-passdb0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbclient0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libldb-devel-1.2.4-lp150.10.1
libsamba-credentials0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-nbt0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-test-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbclient0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libwbclient0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
ctdb-pcp-pmda-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libldb1-debuginfo-1.2.4-lp150.10.1
libsamba-util0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamdb0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamdb0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-krb5pac0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
python-ldb-debuginfo-1.2.4-lp150.10.1
libdcerpc-binding0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbldap2-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-krb5pac-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-credentials-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamdb-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libtevent-util-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libnetapi-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc-binding0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbclient-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
python3-ldb-debuginfo-1.2.4-lp150.10.1
libsamba-hostconfig0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-policy-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbldap2-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-hostconfig-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-debugsource-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
ctdb-pcp-pmda-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-kdc-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-hostconfig0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-util0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-errors0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libnetapi0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-passdb-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
ldb-tools-1.2.4-lp150.10.1
samba-client-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libwbclient-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
ldb-debugsource-1.2.4-lp150.10.1
libdcerpc-samr-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-standard-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-test-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-passdb0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-pidl-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
ctdb-tests-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
python3-ldb-1.2.4-lp150.10.1

samba-winbind-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libtevent-util0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-dsdb-modules-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-core-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libtevent-util0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
python3-ldb-devel-1.2.4-lp150.10.1
libndr-standard0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-libs-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-kdc-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc-samr0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-libs-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
python-ldb-1.2.4-lp150.10.1
libndr-nbt0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-python-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-standard0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-util-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1

noarch
samba-doc-4.7.11+git.153.b36ceaf2235-lp150.3.14.1

x86_64
libdcerpc-binding0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbclient0-32bit-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libnetapi0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbclient0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-policy0-32bit-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsmbclient0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-ceph-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-policy-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libnetapi0-32bit-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libwbclient0-32bit-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc-samr0-32bit-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libnetapi0-32bit-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-nbt0-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-hostconfig0-32bit-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libndr-krb5pac0-32bit-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
samba-client-32bit-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamdb0-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libtevent-util0-32bit-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libdcerpc-binding0-32bit-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-credentials0-32bit-debuginfo-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
libsamba-passdb-devel-4.7.11+git.153.b36ceaf2235-lp150.3.14.1
ctdb-4.7.11+git.153.b36ceaf2235-lp150.3.14.1

160544 - CentOS 6 CESA-2019-0711 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-15473

Description

The scan detected that the host is missing the following update:
CESA-2019-0711

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-April/023261.html

CentOS 6
x86_64
openssh-ldap-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
pam_ssh_agent_auth-0.9.3-124.el6_10
openssh-5.3p1-124.el6_10

i686
openssh-ldap-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
pam_ssh_agent_auth-0.9.3-124.el6_10
openssh-5.3p1-124.el6_10

160545 - CentOS 7 CESA-2019-0710 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
CESA-2019-0710

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-April/023268.html

CentOS 7
x86_64
python-libs-2.7.5-77.el7_6
tkinter-2.7.5-77.el7_6
python-test-2.7.5-77.el7_6
python-2.7.5-77.el7_6
python-debug-2.7.5-77.el7_6
python-tools-2.7.5-77.el7_6
python-devel-2.7.5-77.el7_6

i686
python-libs-2.7.5-77.el7_6

163841 - Oracle Enterprise Linux ELSA-2019-0711 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-15473

Description

The scan detected that the host is missing the following update:
ELSA-2019-0711

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-April/008635.html

OEL6
x86_64
openssh-ldap-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
pam_ssh_agent_auth-0.9.3-124.el6_10
openssh-5.3p1-124.el6_10

i386
openssh-ldap-5.3p1-124.el6_10
openssh-server-5.3p1-124.el6_10
openssh-clients-5.3p1-124.el6_10
openssh-askpass-5.3p1-124.el6_10
pam_ssh_agent_auth-0.9.3-124.el6_10
openssh-5.3p1-124.el6_10

163842 - Oracle Enterprise Linux ELSA-2019-0710 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
ELSA-2019-0710

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-April/008634.html

OEL7
x86_64
python-devel-2.7.5-77.0.1.el7_6
python-2.7.5-77.0.1.el7_6
python-tools-2.7.5-77.0.1.el7_6
python-debug-2.7.5-77.0.1.el7_6
tkinter-2.7.5-77.0.1.el7_6
python-libs-2.7.5-77.0.1.el7_6
python-test-2.7.5-77.0.1.el7_6

178731 - Gentoo Linux GLSA-201904-12 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-201904-12

Observation

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

https://security.gentoo.org/glsa/201904-12

Affected packages:
app-antivirus/clamav < 0.101.2

178732 - Gentoo Linux GLSA-201904-15 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-15

Observation

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

https://security.gentoo.org/glsa/201904-15

Affected packages:
media-libs/tiff < 4.0.10

178733 - Gentoo Linux GLSA-201904-16 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-201904-16

Observation

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

https://security.gentoo.org/glsa/201904-16

Affected packages:
dev-db/phpmyadmin < 4.8.4

178734 - Gentoo Linux GLSA-201904-13 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-201904-13

Observation

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

https://security.gentoo.org/glsa/201904-13

Affected packages:
dev-vcs/git < 2.20.1

178735 - Gentoo Linux GLSA-201904-14 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-201904-14

Observation

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

https://security.gentoo.org/glsa/201904-14

Affected packages:
net-libs/gnutls < 3.6.7

178736 - Gentoo Linux GLSA-201904-11 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-201904-11

Observation

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

https://security.gentoo.org/glsa/201904-11

Affected packages:
app-portage/emerge-delta-webrsync < 3.7.4
sys-apps/portage < 2.3.22

186659 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3944-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10743, CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499

Description

The scan detected that the host is missing the following update:
USN-3944-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004848.html

Ubuntu 16.04

wpasupplicant_2.4-0ubuntu6.4
hostapd_2.4-0ubuntu6.4

Ubuntu 18.10

hostapd_2.6-18ubuntu1.1
wpasupplicant_2.6-18ubuntu1.1

Ubuntu 14.04

wpasupplicant_2.1-0ubuntu1.7
hostapd_2.1-0ubuntu1.7

Ubuntu 18.04

wpasupplicant_2.6-15ubuntu2.2
hostapd_2.6-15ubuntu2.2

195040 - Fedora Linux 29 FEDORA-2019-b3ad0a302b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6251

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b3ad0a302b

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/2019/4/?count=200&page=1

Fedora Core 29

webkit2gtk3-2.24.1-1.fc29

195041 - Fedora Linux 28 FEDORA-2019-a3f67e2364 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9658

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a3f67e2364

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/2019/4/?count=200&page=4

Fedora Core 28

checkstyle-8.0-4.1.fc28

195042 - Fedora Linux 29 FEDORA-2019-da36d5d484 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19935

Description

The scan detected that the host is missing the following update:
FEDORA-2019-da36d5d484

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/2019/4/?count=200&page=3

Fedora Core 29

php-7.2.17-1.fc29

195044 - Fedora Linux 29 FEDORA-2019-e4405b4c9f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9658

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e4405b4c9f

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/2019/4/?count=200&page=4

Fedora Core 29

checkstyle-8.0-4.1.fc29

195045 - Fedora Linux 30 FEDORA-2019-cacf88eabf Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3870, CVE-2019-3880

Description

The scan detected that the host is missing the following update:
FEDORA-2019-cacf88eabf

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/2019/4/?count=200&page=3

Fedora Core 30

samba-4.10.2-0.fc30

195046 - Fedora Linux 30 FEDORA-2019-aef1dac6a0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10894, CVE-2019-10895, CVE-2019-10896, CVE-2019-10897, CVE-2019-10898, CVE-2019-10899, CVE-2019-10900, CVE-2019-10901, CVE-2019-10902, CVE-2019-10903

Description

The scan detected that the host is missing the following update:
FEDORA-2019-aef1dac6a0

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/2019/4/?count=200&page=2

Fedora Core 30

wireshark-3.0.1-1.fc30

195047 - Fedora Linux 28 FEDORA-2019-253da50ddd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19935

Description

The scan detected that the host is missing the following update:
FEDORA-2019-253da50ddd

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/2019/4/?count=200&page=3

Fedora Core 28

php-7.2.17-1.fc28

195052 - Fedora Linux 30 FEDORA-2019-d9a15be3ba Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11070, CVE-2019-6251

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d9a15be3ba

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/2019/4/?count=200&page=3

Fedora Core 30

webkit2gtk3-2.24.1-1.fc30

195056 - Fedora Linux 29 FEDORA-2019-9e67979b2a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19351, CVE-2018-19352, CVE-2019-10255, CVE-2019-9644

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9e67979b2a

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/2019/4/?count=200&page=4

Fedora Core 29

python-notebook-5.7.8-1.fc29

195059 - Fedora Linux 29 FEDORA-2019-db21b5f1d2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14629, CVE-2018-16841, CVE-2018-16851, CVE-2018-16852, CVE-2018-16853, CVE-2018-16857, CVE-2019-3870, CVE-2019-3880

Description

The scan detected that the host is missing the following update:
FEDORA-2019-db21b5f1d2

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/2019/4/?count=200&page=1

Fedora Core 29

samba-4.9.6-0.fc29

196290 - Red Hat Enterprise Linux RHSA-2019-0765 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
RHSA-2019-0765

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-April/msg00014.html

RHEL6S
x86_64
rh-python36-python-test-3.6.3-4.el6
rh-python36-python-libs-3.6.3-4.el6
rh-python36-python-3.6.3-4.el6
rh-python36-python-tools-3.6.3-4.el6
rh-python36-python-devel-3.6.3-4.el6
rh-python36-python-debuginfo-3.6.3-4.el6
rh-python36-python-debug-3.6.3-4.el6
rh-python36-python-tkinter-3.6.3-4.el6

RHEL6WS
x86_64
rh-python36-python-test-3.6.3-4.el6
rh-python36-python-libs-3.6.3-4.el6
rh-python36-python-3.6.3-4.el6
rh-python36-python-tools-3.6.3-4.el6

rh-python36-python-devel-3.6.3-4.el6
rh-python36-python-debuginfo-3.6.3-4.el6
rh-python36-python-debug-3.6.3-4.el6
rh-python36-python-tkinter-3.6.3-4.el6

RHEL7S
aarch64
rh-python36-python-devel-3.6.3-7.el7
rh-python36-python-debug-3.6.3-7.el7
rh-python36-python-debuginfo-3.6.3-7.el7
rh-python36-python-test-3.6.3-7.el7
rh-python36-python-tkinter-3.6.3-7.el7
rh-python36-python-tools-3.6.3-7.el7
rh-python36-python-libs-3.6.3-7.el7
rh-python36-python-3.6.3-7.el7

RHEL7WS
x86_64
rh-python36-python-devel-3.6.3-7.el7
rh-python36-python-debug-3.6.3-7.el7
rh-python36-python-debuginfo-3.6.3-7.el7
rh-python36-python-test-3.6.3-7.el7
rh-python36-python-tkinter-3.6.3-7.el7
rh-python36-python-tools-3.6.3-7.el7
rh-python36-python-libs-3.6.3-7.el7
rh-python36-python-3.6.3-7.el7

131332 - Debian Linux 9.0 DSA-4432-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3835, CVE-2019-3838

Description

The scan detected that the host is missing the following update:
DSA-4432-1

Observation

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

http://www.debian.org/security/2019/dsa-4432

Debian 9.0
all
ghostscript_9.26a~dfsg-0+deb9u2

147832 - SuSE Linux 42.3 openSUSE-SU-2019:1208-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1787, CVE-2019-1788, CVE-2019-1789

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1208-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00128.html

SuSE Linux 42.3
x86_64
clamav-0.100.3-35.1
clamav-debugsource-0.100.3-35.1
clamav-debuginfo-0.100.3-35.1

147836 - SuSE Linux 15.0 openSUSE-SU-2019:1199-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19967

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1199-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00114.html

SuSE Linux 15.0
x86_64
xen-tools-debuginfo-4.10.3_02-lp150.2.16.1
xen-tools-domU-4.10.3_02-lp150.2.16.1
xen-tools-4.10.3_02-lp150.2.16.1
xen-devel-4.10.3_02-lp150.2.16.1
xen-libs-debuginfo-4.10.3_02-lp150.2.16.1
xen-libs-32bit-debuginfo-4.10.3_02-lp150.2.16.1
xen-doc-html-4.10.3_02-lp150.2.16.1
xen-libs-4.10.3_02-lp150.2.16.1
xen-4.10.3_02-lp150.2.16.1
xen-tools-domU-debuginfo-4.10.3_02-lp150.2.16.1
xen-debugsource-4.10.3_02-lp150.2.16.1
xen-libs-32bit-4.10.3_02-lp150.2.16.1

i586
xen-tools-domU-4.10.3_02-lp150.2.16.1
xen-devel-4.10.3_02-lp150.2.16.1
xen-libs-debuginfo-4.10.3_02-lp150.2.16.1
xen-libs-4.10.3_02-lp150.2.16.1
xen-tools-domU-debuginfo-4.10.3_02-lp150.2.16.1
xen-debugsource-4.10.3_02-lp150.2.16.1

147842 - SuSE Linux 15.0 openSUSE-SU-2019:1210-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1787, CVE-2019-1788, CVE-2019-1789

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1210-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00125.html

SuSE Linux 15.0
x86_64
clamav-0.100.3-lp150.2.10.1
libclammspack0-0.100.3-lp150.2.10.1
libclamav7-0.100.3-lp150.2.10.1
clamav-debuginfo-0.100.3-lp150.2.10.1
clamav-devel-0.100.3-lp150.2.10.1
libclamav7-debuginfo-0.100.3-lp150.2.10.1
clamav-debugsource-0.100.3-lp150.2.10.1
libclammspack0-debuginfo-0.100.3-lp150.2.10.1

147844 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0948-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3840, CVE-2019-3886

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0948-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-April/005338.html

SuSE SLED 12 SP4
x86_64
libvirt-daemon-driver-storage-disk-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-mpath-4.0.0-8.9.1
libvirt-admin-4.0.0-8.9.1
libvirt-daemon-driver-storage-logical-4.0.0-8.9.1
libvirt-daemon-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-4.0.0-8.9.1
libvirt-daemon-driver-secret-4.0.0-8.9.1
libvirt-daemon-driver-storage-logical-debuginfo-4.0.0-8.9.1
libvirt-client-debuginfo-4.0.0-8.9.1
libvirt-doc-4.0.0-8.9.1
libvirt-daemon-driver-network-4.0.0-8.9.1
libvirt-daemon-config-nwfilter-4.0.0-8.9.1
libvirt-daemon-driver-storage-core-4.0.0-8.9.1
libvirt-daemon-driver-storage-rbd-4.0.0-8.9.1
libvirt-daemon-lxc-4.0.0-8.9.1
libvirt-daemon-driver-interface-4.0.0-8.9.1
libvirt-4.0.0-8.9.1

libvirt-debugsource-4.0.0-8.9.1
libvirt-daemon-xen-4.0.0-8.9.1
libvirt-daemon-driver-storage-core-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-nwfilter-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-disk-4.0.0-8.9.1
libvirt-daemon-driver-storage-iscsi-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-mpath-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-iscsi-4.0.0-8.9.1
libvirt-client-4.0.0-8.9.1
libvirt-daemon-driver-nodedev-debuginfo-4.0.0-8.9.1
libvirt-libs-4.0.0-8.9.1
libvirt-daemon-driver-lxc-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-nwfilter-4.0.0-8.9.1
libvirt-daemon-driver-lxc-4.0.0-8.9.1
libvirt-daemon-driver-network-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-scsi-4.0.0-8.9.1
libvirt-daemon-4.0.0-8.9.1
libvirt-daemon-driver-storage-rbd-debuginfo-4.0.0-8.9.1
libvirt-daemon-qemu-4.0.0-8.9.1
libvirt-daemon-driver-secret-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-interface-debuginfo-4.0.0-8.9.1
libvirt-daemon-config-network-4.0.0-8.9.1
libvirt-daemon-driver-libxl-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-libxl-4.0.0-8.9.1
libvirt-libs-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-qemu-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-qemu-4.0.0-8.9.1
libvirt-daemon-driver-nodedev-4.0.0-8.9.1
libvirt-admin-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-scsi-debuginfo-4.0.0-8.9.1

SuSE SLES 12 SP4
x86_64
libvirt-daemon-driver-storage-disk-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-mpath-4.0.0-8.9.1
libvirt-admin-4.0.0-8.9.1
libvirt-daemon-driver-storage-logical-4.0.0-8.9.1
libvirt-daemon-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-4.0.0-8.9.1
libvirt-daemon-driver-secret-4.0.0-8.9.1
libvirt-daemon-driver-storage-logical-debuginfo-4.0.0-8.9.1
libvirt-client-debuginfo-4.0.0-8.9.1
libvirt-doc-4.0.0-8.9.1
libvirt-daemon-driver-network-4.0.0-8.9.1
libvirt-daemon-config-nwfilter-4.0.0-8.9.1
libvirt-daemon-driver-storage-core-4.0.0-8.9.1
libvirt-nss-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-rbd-4.0.0-8.9.1
libvirt-daemon-lxc-4.0.0-8.9.1
libvirt-daemon-driver-interface-4.0.0-8.9.1
libvirt-4.0.0-8.9.1
libvirt-debugsource-4.0.0-8.9.1
libvirt-daemon-xen-4.0.0-8.9.1
libvirt-daemon-driver-storage-core-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-nwfilter-debuginfo-4.0.0-8.9.1
libvirt-daemon-hooks-4.0.0-8.9.1
libvirt-daemon-driver-storage-disk-4.0.0-8.9.1
libvirt-daemon-driver-storage-iscsi-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-mpath-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-iscsi-4.0.0-8.9.1

libvirt-client-4.0.0-8.9.1
libvirt-daemon-driver-nodedev-debuginfo-4.0.0-8.9.1
libvirt-lock-sanlock-debuginfo-4.0.0-8.9.1
libvirt-libs-4.0.0-8.9.1
libvirt-daemon-driver-lxc-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-nwfilter-4.0.0-8.9.1
libvirt-daemon-driver-lxc-4.0.0-8.9.1
libvirt-daemon-driver-network-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-scsi-4.0.0-8.9.1
libvirt-daemon-4.0.0-8.9.1
libvirt-daemon-driver-storage-rbd-debuginfo-4.0.0-8.9.1
libvirt-nss-4.0.0-8.9.1
libvirt-daemon-qemu-4.0.0-8.9.1
libvirt-daemon-driver-secret-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-interface-debuginfo-4.0.0-8.9.1
libvirt-daemon-config-network-4.0.0-8.9.1
libvirt-daemon-driver-libxl-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-libxl-4.0.0-8.9.1
libvirt-libs-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-qemu-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-qemu-4.0.0-8.9.1
libvirt-lock-sanlock-4.0.0-8.9.1
libvirt-daemon-driver-nodedev-4.0.0-8.9.1
libvirt-admin-debuginfo-4.0.0-8.9.1
libvirt-daemon-driver-storage-scsi-debuginfo-4.0.0-8.9.1

147848 - SuSE Linux 15.0 openSUSE-SU-2019:1200-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-8975

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1200-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00113.html

SuSE Linux 15.0
x86_64
netpbm-debuginfo-10.80.1-lp150.2.3.1
libnetpbm11-32bit-debuginfo-10.80.1-lp150.2.3.1
libnetpbm11-32bit-10.80.1-lp150.2.3.1
netpbm-debugsource-10.80.1-lp150.2.3.1
libnetpbm11-debuginfo-10.80.1-lp150.2.3.1
libnetpbm11-10.80.1-lp150.2.3.1
netpbm-10.80.1-lp150.2.3.1
libnetpbm-devel-10.80.1-lp150.2.3.1

i586
netpbm-debuginfo-10.80.1-lp150.2.3.1
netpbm-debugsource-10.80.1-lp150.2.3.1
libnetpbm11-debuginfo-10.80.1-lp150.2.3.1
libnetpbm11-10.80.1-lp150.2.3.1

netpbm-10.80.1-lp150.2.3.1
libnetpbm-devel-10.80.1-lp150.2.3.1

160547 - CentOS 6 CESA-2019-0717 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-13405

Description

The scan detected that the host is missing the following update:
CESA-2019-0717

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-April/023265.html

CentOS 6
i686
python-perf-2.6.32-754.12.1.el6
kernel-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-754.12.1.el6
kernel-firmware-2.6.32-754.12.1.el6
kernel-doc-2.6.32-754.12.1.el6

x86_64
python-perf-2.6.32-754.12.1.el6
kernel-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6

163843 - Oracle Enterprise Linux ELSA-2019-0717 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-13405

Description

The scan detected that the host is missing the following update:
ELSA-2019-0717

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-April/008641.html

OEL6
x86_64
kernel-firmware-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6
kernel-doc-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-abi-whitelists-2.6.32-754.12.1.el6
python-perf-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6
kernel-2.6.32-754.12.1.el6

i386
kernel-firmware-2.6.32-754.12.1.el6
kernel-headers-2.6.32-754.12.1.el6
kernel-debug-2.6.32-754.12.1.el6
perf-2.6.32-754.12.1.el6
kernel-doc-2.6.32-754.12.1.el6
kernel-devel-2.6.32-754.12.1.el6
kernel-abi-whitelists-2.6.32-754.12.1.el6
python-perf-2.6.32-754.12.1.el6
kernel-debug-devel-2.6.32-754.12.1.el6
kernel-2.6.32-754.12.1.el6

186657 - Ubuntu Linux 18.04 USN-3949-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
USN-3949-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004854.html

Ubuntu 18.04

openjdk-11-jdk_11.0.2+9-3ubuntu1~18.04.3
openjdk-11-jre_11.0.2+9-3ubuntu1~18.04.3

195050 - Fedora Linux 30 FEDORA-2019-3fa5db9e19 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3842

Description

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

FEDORA-2019-3fa5db9e19

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/2019/4/?count=200&page=4

Fedora Core 30

systemd-241-5.git3d835d0.fc30

195051 - Fedora Linux 29 FEDORA-2019-88f264563f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19840, CVE-2018-19841

Description

The scan detected that the host is missing the following update:
FEDORA-2019-88f264563f

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/2019/4/?count=200&page=1

Fedora Core 29

wavpack-5.1.0-12.fc29

195053 - Fedora Linux 29 FEDORA-2019-36ce1cb623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9844

Description

The scan detected that the host is missing the following update:
FEDORA-2019-36ce1cb623

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/2019/4/?count=200&page=2

Fedora Core 29

nodejs-simple-markdown-0.4.4-1.fc29

195055 - Fedora Linux 28 FEDORA-2019-8e7c71f45b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9844

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8e7c71f45b

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/2019/4/?count=200&page=3

Fedora Core 28

nodejs-simple-markdown-0.4.4-1.fc28

195057 - Fedora Linux 30 FEDORA-2019-c9cbbbb5c0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20096, CVE-2018-20097, CVE-2018-20098, CVE-2018-20099

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c9cbbbb5c0

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/2019/4/?count=200&page=2

Fedora Core 30

mingw-exiv2-0.27-3.fc30

195061 - Fedora Linux 30 FEDORA-2019-1315f2dc3a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19840, CVE-2018-19841

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1315f2dc3a

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/2019/4/?count=200&page=3

Fedora Core 30

wavpack-5.1.0-12.fc30

195063 - Fedora Linux 30 FEDORA-2019-8790e70a89 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9917

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8790e70a89

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/2019/4/?count=200&page=1

Fedora Core 30

znc-1.7.3-1.fc30

195064 - Fedora Linux 30 FEDORA-2019-982b97f553 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3887

Description

The scan detected that the host is missing the following update:
FEDORA-2019-982b97f553

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/2019/4/?count=200&page=3

Fedora Core 30

kernel-tools-5.0.7-300.fc30
kernel-5.0.7-300.fc30
kernel-headers-5.0.7-300.fc30

25030 - Cisco Nexus 9000 Series Fabric Switches Application-Centric Infrastructure Mode Arbitrary File Read Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2019-1588

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in improper validation mechanism. Successful exploitation could allow a local attacker to access or read arbitrary files of the affected system.

131333 - Debian Linux 9.0 DSA-4430-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499

Description

The scan detected that the host is missing the following update:
DSA-4430-1

Observation

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

http://www.debian.org/security/2019/dsa-4430

Debian 9.0
all
wpasupplicant_2:2.4-1+deb9u3
wpasupplicant-udeb_2:2.4-1+deb9u3
wpagui_2:2.4-1+deb9u3
hostapd_2:2.4-1+deb9u3

182951 - FreeBSD Gitlab Group Runner Registration Token Exposure (a0602fa0-5c1c-11e9-abd6-001b217b3468)

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

Risk Level: Low

CVE: CVE-2019-11000

Description

The scan detected that the host is missing the following update:
Gitlab -- Group Runner Registration Token Exposure (a0602fa0-5c1c-11e9-abd6-001b217b3468)

Observation

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

http://www.vuxml.org/freebsd/a0602fa0-5c1c-11e9-abd6-001b217b3468.html

Affected packages:
11.9.0 <= gitlab-ce < 11.9.7
11.8.0 <= gitlab-ce < 11.8.7
10.4.0 <= gitlab-ce < 11.7.11

182953 - FreeBSD Flash Player Multiple Vulnerabilities (45d89773-5b64-11e9-80ed-d43d7ef03aa6)

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

Risk Level: Low

CVE: CVE-2019-7096, CVE-2019-7108

Description

The scan detected that the host is missing the following update:
Flash Player -- multiple vulnerabilities (45d89773-5b64-11e9-80ed-d43d7ef03aa6)

Observation

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

http://www.vuxml.org/freebsd/45d89773-5b64-11e9-80ed-d43d7ef03aa6.html

Affected packages:
linux-flashplayer < 32.0.0.171

182954 - FreeBSD MySQL Multiple Vulnerabilities (4e1997e8-5de0-11e9-b95c-b499baebfeaf)

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:
MySQL -- multiple vulnerabilities (4e1997e8-5de0-11e9-b95c-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/4e1997e8-5de0-11e9-b95c-b499baebfeaf.html

Affected packages:
mariadb55-server < 5.5.64
mariadb101-server < 10.1.39
mariadb102-server < 10.2.23
mariadb103-server < 10.3.14
mysql56-server < 5.6.44
mysql57-server < 5.7.26
mysql80-server < 8.0.15
percona55-server < 5.5.64
percona56-server < 5.6.44
percona57-server < 5.7.26

182955 - FreeBSD jenkins Multiple Vulnerabilities (8e9c3f5a-715b-4336-8d05-19babef55e9e)

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:
jenkins -- multiple vulnerabilities (8e9c3f5a-715b-4336-8d05-19babef55e9e)

Observation

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

For more information see:

http://www.vuxml.org/freebsd/8e9c3f5a-715b-4336-8d05-19babef55e9e.html

Affected packages:
jenkins < 2.172
jenkins-lts < 2.164.2

195058 - Fedora Linux 29 FEDORA-2019-c308ad8ee5 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-2019-c308ad8ee5

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/2019/4/?count=200&page=1

Fedora Core 29

pcsc-lite-1.8.25-1.fc29

195066 - Fedora Linux 30 FEDORA-2019-aa7f37cd4d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1000108

Description

The scan detected that the host is missing the following update:
FEDORA-2019-aa7f37cd4d

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/2019/4/?count=200&page=2

Fedora Core 30

yaws-2.0.6-1.fc30

195067 - Fedora Linux 30 FEDORA-2019-ca49dfd42f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9494, CVE-2019-9495, CVE-2019-9496, CVE-2019-9497, CVE-2019-9498

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ca49dfd42f

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/2019/4/?count=200&page=1

Fedora Core 30

wpa_supplicant-2.7-5.fc30

182952 - FreeBSD wget Security Flaw In Caching Credentials Passed As A Part Of The URL (a737eb11-5cfc-11e9-ab87-8cec4bf8fcfb)

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

Risk Level: Low

CVE: CVE-2018-20483

Description

The scan detected that the host is missing the following update:
wget -- security flaw in caching credentials passed as a part of the URL (a737eb11-5cfc-11e9-ab87-8cec4bf8fcfb)

Observation

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

http://www.vuxml.org/freebsd/a737eb11-5cfc-11e9-ab87-8cec4bf8fcfb.html

Affected packages:
1.19 <= wget < 1.20.1

195054 - Fedora Linux 30 FEDORA-2019-248ad990b4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3500

Description

The scan detected that the host is missing the following update:
FEDORA-2019-248ad990b4

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/2019/4/?count=200&page=4

Fedora Core 30

aria2-1.34.0-4.fc30

135236 - Oracle Solaris 11.4.8.5.0 Update Is Not Installed (CVE-2019-2704)

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

Risk Level: Low

CVE: CVE-2019-2704

Description

The scan detected that the host is missing the following update:
SRU 11.4.8.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2525967.1&_adf.ctrl-state=9h6nepoah_4&_afrLoop=324277912399545

135237 - Oracle Solaris 11.4.6.4.0 Update Is Not Installed (CVE-2019-2577)

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

Risk Level: Low

CVE: CVE-2019-2577

Description

The scan detected that the host is missing the following update:
SRU 11.4.6.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2525967.1&_adf.ctrl-state=9h6nepoah_4&_afrLoop=324277912399545

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.

21165 - (K17075474) F5 BIG-IP Glibc Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-4429

Update Details

Documentation is updated

23325 - (K61223103) F5 BIG-IP Linux kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-9074

Update Details

Observation is updated Documentation is updated FASLScript is updated

89016 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-096-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-0211

Update Details
Risk is updated

182947 - FreeBSD Apache Multiple Vulnerabilities (cf2105c6-551b-11e9-b95c-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-0196, CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220

Update Details
Risk is updated

195015 - Fedora Linux 29 FEDORA-2019-119b14075a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220

Update Details
Risk is updated

195020 - Fedora Linux 30 FEDORA-2019-cf7695b470 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-0196, CVE-2019-0197, CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220

Update Details
Risk is updated

32622 - Oracle Solaris 143725-12 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2009-3563, CVE-2013-5211, CVE-2014-9295, CVE-2014-9296

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32623 - Oracle Solaris 143726-12 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Medium

CVE: CVE-2009-3563, CVE-2013-5211, CVE-2014-9295, CVE-2014-9296

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33145 - Oracle Solaris 150401-65 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5544, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122, CVE-2018-1171, CVE-2018-2710, CVE-2018-2717, CVE-2018-2764, CVE-2018-2903, CVE-2019-2544

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33057 - Oracle Solaris 147794-23 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2002-2443, CVE-2013-1417, CVE-2013-1418, CVE-2014-4341, CVE-2014-4342, CVE-2014-4345

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33066 - Oracle Solaris 147793-23 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2002-2443, CVE-2013-1417, CVE-2013-1418, CVE-2014-4341, CVE-2014-4342, CVE-2014-4345

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33146 - Oracle Solaris 148104-29 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5107, CVE-2012-0814

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33147 - Oracle Solaris 148105-29 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5107, CVE-2012-0814

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

131310 - Debian Linux 9.0 DSA-4407-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-9628

Update Details
Risk is updated

131329 - Debian Linux 9.0 DSA-4427-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-3880

Update Details
Risk is updated

141569 - Red Hat Enterprise Linux RHSA-2017-1202 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3139

Update Details
Risk is updated

160248 - CentOS 6 CESA-2017-1202 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3139

Update Details
Risk is updated

163344 - Oracle Enterprise Linux ELSA-2017-1202 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3139

Update Details
Risk is updated

170816 - Amazon Linux AMI ALAS-2017-833 Update Is Not Installed

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

CVE: CVE-2017-3139

Update Details

Risk is updated

175171 - Scientific Linux Security ERRATA Important: bind on SL6.x i386/x86_64 (1705-2507)

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

Risk Level: Medium

CVE: CVE-2017-3139

Update Details

Risk is updated

186616 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3921-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9628

Update Details

Risk is updated

186645 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3939-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3880

Update Details

Risk is updated

33162 - Oracle Solaris 150400-65 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122, CVE-2018-1171, CVE-2018-2710, CVE-2018-2717, CVE-2018-2764, CVE-2018-2903, CVE-2019-2544, CVE-2019-2545

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

131311 - Debian Linux 9.0 DSA-4406-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-0804

Update Details

Risk is updated

131326 - Debian Linux 9.0 DSA-4428-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-3842

Update Details
Risk is updated

147755 - SuSE Linux 15.0 openSUSE-SU-2019:1106-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-0804

Update Details
Risk is updated

147820 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0897-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-1787, CVE-2019-1788, CVE-2019-1789

Update Details
Risk is updated

182907 - FreeBSD Gitlab Multiple Vulnerabilities (43ee6c1d-29ee-11e9-82a1-001b217b3468)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-6796, CVE-2019-7353

Update Details
Risk is updated

186601 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3907-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-0804

Update Details
Risk is updated

186644 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3940-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium

CVE: CVE-2019-1787, CVE-2019-1788, CVE-2019-1789

Update Details

Risk is updated

195007 - Fedora Linux 30 FEDORA-2019-9effd63191 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-0804

Update Details

Risk is updated

33319 - Oracle Solaris 151913-14 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33323 - Oracle Solaris 151912-14 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33393 - Oracle Solaris 152925-21 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33394 - Oracle Solaris 152923-21 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33395 - Oracle Solaris 152926-21 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33396 - Oracle Solaris 152924-21 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33397 - Oracle Solaris 152927-12 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33398 - Oracle Solaris 152928-12 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details
Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

160532 - CentOS 7 CESA-2019-0597 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-0816

Update Details
Risk is updated

163825 - Oracle Enterprise Linux ELSA-2019-0597 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-0816

Update Details

Risk is updated

196271 - Red Hat Enterprise Linux RHSA-2019-0597 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-0816

Update Details

Risk 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.