2019-JAN-30
FSL version 7.6.93

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

147580 - SuSE Linux 15.0 openSUSE-SU-2019:0087-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6250

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0087-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00084.html

SuSE Linux 15.0
x86_64
zeromq-devel-4.2.3-lp150.2.10.1
zeromq-tools-debuginfo-4.2.3-lp150.2.10.1
zeromq-debugsource-4.2.3-lp150.2.10.1
libzmq5-debuginfo-4.2.3-lp150.2.10.1
libzmq5-4.2.3-lp150.2.10.1
zeromq-tools-4.2.3-lp150.2.10.1

182893 - FreeBSD libzmq4 Remote Code Execution Vulnerability (8e48365a-214d-11e9-9f8a-0050562a4d7b)

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

Risk Level: High

CVE: CVE-2019-6250

Description

The scan detected that the host is missing the following update:
libzmq4 -- Remote Code Execution Vulnerability (8e48365a-214d-11e9-9f8a-0050562a4d7b)

Observation

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

http://www.vuxml.org/freebsd/8e48365a-214d-11e9-9f8a-0050562a4d7b.html

Affected packages:
4.2.0 <= libzmq4 < 4.3.1

24633 - (JSA10889) Juniper Junos OS Jdhcpd Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-0055

Description

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

Observation

Juniper Junos OS is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos OS. The flaw lies in the jdhcpd service. Successful exploitation could allow a remote attacker to cause a denial of service condition in the target system.

24646 - Oracle WebCenter Portal Critical Patch Update January 2019

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

Risk Level: High

CVE: CVE-2018-1000180, CVE-2018-14718, CVE-2019-2427

Description

Multiple vulnerabilities are present in some versions of Oracle WebCenter Portal.

Observation

Oracle WebCenter Portal is a web platform that helps organizations in fast and easy creation of intranets, extranets, composite applications and self-service portals.

Multiple vulnerabilities are present in some versions of Oracle WebCenter Portal. The flaws lie in several components. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

24648 - (JSA10912) Juniper Junos OS RPD Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-0012

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in BGP module. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

24650 - Oracle VM VirtualBox Critical Patch Update January 2019

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

Risk Level: High

CVE: CVE-2018-0734, CVE-2018-3309, CVE-2019-2446, CVE-2019-2448, CVE-2019-2450, CVE-2019-2451, CVE-2019-2500, CVE-

2019-2501, CVE-2019-2504, CVE-2019-2505, CVE-2019-2506, CVE-2019-2508, CVE-2019-2509, CVE-2019-2511, CVE-2019-2520, CVE-2019-2521, CVE-2019-2522, CVE-2019-2523, CVE-2019-2524, CVE-2019-2525, CVE-2019-2526, CVE-2019-2527, CVE-2019-2548, CVE-2019-2552, CVE-2019-2553, CVE-2019-2554, CVE-2019-2555, CVE-2019-2556

Description

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

Observation

Oracle VM VirtualBox is a virtualization software.

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

24655 - Oracle WebLogic Server Critical Patch Update January 2019

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

Risk Level: High

CVE: CVE-2015-1832, CVE-2015-9251, CVE-2018-1000180, CVE-2019-2395, CVE-2019-2398, CVE-2019-2418, CVE-2019-2441, CVE-2019-2452

Description

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

Observation

Oracle WebLogic Server is a Java EE application server.

Multiple vulnerabilities are present in some versions of Oracle WebLogic Server. The flaws lie in several components. Successful exploitation could allow an attacker to disclose sensitive information or cause denial of service condition on the target system.

24659 - (HT209443) Apple iOS Multiple Vulnerabilities Prior To 12.1.3

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2019-6200, CVE-2019-6202, CVE-2019-6205, CVE-2019-6206, CVE-2019-6208, CVE-2019-6209, CVE-2019-6210, CVE-2019-6211, CVE-2019-6212, CVE-2019-6213, CVE-2019-6214, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6218, CVE-2019-6219, CVE-2019-6221, CVE-2019-6224, CVE-2019-6225, CVE-2019-6226, CVE-2019-6227, CVE-2019-6228, CVE-2019-6229, CVE-2019-6230, CVE-2019-6231, CVE-2019-6233, CVE-2019-6234, CVE-2019-6235

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

Apple iOS is the operating system used by Apple iPhone, iPad, and iPod touch.

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, execute arbitrary code or escalate privileges.

24668 - (HT209449) Apple Safari Vulnerabilities Prior To 12.0.3

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

Risk Level: High

CVE: CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226, CVE-2019-6227, CVE-2019-6228, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

Multiple vulnerabilities are present in some versions of Apple Safari. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a cross site scripting attack and execute arbitrary codes on the targeted system.

131280 - Debian Linux 9.0 DSA-4374-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15518, CVE-2018-19870, CVE-2018-19873

Description

The scan detected that the host is missing the following update:
DSA-4374-1

Observation

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

http://www.debian.org/security/2019/dsa-4374

Debian 9.0
all
qt5-gtk-platformtheme_5.7.1+dfsg-3+deb9u1
libqt5network5_5.7.1+dfsg-3+deb9u1
qtbase5-doc-html_5.7.1+dfsg-3+deb9u1
libqt5xml5_5.7.1+dfsg-3+deb9u1
libqt5concurrent5_5.7.1+dfsg-3+deb9u1
qtbase5-dev_5.7.1+dfsg-3+deb9u1
libqt5sql5-ibase_5.7.1+dfsg-3+deb9u1
libqt5sql5-mysql_5.7.1+dfsg-3+deb9u1
libqt5core5a_5.7.1+dfsg-3+deb9u1
qtbase5-dev-tools_5.7.1+dfsg-3+deb9u1
qt5-qmake_5.7.1+dfsg-3+deb9u1
libqt5test5_5.7.1+dfsg-3+deb9u1
libqt5sql5-tds_5.7.1+dfsg-3+deb9u1
qtbase5-doc_5.7.1+dfsg-3+deb9u1
qtbase5-private-dev_5.7.1+dfsg-3+deb9u1
libqt5sql5-sqlite_5.7.1+dfsg-3+deb9u1
libqt5dbus5_5.7.1+dfsg-3+deb9u1
libqt5opengl5-dev_5.7.1+dfsg-3+deb9u1
libqt5sql5-psql_5.7.1+dfsg-3+deb9u1
qtbase5-examples_5.7.1+dfsg-3+deb9u1
libqt5printsupport5_5.7.1+dfsg-3+deb9u1
libqt5widgets5_5.7.1+dfsg-3+deb9u1
libqt5sql5-odbc_5.7.1+dfsg-3+deb9u1
libqt5sql5_5.7.1+dfsg-3+deb9u1
libqt5opengl5_5.7.1+dfsg-3+deb9u1
libqt5gui5_5.7.1+dfsg-3+deb9u1
qt5-default_5.7.1+dfsg-3+deb9u1

147570 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0144-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6116

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0144-1

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-January/005061.html

SuSE SLED 12 SP3
x86_64
libspectre-debugsource-0.2.7-12.6.1
ghostscript-9.26a-23.19.1
ghostscript-debuginfo-9.26a-23.19.1
libspectre1-debuginfo-0.2.7-12.6.1
libspectre1-0.2.7-12.6.1
ghostscript-debugsource-9.26a-23.19.1
ghostscript-x11-9.26a-23.19.1
ghostscript-x11-debuginfo-9.26a-23.19.1

SuSE SLED 12 SP4
x86_64
libspectre-debugsource-0.2.7-12.6.1
ghostscript-9.26a-23.19.1
ghostscript-debuginfo-9.26a-23.19.1
libspectre1-debuginfo-0.2.7-12.6.1
libspectre1-0.2.7-12.6.1
ghostscript-debugsource-9.26a-23.19.1
ghostscript-x11-9.26a-23.19.1
ghostscript-x11-debuginfo-9.26a-23.19.1

SuSE SLES 12 SP4
x86_64
libspectre-debugsource-0.2.7-12.6.1
ghostscript-9.26a-23.19.1
ghostscript-debuginfo-9.26a-23.19.1
libspectre1-debuginfo-0.2.7-12.6.1
libspectre1-0.2.7-12.6.1
ghostscript-debugsource-9.26a-23.19.1
ghostscript-x11-9.26a-23.19.1
ghostscript-x11-debuginfo-9.26a-23.19.1

SuSE SLES 12 SP3
x86_64
libspectre-debugsource-0.2.7-12.6.1
ghostscript-9.26a-23.19.1
ghostscript-debuginfo-9.26a-23.19.1
libspectre1-debuginfo-0.2.7-12.6.1
libspectre1-0.2.7-12.6.1
ghostscript-debugsource-9.26a-23.19.1

ghostscript-x11-9.26a-23.19.1
ghostscript-x11-debuginfo-9.26a-23.19.1

147571 - SuSE Linux 42.3 openSUSE-SU-2019:0085-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20217

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0085-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00086.html

SuSE Linux 42.3
x86_64
krb5-debuginfo-32bit-1.12.5-22.1
krb5-debugsource-1.12.5-22.1
krb5-mini-devel-1.12.5-22.1
krb5-mini-debugsource-1.12.5-22.1
krb5-32bit-1.12.5-22.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-22.1
krb5-plugin-kdb-ldap-1.12.5-22.1
krb5-client-1.12.5-22.1
krb5-devel-32bit-1.12.5-22.1
krb5-debuginfo-1.12.5-22.1
krb5-plugin-preauth-otp-1.12.5-22.1
krb5-doc-1.12.5-22.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-22.1
krb5-mini-debuginfo-1.12.5-22.1
krb5-client-debuginfo-1.12.5-22.1
krb5-server-1.12.5-22.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-22.1
krb5-devel-1.12.5-22.1
krb5-server-debuginfo-1.12.5-22.1
krb5-mini-1.12.5-22.1
krb5-plugin-preauth-pkinit-1.12.5-22.1
krb5-1.12.5-22.1

i586
krb5-debugsource-1.12.5-22.1
krb5-mini-devel-1.12.5-22.1
krb5-mini-debugsource-1.12.5-22.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-22.1
krb5-plugin-kdb-ldap-1.12.5-22.1
krb5-client-1.12.5-22.1
krb5-debuginfo-1.12.5-22.1
krb5-plugin-preauth-otp-1.12.5-22.1
krb5-doc-1.12.5-22.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-22.1
krb5-mini-debuginfo-1.12.5-22.1
krb5-client-debuginfo-1.12.5-22.1
krb5-server-1.12.5-22.1

krb5-plugin-preauth-otp-debuginfo-1.12.5-22.1
krb5-devel-1.12.5-22.1
krb5-server-debuginfo-1.12.5-22.1
krb5-mini-1.12.5-22.1
krb5-plugin-preauth-pkinit-1.12.5-22.1
krb5-1.12.5-22.1

147572 - SuSE Linux 42.3 openSUSE-SU-2019:0097-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0097-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00093.html

SuSE Linux 42.3
i586
libudev-mini-devel-228-65.1
libsystemd0-mini-228-65.1
systemd-logger-228-65.1
systemd-mini-debugsource-228-65.1
udev-mini-debuginfo-228-65.1
systemd-mini-sysvinit-228-65.1
udev-228-65.1
systemd-mini-devel-228-65.1
systemd-mini-228-65.1
systemd-sysvinit-228-65.1
libudev-devel-228-65.1
nss-myhostname-debuginfo-228-65.1
systemd-devel-228-65.1
nss-mymachines-228-65.1
nss-mymachines-debuginfo-228-65.1
libudev-mini1-debuginfo-228-65.1
libsystemd0-debuginfo-228-65.1
libsystemd0-228-65.1
systemd-228-65.1
udev-debuginfo-228-65.1
systemd-debugsource-228-65.1
libsystemd0-mini-debuginfo-228-65.1
libudev-mini1-228-65.1
nss-myhostname-228-65.1
systemd-mini-debuginfo-228-65.1
libudev1-228-65.1
systemd-debuginfo-228-65.1
udev-mini-228-65.1
libudev1-debuginfo-228-65.1

noarch
systemd-bash-completion-228-65.1
systemd-mini-bash-completion-228-65.1

x86_64
systemd-32bit-228-65.1
libudev-mini-devel-228-65.1
libsystemd0-mini-228-65.1
systemd-logger-228-65.1
systemd-mini-debugsource-228-65.1
libudev1-debuginfo-32bit-228-65.1
udev-mini-debuginfo-228-65.1
systemd-mini-sysvinit-228-65.1
udev-228-65.1
nss-myhostname-32bit-228-65.1
systemd-mini-devel-228-65.1
systemd-mini-228-65.1
systemd-sysvinit-228-65.1
nss-myhostname-debuginfo-32bit-228-65.1
systemd-debuginfo-32bit-228-65.1
libsystemd0-debuginfo-32bit-228-65.1
libudev-devel-228-65.1
nss-myhostname-debuginfo-228-65.1
systemd-devel-228-65.1
libsystemd0-32bit-228-65.1
nss-mymachines-228-65.1
nss-mymachines-debuginfo-228-65.1
libudev-mini1-debuginfo-228-65.1
libsystemd0-debuginfo-228-65.1
libsystemd0-228-65.1
libudev1-32bit-228-65.1
systemd-228-65.1
udev-debuginfo-228-65.1
systemd-debugsource-228-65.1
libsystemd0-mini-debuginfo-228-65.1
libudev-mini1-228-65.1
nss-myhostname-228-65.1
systemd-mini-debuginfo-228-65.1
libudev1-228-65.1
systemd-debuginfo-228-65.1
udev-mini-228-65.1
libudev1-debuginfo-228-65.1

147576 - SuSE SLES 12 SP3 SUSE-SU-2019:0148-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16939, CVE-2018-1120, CVE-2018-16862, CVE-2018-16884, CVE-2018-19407, CVE-2018-19824, CVE-2018-19985, CVE-2018-20169, CVE-2018-3639, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0148-1

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-January/005060.html

SuSE SLES 12 SP3
x86_64

kernel-azure-4.4.170-4.22.1
kernel-azure-debugsource-4.4.170-4.22.1
kernel-azure-devel-4.4.170-4.22.1
kernel-syms-azure-4.4.170-4.22.1
kernel-azure-debuginfo-4.4.170-4.22.1
kernel-azure-base-debuginfo-4.4.170-4.22.1
kernel-azure-base-4.4.170-4.22.1

noarch
kernel-devel-azure-4.4.170-4.22.1
kernel-source-azure-4.4.170-4.22.1

147577 - SuSE Linux 42.3 openSUSE-SU-2019:0090-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0090-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00091.html

SuSE Linux 42.3
i586
PackageKit-backend-zypp-1.1.3-5.6.1
PackageKit-debuginfo-1.1.3-5.6.1
PackageKit-1.1.3-5.6.1
PackageKit-devel-debuginfo-1.1.3-5.6.1
libpackagekit-glib2-devel-1.1.3-5.6.1
PackageKit-gstreamer-plugin-1.1.3-5.6.1
PackageKit-gstreamer-plugin-debuginfo-1.1.3-5.6.1
PackageKit-backend-zypp-debuginfo-1.1.3-5.6.1
PackageKit-gtk3-module-1.1.3-5.6.1
libpackagekit-glib2-18-1.1.3-5.6.1
libpackagekit-glib2-18-debuginfo-1.1.3-5.6.1
typelib-1_0-PackageKitGlib-1_0-1.1.3-5.6.1
PackageKit-debugsource-1.1.3-5.6.1
PackageKit-devel-1.1.3-5.6.1
PackageKit-gtk3-module-debuginfo-1.1.3-5.6.1

noarch
PackageKit-lang-1.1.3-5.6.1
PackageKit-branding-upstream-1.1.3-5.6.1

x86_64
libpackagekit-glib2-18-32bit-1.1.3-5.6.1
PackageKit-backend-zypp-1.1.3-5.6.1
PackageKit-debuginfo-1.1.3-5.6.1
PackageKit-1.1.3-5.6.1
PackageKit-devel-debuginfo-1.1.3-5.6.1
libpackagekit-glib2-devel-32bit-1.1.3-5.6.1
libpackagekit-glib2-devel-1.1.3-5.6.1

PackageKit-gstreamer-plugin-1.1.3-5.6.1
libpackagekit-glib2-18-debuginfo-32bit-1.1.3-5.6.1
PackageKit-gstreamer-plugin-debuginfo-1.1.3-5.6.1
PackageKit-backend-zypp-debuginfo-1.1.3-5.6.1
PackageKit-gtk3-module-1.1.3-5.6.1
libpackagekit-glib2-18-1.1.3-5.6.1
libpackagekit-glib2-18-debuginfo-1.1.3-5.6.1
typelib-1_0-PackageKitGlib-1_0-1.1.3-5.6.1
PackageKit-debugsource-1.1.3-5.6.1
PackageKit-devel-1.1.3-5.6.1
PackageKit-gtk3-module-debuginfo-1.1.3-5.6.1

147578 - SuSE Linux 42.3 openSUSE-SU-2019:0096-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0886, CVE-2018-1000852, CVE-2018-8784, CVE-2018-8785, CVE-2018-8786, CVE-2018-8787, CVE-2018-8788, CVE-2018-8789

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0096-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00100.html

SuSE Linux 42.3
x86_64
libfreerdp2-2.0.0~git.1463131968.4e66df7-13.1
freerdp-2.0.0~git.1463131968.4e66df7-13.1
freerdp-debuginfo-2.0.0~git.1463131968.4e66df7-13.1
freerdp-debugsource-2.0.0~git.1463131968.4e66df7-13.1
freerdp-devel-2.0.0~git.1463131968.4e66df7-13.1
libfreerdp2-debuginfo-2.0.0~git.1463131968.4e66df7-13.1

i586
libfreerdp2-2.0.0~git.1463131968.4e66df7-13.1
freerdp-2.0.0~git.1463131968.4e66df7-13.1
freerdp-debuginfo-2.0.0~git.1463131968.4e66df7-13.1
freerdp-debugsource-2.0.0~git.1463131968.4e66df7-13.1
freerdp-devel-2.0.0~git.1463131968.4e66df7-13.1
libfreerdp2-debuginfo-2.0.0~git.1463131968.4e66df7-13.1

147581 - SuSE Linux 42.3 openSUSE-SU-2019:0084-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0734, CVE-2018-11763, CVE-2018-11784, CVE-2018-3309, CVE-2019-2446, CVE-2019-2448, CVE-2019-2450, CVE-2019-2451, CVE-2019-2500, CVE-2019-2501, CVE-2019-2504, CVE-2019-2505, CVE-2019-2506, CVE-2019-2508, CVE-2019-2509, CVE-2019-2511, CVE-2019-2520, CVE-2019-2521, CVE-2019-2522, CVE-2019-2523, CVE-2019-2524, CVE-2019-2525, CVE-2019-2526, CVE-2019-2527, CVE-2019-2548, CVE-2019-2552, CVE-2019-2553, CVE-2019-2554, CVE-2019-2555, CVE-2019-2556

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0084-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00087.html

SuSE Linux 42.3
x86_64
virtualbox-vnc-5.2.24-66.1
python-virtualbox-debuginfo-5.2.24-66.1
virtualbox-guest-tools-debuginfo-5.2.24-66.1
virtualbox-guest-tools-5.2.24-66.1
virtualbox-host-kmp-default-debuginfo-5.2.24_k4.4.165_81-66.1
virtualbox-websrv-debuginfo-5.2.24-66.1
python-virtualbox-5.2.24-66.1
virtualbox-websrv-5.2.24-66.1
virtualbox-guest-x11-debuginfo-5.2.24-66.1
virtualbox-host-kmp-default-5.2.24_k4.4.165_81-66.1
virtualbox-debuginfo-5.2.24-66.1
virtualbox-guest-kmp-default-debuginfo-5.2.24_k4.4.165_81-66.1
virtualbox-qt-5.2.24-66.1
virtualbox-qt-debuginfo-5.2.24-66.1
virtualbox-guest-x11-5.2.24-66.1
virtualbox-guest-kmp-default-5.2.24_k4.4.165_81-66.1
virtualbox-devel-5.2.24-66.1
virtualbox-debugsource-5.2.24-66.1
virtualbox-5.2.24-66.1

noarch
virtualbox-guest-desktop-icons-5.2.24-66.1
virtualbox-host-source-5.2.24-66.1
virtualbox-guest-source-5.2.24-66.1

147582 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0196-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12232, CVE-2018-14625, CVE-2018-16862, CVE-2018-16884, CVE-2018-18397, CVE-2018-19407, CVE-2018-19854, CVE-2018-19985, CVE-2018-20169, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0196-1

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-January/005069.html

SuSE SLED 12 SP4
x86_64
kernel-default-debuginfo-4.12.14-95.6.1
kernel-default-debugsource-4.12.14-95.6.1

kernel-default-4.12.14-95.6.1
kernel-syms-4.12.14-95.6.1
kernel-default-extra-4.12.14-95.6.1
kernel-default-devel-4.12.14-95.6.1
kernel-default-extra-debuginfo-4.12.14-95.6.1
kernel-default-devel-debuginfo-4.12.14-95.6.1

noarch
kernel-devel-4.12.14-95.6.1
kernel-macros-4.12.14-95.6.1
kernel-source-4.12.14-95.6.1

SuSE SLES 12 SP4
noarch
kernel-devel-4.12.14-95.6.1
kernel-macros-4.12.14-95.6.1
kernel-source-4.12.14-95.6.1

x86_64
kernel-default-debuginfo-4.12.14-95.6.1
kernel-default-4.12.14-95.6.1
kernel-default-base-debuginfo-4.12.14-95.6.1
kernel-syms-4.12.14-95.6.1
kernel-default-devel-debuginfo-4.12.14-95.6.1
kernel-default-devel-4.12.14-95.6.1
kernel-default-debugsource-4.12.14-95.6.1
kernel-default-base-4.12.14-95.6.1

147583 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0179-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000845

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0179-1

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-January/005065.html

SuSE SLES 12 SP3
noarch
avahi-lang-0.6.32-32.3.1

x86_64
avahi-debuginfo-32bit-0.6.32-32.3.1
libavahi-glib1-32bit-0.6.32-32.3.2
libavahi-client3-32bit-0.6.32-32.3.1
avahi-utils-debuginfo-0.6.32-32.3.1
libavahi-core7-0.6.32-32.3.1
libavahi-common3-0.6.32-32.3.1
libdns_sd-32bit-0.6.32-32.3.1
libavahi-client3-debuginfo-32bit-0.6.32-32.3.1
avahi-debugsource-0.6.32-32.3.1

avahi-0.6.32-32.3.1
libdns_sd-debuginfo-32bit-0.6.32-32.3.1
libdns_sd-debuginfo-0.6.32-32.3.1
libavahi-client3-0.6.32-32.3.1
avahi-glib2-debugsource-0.6.32-32.3.2
avahi-utils-0.6.32-32.3.1
libavahi-glib1-0.6.32-32.3.2
libavahi-core7-debuginfo-0.6.32-32.3.1
libavahi-glib1-debuginfo-32bit-0.6.32-32.3.2
libavahi-common3-32bit-0.6.32-32.3.1
avahi-debuginfo-0.6.32-32.3.1
libdns_sd-0.6.32-32.3.1
libavahi-glib1-debuginfo-0.6.32-32.3.2
libavahi-common3-debuginfo-0.6.32-32.3.1
libavahi-client3-debuginfo-0.6.32-32.3.1
libavahi-common3-debuginfo-32bit-0.6.32-32.3.1

SuSE SLES 12 SP4
noarch
avahi-lang-0.6.32-32.3.1

x86_64
avahi-debuginfo-32bit-0.6.32-32.3.1
libavahi-glib1-32bit-0.6.32-32.3.2
libavahi-client3-32bit-0.6.32-32.3.1
avahi-utils-debuginfo-0.6.32-32.3.1
libavahi-core7-0.6.32-32.3.1
libavahi-common3-0.6.32-32.3.1
libdns_sd-32bit-0.6.32-32.3.1
libavahi-client3-debuginfo-32bit-0.6.32-32.3.1
avahi-debugsource-0.6.32-32.3.1
avahi-0.6.32-32.3.1
libdns_sd-debuginfo-32bit-0.6.32-32.3.1
libdns_sd-debuginfo-0.6.32-32.3.1
libavahi-client3-0.6.32-32.3.1
avahi-glib2-debugsource-0.6.32-32.3.2
avahi-utils-0.6.32-32.3.1
libavahi-glib1-0.6.32-32.3.2
libavahi-core7-debuginfo-0.6.32-32.3.1
libavahi-glib1-debuginfo-32bit-0.6.32-32.3.2
libavahi-common3-32bit-0.6.32-32.3.1
avahi-debuginfo-0.6.32-32.3.1
libdns_sd-0.6.32-32.3.1
libavahi-glib1-debuginfo-0.6.32-32.3.2
libavahi-common3-debuginfo-0.6.32-32.3.1
libavahi-client3-debuginfo-0.6.32-32.3.1
libavahi-common3-debuginfo-32bit-0.6.32-32.3.1

SuSE SLED 12 SP4
x86_64
avahi-0.6.32-32.3.1
libavahi-glib1-debuginfo-32bit-0.6.32-32.3.2
libavahi-client3-debuginfo-32bit-0.6.32-32.3.1
libavahi-gobject0-debuginfo-0.6.32-32.3.2
libdns_sd-32bit-0.6.32-32.3.1
libavahi-common3-debuginfo-32bit-0.6.32-32.3.1
libdns_sd-debuginfo-32bit-0.6.32-32.3.1
libavahi-gobject0-0.6.32-32.3.2
libavahi-client3-32bit-0.6.32-32.3.1
libavahi-ui0-0.6.32-32.3.2

libavahi-glib1-0.6.32-32.3.2
libavahi-core7-0.6.32-32.3.1
avahi-debugsource-0.6.32-32.3.1
libavahi-common3-32bit-0.6.32-32.3.1
avahi-debuginfo-0.6.32-32.3.1
libavahi-glib1-32bit-0.6.32-32.3.2
avahi-debuginfo-32bit-0.6.32-32.3.1
libdns_sd-0.6.32-32.3.1
libavahi-common3-debuginfo-0.6.32-32.3.1
avahi-glib2-debugsource-0.6.32-32.3.2
libavahi-ui-gtk3-0-0.6.32-32.3.2
libavahi-glib1-debuginfo-0.6.32-32.3.2
libavahi-ui0-debuginfo-0.6.32-32.3.2
libavahi-ui-gtk3-0-debuginfo-0.6.32-32.3.2
libdns_sd-debuginfo-0.6.32-32.3.1
libavahi-common3-0.6.32-32.3.1
libavahi-core7-debuginfo-0.6.32-32.3.1
libavahi-client3-0.6.32-32.3.1
libavahi-client3-debuginfo-0.6.32-32.3.1

noarch
avahi-lang-0.6.32-32.3.1

SuSE SLED 12 SP3
x86_64
avahi-0.6.32-32.3.1
libavahi-glib1-debuginfo-32bit-0.6.32-32.3.2
libavahi-client3-debuginfo-32bit-0.6.32-32.3.1
libavahi-gobject0-debuginfo-0.6.32-32.3.2
libdns_sd-32bit-0.6.32-32.3.1
libavahi-common3-debuginfo-32bit-0.6.32-32.3.1
libdns_sd-debuginfo-32bit-0.6.32-32.3.1
libavahi-gobject0-0.6.32-32.3.2
libavahi-client3-32bit-0.6.32-32.3.1
libavahi-ui0-0.6.32-32.3.2
libavahi-glib1-0.6.32-32.3.2
libavahi-core7-0.6.32-32.3.1
avahi-debugsource-0.6.32-32.3.1
libavahi-common3-32bit-0.6.32-32.3.1
avahi-debuginfo-0.6.32-32.3.1
libavahi-glib1-32bit-0.6.32-32.3.2
avahi-debuginfo-32bit-0.6.32-32.3.1
libdns_sd-0.6.32-32.3.1
libavahi-common3-debuginfo-0.6.32-32.3.1
avahi-glib2-debugsource-0.6.32-32.3.2
libavahi-ui-gtk3-0-0.6.32-32.3.2
libavahi-glib1-debuginfo-0.6.32-32.3.2
libavahi-ui0-debuginfo-0.6.32-32.3.2
libavahi-ui-gtk3-0-debuginfo-0.6.32-32.3.2
libdns_sd-debuginfo-0.6.32-32.3.1
libavahi-common3-0.6.32-32.3.1
libavahi-core7-debuginfo-0.6.32-32.3.1
libavahi-client3-0.6.32-32.3.1
libavahi-client3-debuginfo-0.6.32-32.3.1

noarch
avahi-lang-0.6.32-32.3.1

147585 - SuSE Linux 15.0 openSUSE-SU-2019:0098-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16864, CVE-2018-16865, CVE-2018-16866, CVE-2018-6954

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0098-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00096.html

SuSE Linux 15.0
i586
libudev-mini-devel-234-lp150.20.12.1
libsystemd0-mini-debuginfo-234-lp150.20.12.1
systemd-mini-debugsource-234-lp150.20.12.1
systemd-mini-container-mini-debuginfo-234-lp150.20.12.1
systemd-mini-devel-234-lp150.20.12.1
udev-234-lp150.20.12.1
nss-myhostname-234-lp150.20.12.1
nss-systemd-debuginfo-234-lp150.20.12.1
nss-mymachines-234-lp150.20.12.1
libudev-devel-234-lp150.20.12.1
systemd-mini-234-lp150.20.12.1
libudev-mini1-debuginfo-234-lp150.20.12.1
systemd-mini-coredump-mini-debuginfo-234-lp150.20.12.1
libudev-mini1-234-lp150.20.12.1
systemd-mini-debuginfo-234-lp150.20.12.1
nss-systemd-234-lp150.20.12.1
systemd-mini-coredump-mini-234-lp150.20.12.1
udev-mini-234-lp150.20.12.1
libsystemd0-234-lp150.20.12.1
systemd-coredump-234-lp150.20.12.1
systemd-container-debuginfo-234-lp150.20.12.1
libudev1-debuginfo-234-lp150.20.12.1
nss-myhostname-debuginfo-234-lp150.20.12.1
systemd-container-234-lp150.20.12.1
systemd-debuginfo-234-lp150.20.12.1
systemd-sysvinit-234-lp150.20.12.1
udev-mini-debuginfo-234-lp150.20.12.1
systemd-234-lp150.20.12.1
systemd-logger-234-lp150.20.12.1
libsystemd0-debuginfo-234-lp150.20.12.1
udev-debuginfo-234-lp150.20.12.1
libsystemd0-mini-234-lp150.20.12.1
systemd-debugsource-234-lp150.20.12.1
systemd-mini-container-mini-234-lp150.20.12.1
nss-mymachines-debuginfo-234-lp150.20.12.1
libudev1-234-lp150.20.12.1
systemd-coredump-debuginfo-234-lp150.20.12.1
systemd-devel-234-lp150.20.12.1
systemd-mini-sysvinit-234-lp150.20.12.1

noarch
systemd-bash-completion-234-lp150.20.12.1
systemd-mini-bash-completion-234-lp150.20.12.1

x86_64
nss-myhostname-32bit-234-lp150.20.12.1
libudev-mini-devel-234-lp150.20.12.1
systemd-32bit-234-lp150.20.12.1
libudev1-32bit-234-lp150.20.12.1
libsystemd0-mini-debuginfo-234-lp150.20.12.1
libudev1-32bit-debuginfo-234-lp150.20.12.1
systemd-mini-debugsource-234-lp150.20.12.1
nss-myhostname-32bit-debuginfo-234-lp150.20.12.1
systemd-mini-container-mini-debuginfo-234-lp150.20.12.1
systemd-mini-devel-234-lp150.20.12.1
udev-234-lp150.20.12.1
nss-mymachines-32bit-debuginfo-234-lp150.20.12.1
nss-myhostname-234-lp150.20.12.1
libsystemd0-32bit-234-lp150.20.12.1
nss-systemd-debuginfo-234-lp150.20.12.1
nss-mymachines-234-lp150.20.12.1
libudev-devel-234-lp150.20.12.1
systemd-mini-234-lp150.20.12.1
libudev-mini1-debuginfo-234-lp150.20.12.1
systemd-mini-coredump-mini-debuginfo-234-lp150.20.12.1
libudev-mini1-234-lp150.20.12.1
nss-mymachines-32bit-234-lp150.20.12.1
systemd-mini-debuginfo-234-lp150.20.12.1
nss-systemd-234-lp150.20.12.1
systemd-mini-coredump-mini-234-lp150.20.12.1
udev-mini-234-lp150.20.12.1
libsystemd0-234-lp150.20.12.1
systemd-coredump-234-lp150.20.12.1
libsystemd0-32bit-debuginfo-234-lp150.20.12.1
systemd-container-debuginfo-234-lp150.20.12.1
libudev1-debuginfo-234-lp150.20.12.1
nss-myhostname-debuginfo-234-lp150.20.12.1
systemd-container-234-lp150.20.12.1
systemd-debuginfo-234-lp150.20.12.1
systemd-sysvinit-234-lp150.20.12.1
udev-mini-debuginfo-234-lp150.20.12.1
systemd-234-lp150.20.12.1
systemd-logger-234-lp150.20.12.1
libsystemd0-debuginfo-234-lp150.20.12.1
udev-debuginfo-234-lp150.20.12.1
libsystemd0-mini-234-lp150.20.12.1
systemd-debugsource-234-lp150.20.12.1
systemd-32bit-debuginfo-234-lp150.20.12.1
systemd-mini-container-mini-234-lp150.20.12.1
nss-mymachines-debuginfo-234-lp150.20.12.1
libudev1-234-lp150.20.12.1
systemd-coredump-debuginfo-234-lp150.20.12.1
systemd-devel-234-lp150.20.12.1
systemd-mini-sysvinit-234-lp150.20.12.1
libudev-devel-32bit-234-lp150.20.12.1

147587 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0146-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-4437, CVE-2018-4438, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4464

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0146-1

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-January/005058.html

SuSE SLES 12 SP3
x86_64
webkit2gtk-4_0-injected-bundles-2.22.5-2.32.2
libwebkit2gtk-4_0-37-2.22.5-2.32.2
libjavascriptcoregtk-4_0-18-2.22.5-2.32.2
libwebkit2gtk-4_0-37-debuginfo-2.22.5-2.32.2
webkit2gtk3-debugsource-2.22.5-2.32.2
typelib-1_0-WebKit2-4_0-2.22.5-2.32.2
libjavascriptcoregtk-4_0-18-debuginfo-2.22.5-2.32.2
typelib-1_0-JavaScriptCore-4_0-2.22.5-2.32.2
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.5-2.32.2

SuSE SLES 12 SP4
x86_64
webkit2gtk-4_0-injected-bundles-2.22.5-2.32.2
libwebkit2gtk-4_0-37-2.22.5-2.32.2
libjavascriptcoregtk-4_0-18-2.22.5-2.32.2
libwebkit2gtk-4_0-37-debuginfo-2.22.5-2.32.2
webkit2gtk3-debugsource-2.22.5-2.32.2
typelib-1_0-WebKit2-4_0-2.22.5-2.32.2
libjavascriptcoregtk-4_0-18-debuginfo-2.22.5-2.32.2
typelib-1_0-JavaScriptCore-4_0-2.22.5-2.32.2
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.5-2.32.2

SuSE SLED 12 SP4
x86_64
webkit2gtk-4_0-injected-bundles-2.22.5-2.32.2
libwebkit2gtk-4_0-37-2.22.5-2.32.2
libjavascriptcoregtk-4_0-18-2.22.5-2.32.2
libwebkit2gtk-4_0-37-debuginfo-2.22.5-2.32.2
webkit2gtk3-debugsource-2.22.5-2.32.2
typelib-1_0-WebKit2-4_0-2.22.5-2.32.2
libjavascriptcoregtk-4_0-18-debuginfo-2.22.5-2.32.2
typelib-1_0-JavaScriptCore-4_0-2.22.5-2.32.2
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.5-2.32.2

noarch
libwebkit2gtk3-lang-2.22.5-2.32.2

SuSE SLED 12 SP3
x86_64
webkit2gtk-4_0-injected-bundles-2.22.5-2.32.2
libwebkit2gtk-4_0-37-2.22.5-2.32.2
libjavascriptcoregtk-4_0-18-2.22.5-2.32.2
libwebkit2gtk-4_0-37-debuginfo-2.22.5-2.32.2
webkit2gtk3-debugsource-2.22.5-2.32.2
typelib-1_0-WebKit2-4_0-2.22.5-2.32.2
libjavascriptcoregtk-4_0-18-debuginfo-2.22.5-2.32.2
typelib-1_0-JavaScriptCore-4_0-2.22.5-2.32.2

webkit2gtk-4_0-injected-bundles-debuginfo-2.22.5-2.32.2

noarch
libwebkit2gtk3-lang-2.22.5-2.32.2

160505 - CentOS 7 CESA-2019-0109 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18311

Description

The scan detected that the host is missing the following update:
CESA-2019-0109

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-January/023148.html

CentOS 7
i686
perl-devel-5.16.3-294.el7_6
perl-libs-5.16.3-294.el7_6

noarch
perl-ExtUtils-Embed-1.30-294.el7_6
perl-Module-CoreList-2.76.02-294.el7_6
perl-Object-Accessor-0.42-294.el7_6
perl-ExtUtils-Install-1.58-294.el7_6
perl-Package-Constants-0.02-294.el7_6
perl-Module-Loaded-0.08-294.el7_6
perl-CPAN-1.9800-294.el7_6
perl-IO-Zlib-1.10-294.el7_6
perl-Locale-Maketext-Simple-0.21-294.el7_6
perl-ExtUtils-CBuilder-0.28.2.6-294.el7_6
perl-Pod-Escapes-1.04-294.el7_6

x86_64
perl-5.16.3-294.el7_6
perl-Time-Piece-1.20.1-294.el7_6
perl-devel-5.16.3-294.el7_6
perl-core-5.16.3-294.el7_6
perl-macros-5.16.3-294.el7_6
perl-libs-5.16.3-294.el7_6
perl-tests-5.16.3-294.el7_6

171063 - Amazon Linux AMI ALAS-2019-1148 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16839, CVE-2018-16840, CVE-2018-16842

Description

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

ALAS-2019-1148

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1148.html

Amazon Linux AMI
x86_64
curl-debuginfo-7.53.1-16.86.amzn1
libcurl-7.53.1-16.86.amzn1
libcurl-devel-7.53.1-16.86.amzn1
curl-7.53.1-16.86.amzn1

i686
curl-debuginfo-7.53.1-16.86.amzn1
libcurl-7.53.1-16.86.amzn1
libcurl-devel-7.53.1-16.86.amzn1
curl-7.53.1-16.86.amzn1

171064 - Amazon Linux AMI ALAS-2019-1149 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16884

Description

The scan detected that the host is missing the following update:
ALAS-2019-1149

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1149.html

Amazon Linux AMI
x86_64
kernel-4.14.94-73.73.amzn1
kernel-debuginfo-common-x86_64-4.14.94-73.73.amzn1
kernel-tools-4.14.94-73.73.amzn1
kernel-tools-devel-4.14.94-73.73.amzn1
perf-debuginfo-4.14.94-73.73.amzn1
perf-4.14.94-73.73.amzn1
kernel-debuginfo-4.14.94-73.73.amzn1
kernel-headers-4.14.94-73.73.amzn1
kernel-devel-4.14.94-73.73.amzn1
kernel-tools-debuginfo-4.14.94-73.73.amzn1

i686
kernel-devel-4.14.94-73.73.amzn1
kernel-tools-4.14.94-73.73.amzn1
kernel-debuginfo-4.14.94-73.73.amzn1
perf-debuginfo-4.14.94-73.73.amzn1
perf-4.14.94-73.73.amzn1
kernel-tools-devel-4.14.94-73.73.amzn1

kernel-headers-4.14.94-73.73.amzn1
kernel-4.14.94-73.73.amzn1
kernel-debuginfo-common-i686-4.14.94-73.73.amzn1
kernel-tools-debuginfo-4.14.94-73.73.amzn1

186550 - Ubuntu Linux 18.04 USN-3871-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10876, CVE-2018-10877, CVE-2018-10878, CVE-2018-10879, CVE-2018-10880, CVE-2018-10882, CVE-2018-10883, CVE-2018-14625, CVE-2018-16882, CVE-2018-17972, CVE-2018-18281, CVE-2018-19407, CVE-2018-9516

Description

The scan detected that the host is missing the following update:
USN-3871-1

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-January/004744.html

Ubuntu 18.04

linux-image-4.15.0-44-generic_4.15.0-44.47
linux-image-snapdragon_4.15.0.44.46
linux-image-generic_4.15.0.44.46
linux-image-4.15.0-44-lowlatency_4.15.0-44.47
linux-image-lowlatency_4.15.0.44.46
linux-image-4.15.0-44-generic-lpae_4.15.0-44.47
linux-image-generic-lpae_4.15.0.44.46
linux-image-4.15.0-44-snapdragon_4.15.0-44.47

194712 - Fedora Linux 29 FEDORA-2019-376ecc221c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8641, CVE-2018-13441, CVE-2018-13457, CVE-2018-13458, CVE-2018-18245

Description

The scan detected that the host is missing the following update:
FEDORA-2019-376ecc221c

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

Fedora Core 29

nagios-4.4.3-1.fc29

194719 - Fedora Linux 29 FEDORA-2019-3c45bd2cc3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15518, CVE-2018-19869, CVE-2018-19870, CVE-2018-19871, CVE-2018-19873

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3c45bd2cc3

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

Fedora Core 29

mingw-sip-4.19.13-2.fc29
mingw-qt5-qtserialport-5.11.3-1.fc29
mingw-qt5-qtscript-5.11.3-1.fc29
mingw-qt5-qt3d-5.11.3-1.fc29
mingw-qt5-qtsensors-5.11.3-1.fc29
mingw-qt5-qttranslations-5.11.3-1.fc29
mingw-qt5-qtmultimedia-5.11.3-1.fc29
mingw-qt5-qtgraphicaleffects-5.11.3-1.fc29
mingw-qt5-qtbase-5.11.3-1.fc29
mingw-qt5-qtsvg-5.11.3-1.fc29
mingw-qt5-qttools-5.11.3-1.fc29
mingw-qt5-qtcharts-5.11.3-1.fc29
mingw-qt5-qtquickcontrols-5.11.3-1.fc29
mingw-python-qt5-5.11.3-2.fc29
mingw-qt5-qtactiveqt-5.11.3-1.fc29
mingw-qt5-qtwebsockets-5.11.3-1.fc29
mingw-qt5-qtimageformats-5.11.3-1.fc29
mingw-qt5-qtlocation-5.11.3-1.fc29
mingw-qt5-qtxmlpatterns-5.11.3-1.fc29
mingw-qt5-qtdeclarative-5.11.3-1.fc29
mingw-qt5-qtwinextras-5.11.3-1.fc29
mingw-qt5-qtwebkit-5.9.4-0.8.gitbd0657f.fc29

194724 - Fedora Linux 28 FEDORA-2019-0b44528ff1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8641, CVE-2018-13441, CVE-2018-13457, CVE-2018-13458, CVE-2018-18245

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0b44528ff1

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

Fedora Core 28

nagios-4.4.3-1.fc28

194726 - Fedora Linux 29 FEDORA-2019-427a0ba9e3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2018-20483

Description

The scan detected that the host is missing the following update:
FEDORA-2019-427a0ba9e3

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/2019/1/?count=200&page=2

Fedora Core 29

curl-7.61.1-7.fc29

24657 - (JSA10911) Juniper Junos OS Kernel Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0011

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in kernel. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

24662 - Oracle Database Server Critical Patch Update January 2019

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

Risk Level: Medium

CVE: CVE-2019-2406, CVE-2019-2444, CVE-2019-2547

Description

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

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to compromise Core RDBMS and Java VM on the target.

24663 - Oracle Database Server Critical Patch Update January 2019

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-2406, CVE-2019-2444, CVE-2019-2547

Description

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

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to compromise Core RDBMS and Java VM on the target.

147569 - SuSE Linux 15.0 openSUSE-SU-2019:0100-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3807

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0100-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00098.html

SuSE Linux 15.0
x86_64
pdns-recursor-debuginfo-4.1.2-lp150.2.6.1
pdns-recursor-4.1.2-lp150.2.6.1
pdns-recursor-debugsource-4.1.2-lp150.2.6.1

147573 - SuSE Linux 42.3 openSUSE-SU-2019:0088-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-0734, CVE-2018-12116, CVE-2018-12120, CVE-2018-12121, CVE-2018-12122, CVE-2018-12123, CVE-2018-5407

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0088-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00088.html

SuSE Linux 42.3

i586
nodejs4-debuginfo-4.9.1-20.1
nodejs4-debugsource-4.9.1-20.1
nodejs4-4.9.1-20.1
npm4-4.9.1-20.1
nodejs4-devel-4.9.1-20.1

noarch
nodejs4-docs-4.9.1-20.1

x86_64
nodejs4-debuginfo-4.9.1-20.1
nodejs4-debugsource-4.9.1-20.1
nodejs4-4.9.1-20.1
npm4-4.9.1-20.1
nodejs4-devel-4.9.1-20.1

147574 - SuSE Linux 15.0 openSUSE-SU-2019:0082-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6442, CVE-2019-6443, CVE-2019-6444, CVE-2019-6445

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0082-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00082.html

SuSE Linux 15.0
x86_64
python3-ntp-debuginfo-1.1.3-lp150.2.3.1
ntpsec-debugsource-1.1.3-lp150.2.3.1
ntpsec-1.1.3-lp150.2.3.1
python3-ntp-1.1.3-lp150.2.3.1
ntpsec-debuginfo-1.1.3-lp150.2.3.1
ntpsec-utils-1.1.3-lp150.2.3.1

147579 - SuSE Linux 15.0 openSUSE-SU-2019:0081-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11713, CVE-2018-4162, CVE-2018-4163, CVE-2018-4165, CVE-2018-4191, CVE-2018-4197, CVE-2018-4207, CVE-2018-4208, CVE-2018-4209, CVE-2018-4210, CVE-2018-4212, CVE-2018-4213, CVE-2018-4299, CVE-2018-4306, CVE-2018-4309, CVE-2018-4312, CVE-2018-4314, CVE-2018-4315, CVE-2018-4316, CVE-2018-4317, CVE-2018-4318, CVE-2018-4319, CVE-2018-4323, CVE-2018-4328, CVE-2018-4345, CVE-2018-4358, CVE-2018-4359, CVE-2018-4361, CVE-2018-4372, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4386, CVE-2018-4392, CVE-2018-4416, CVE-2018-4437, CVE-2018-4438, CVE-2018-4441, CVE-2018-4442, CVE-2018-4443, CVE-2018-4464

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0081-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00081.html

SuSE Linux 15.0
i586
webkit-jsc-4-2.22.5-lp150.2.9.1
webkit2gtk-4_0-injected-bundles-2.22.5-lp150.2.9.1
webkit2gtk3-plugin-process-gtk2-2.22.5-lp150.2.9.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.5-lp150.2.9.1
typelib-1_0-JavaScriptCore-4_0-2.22.5-lp150.2.9.1
typelib-1_0-WebKit2WebExtension-4_0-2.22.5-lp150.2.9.1
webkit2gtk3-debugsource-2.22.5-lp150.2.9.1
webkit2gtk3-minibrowser-debuginfo-2.22.5-lp150.2.9.1
libwebkit2gtk-4_0-37-2.22.5-lp150.2.9.1
webkit-jsc-4-debuginfo-2.22.5-lp150.2.9.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.22.5-lp150.2.9.1
webkit2gtk3-minibrowser-2.22.5-lp150.2.9.1
libwebkit2gtk-4_0-37-debuginfo-2.22.5-lp150.2.9.1
libjavascriptcoregtk-4_0-18-2.22.5-lp150.2.9.1
webkit2gtk3-devel-2.22.5-lp150.2.9.1
typelib-1_0-WebKit2-4_0-2.22.5-lp150.2.9.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.5-lp150.2.9.1

noarch
libwebkit2gtk3-lang-2.22.5-lp150.2.9.1

x86_64
webkit-jsc-4-2.22.5-lp150.2.9.1
libwebkit2gtk-4_0-37-32bit-2.22.5-lp150.2.9.1
webkit2gtk-4_0-injected-bundles-2.22.5-lp150.2.9.1
webkit2gtk3-plugin-process-gtk2-2.22.5-lp150.2.9.1
libjavascriptcoregtk-4_0-18-32bit-2.22.5-lp150.2.9.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.5-lp150.2.9.1
typelib-1_0-JavaScriptCore-4_0-2.22.5-lp150.2.9.1
libjavascriptcoregtk-4_0-18-32bit-debuginfo-2.22.5-lp150.2.9.1
typelib-1_0-WebKit2WebExtension-4_0-2.22.5-lp150.2.9.1
webkit2gtk3-debugsource-2.22.5-lp150.2.9.1
webkit2gtk3-minibrowser-debuginfo-2.22.5-lp150.2.9.1
libwebkit2gtk-4_0-37-2.22.5-lp150.2.9.1
webkit-jsc-4-debuginfo-2.22.5-lp150.2.9.1
libwebkit2gtk-4_0-37-32bit-debuginfo-2.22.5-lp150.2.9.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.22.5-lp150.2.9.1
webkit2gtk3-minibrowser-2.22.5-lp150.2.9.1
libwebkit2gtk-4_0-37-debuginfo-2.22.5-lp150.2.9.1
libjavascriptcoregtk-4_0-18-2.22.5-lp150.2.9.1
webkit2gtk3-devel-2.22.5-lp150.2.9.1
typelib-1_0-WebKit2-4_0-2.22.5-lp150.2.9.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.5-lp150.2.9.1

147588 - SuSE Linux 15.0 openSUSE-SU-2019:0086-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17097, CVE-2018-17098

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0086-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00085.html

SuSE Linux 15.0
x86_64
soundtouch-1.8.0-lp150.2.9.1
libSoundTouch0-debuginfo-1.8.0-lp150.2.9.1
soundtouch-debuginfo-1.8.0-lp150.2.9.1
soundtouch-debugsource-1.8.0-lp150.2.9.1
soundtouch-devel-1.8.0-lp150.2.9.1
libSoundTouch0-32bit-1.8.0-lp150.2.9.1
libSoundTouch0-32bit-debuginfo-1.8.0-lp150.2.9.1
libSoundTouch0-1.8.0-lp150.2.9.1

i586
soundtouch-1.8.0-lp150.2.9.1
libSoundTouch0-debuginfo-1.8.0-lp150.2.9.1
soundtouch-debuginfo-1.8.0-lp150.2.9.1
soundtouch-debugsource-1.8.0-lp150.2.9.1
soundtouch-devel-1.8.0-lp150.2.9.1
libSoundTouch0-1.8.0-lp150.2.9.1

147590 - SuSE Linux 15.0 openSUSE-SU-2019:0094-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20337, CVE-2018-20363, CVE-2018-20364, CVE-2018-20365, CVE-2018-5817, CVE-2018-5818, CVE-2018-5819

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0094-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00099.html

SuSE Linux 15.0
x86_64
libraw16-debuginfo-0.18.9-lp150.2.6.1
libraw-debuginfo-0.18.9-lp150.2.6.1
libraw-debugsource-0.18.9-lp150.2.6.1
libraw-tools-debuginfo-0.18.9-lp150.2.6.1
libraw16-0.18.9-lp150.2.6.1
libraw-tools-0.18.9-lp150.2.6.1
libraw-devel-0.18.9-lp150.2.6.1
libraw-devel-static-0.18.9-lp150.2.6.1

i586

libraw16-debuginfo-0.18.9-lp150.2.6.1
libraw-debuginfo-0.18.9-lp150.2.6.1
libraw-debugsource-0.18.9-lp150.2.6.1
libraw-tools-debuginfo-0.18.9-lp150.2.6.1
libraw16-0.18.9-lp150.2.6.1
libraw-tools-0.18.9-lp150.2.6.1
libraw-devel-0.18.9-lp150.2.6.1
libraw-devel-static-0.18.9-lp150.2.6.1

163789 - Oracle Enterprise Linux ELSA-2019-0159 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12405, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498

Description

The scan detected that the host is missing the following update:
ELSA-2019-0159

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-January/008388.html

OEL6
x86_64
thunderbird-60.4.0-1.0.1.el6

163790 - Oracle Enterprise Linux ELSA-2019-0160 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12405, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498

Description

The scan detected that the host is missing the following update:
ELSA-2019-0160

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-January/008385.html

OEL7
x86_64
thunderbird-60.4.0-1.0.1.el7_6

171062 - Amazon Linux AMI ALAS-2018-1126 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1050, CVE-2018-10858, CVE-2018-1139

Description

The scan detected that the host is missing the following update:
ALAS-2018-1126

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1126.html

Amazon Linux AMI
i686
samba-common-libs-4.8.3-4.amzn1
ctdb-4.8.3-4.amzn1
libwbclient-4.8.3-4.amzn1
samba-winbind-krb5-locator-4.8.3-4.amzn1
samba-python-4.8.3-4.amzn1
samba-common-tools-4.8.3-4.amzn1
libsmbclient-4.8.3-4.amzn1
samba-winbind-clients-4.8.3-4.amzn1
samba-krb5-printing-4.8.3-4.amzn1
samba-libs-4.8.3-4.amzn1
ctdb-tests-4.8.3-4.amzn1
samba-debuginfo-4.8.3-4.amzn1
samba-4.8.3-4.amzn1
libsmbclient-devel-4.8.3-4.amzn1
samba-client-4.8.3-4.amzn1
samba-test-4.8.3-4.amzn1
samba-devel-4.8.3-4.amzn1
samba-winbind-4.8.3-4.amzn1
samba-test-libs-4.8.3-4.amzn1
samba-winbind-modules-4.8.3-4.amzn1
samba-client-libs-4.8.3-4.amzn1
libwbclient-devel-4.8.3-4.amzn1
samba-python-test-4.8.3-4.amzn1

noarch
samba-pidl-4.8.3-4.amzn1
samba-common-4.8.3-4.amzn1

x86_64
samba-common-libs-4.8.3-4.amzn1
ctdb-4.8.3-4.amzn1
libwbclient-4.8.3-4.amzn1
samba-winbind-krb5-locator-4.8.3-4.amzn1
samba-common-tools-4.8.3-4.amzn1
samba-python-4.8.3-4.amzn1
samba-client-libs-4.8.3-4.amzn1
libsmbclient-4.8.3-4.amzn1
samba-4.8.3-4.amzn1
samba-winbind-clients-4.8.3-4.amzn1
samba-libs-4.8.3-4.amzn1
ctdb-tests-4.8.3-4.amzn1
samba-debuginfo-4.8.3-4.amzn1
libsmbclient-devel-4.8.3-4.amzn1
samba-test-libs-4.8.3-4.amzn1
samba-client-4.8.3-4.amzn1
samba-test-4.8.3-4.amzn1
samba-devel-4.8.3-4.amzn1

samba-winbind-4.8.3-4.amzn1
samba-krb5-printing-4.8.3-4.amzn1
samba-winbind-modules-4.8.3-4.amzn1
libwbclient-devel-4.8.3-4.amzn1
samba-python-test-4.8.3-4.amzn1

171066 - Amazon Linux AMI ALAS-2018-1129 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ALAS-2018-1129

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1129.html

Amazon Linux AMI
x86_64
krb5-server-1.15.1-34.44.amzn1
krb5-devel-1.15.1-34.44.amzn1
krb5-pkinit-openssl-1.15.1-34.44.amzn1
krb5-debuginfo-1.15.1-34.44.amzn1
krb5-server-ldap-1.15.1-34.44.amzn1
libkadm5-1.15.1-34.44.amzn1
krb5-libs-1.15.1-34.44.amzn1
krb5-workstation-1.15.1-34.44.amzn1

i686
libkadm5-1.15.1-34.44.amzn1
krb5-devel-1.15.1-34.44.amzn1
krb5-pkinit-openssl-1.15.1-34.44.amzn1
krb5-debuginfo-1.15.1-34.44.amzn1
krb5-server-1.15.1-34.44.amzn1
krb5-workstation-1.15.1-34.44.amzn1
krb5-libs-1.15.1-34.44.amzn1
krb5-server-ldap-1.15.1-34.44.amzn1

182897 - FreeBSD powerdns-recursor Multiple Vulnerabilities (40d92cc5-1e2b-11e9-bef6-6805ca2fa271)

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

Risk Level: Medium

CVE: CVE-2019-3806, CVE-2019-3807

Description

The scan detected that the host is missing the following update:
powerdns-recursor -- multiple vulnerabilities (40d92cc5-1e2b-11e9-bef6-6805ca2fa271)

Observation

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

http://www.vuxml.org/freebsd/40d92cc5-1e2b-11e9-bef6-6805ca2fa271.html

Affected packages:
powerdns-recursor < 4.1.9

196235 - Red Hat Enterprise Linux RHSA-2019-0159 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12405, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498

Description

The scan detected that the host is missing the following update:
RHSA-2019-0159

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00025.html

RHEL6S
i386
thunderbird-debuginfo-60.4.0-1.el6
thunderbird-60.4.0-1.el6

x86_64
thunderbird-debuginfo-60.4.0-1.el6
thunderbird-60.4.0-1.el6

RHEL6D
x86_64
thunderbird-debuginfo-60.4.0-1.el6
thunderbird-60.4.0-1.el6

i386
thunderbird-debuginfo-60.4.0-1.el6
thunderbird-60.4.0-1.el6

RHEL6WS
x86_64
thunderbird-debuginfo-60.4.0-1.el6
thunderbird-60.4.0-1.el6

i386
thunderbird-debuginfo-60.4.0-1.el6
thunderbird-60.4.0-1.el6

196237 - Red Hat Enterprise Linux RHSA-2019-0163 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18397, CVE-2018-18559

Description

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

RHSA-2019-0163

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00031.html

RHEL7D
x86_64
kernel-debug-3.10.0-957.5.1.el7
bpftool-3.10.0-957.5.1.el7
kernel-debuginfo-common-x86_64-3.10.0-957.5.1.el7
kernel-devel-3.10.0-957.5.1.el7
kernel-tools-libs-3.10.0-957.5.1.el7
kernel-headers-3.10.0-957.5.1.el7
kernel-tools-debuginfo-3.10.0-957.5.1.el7
perf-debuginfo-3.10.0-957.5.1.el7
kernel-debuginfo-3.10.0-957.5.1.el7
python-perf-3.10.0-957.5.1.el7
kernel-debug-devel-3.10.0-957.5.1.el7
kernel-tools-libs-devel-3.10.0-957.5.1.el7
kernel-debug-debuginfo-3.10.0-957.5.1.el7
perf-3.10.0-957.5.1.el7
kernel-tools-3.10.0-957.5.1.el7
kernel-3.10.0-957.5.1.el7
python-perf-debuginfo-3.10.0-957.5.1.el7

noarch
kernel-doc-3.10.0-957.5.1.el7
kernel-abi-whitelists-3.10.0-957.5.1.el7

RHEL7S
noarch
kernel-doc-3.10.0-957.5.1.el7
kernel-abi-whitelists-3.10.0-957.5.1.el7

x86_64
kernel-debug-3.10.0-957.5.1.el7
bpftool-3.10.0-957.5.1.el7
kernel-debuginfo-common-x86_64-3.10.0-957.5.1.el7
kernel-devel-3.10.0-957.5.1.el7
kernel-tools-libs-3.10.0-957.5.1.el7
kernel-headers-3.10.0-957.5.1.el7
kernel-tools-debuginfo-3.10.0-957.5.1.el7
perf-debuginfo-3.10.0-957.5.1.el7
kernel-debuginfo-3.10.0-957.5.1.el7
python-perf-3.10.0-957.5.1.el7
kernel-debug-devel-3.10.0-957.5.1.el7
kernel-tools-libs-devel-3.10.0-957.5.1.el7
kernel-debug-debuginfo-3.10.0-957.5.1.el7
perf-3.10.0-957.5.1.el7
kernel-tools-3.10.0-957.5.1.el7
kernel-3.10.0-957.5.1.el7
python-perf-debuginfo-3.10.0-957.5.1.el7

RHEL7WS
x86_64
kernel-debug-3.10.0-957.5.1.el7
bpftool-3.10.0-957.5.1.el7

kernel-debuginfo-common-x86_64-3.10.0-957.5.1.el7
kernel-devel-3.10.0-957.5.1.el7
kernel-tools-libs-3.10.0-957.5.1.el7
kernel-headers-3.10.0-957.5.1.el7
kernel-tools-debuginfo-3.10.0-957.5.1.el7
perf-debuginfo-3.10.0-957.5.1.el7
kernel-debuginfo-3.10.0-957.5.1.el7
python-perf-3.10.0-957.5.1.el7
kernel-debug-devel-3.10.0-957.5.1.el7
kernel-tools-libs-devel-3.10.0-957.5.1.el7
kernel-debug-debuginfo-3.10.0-957.5.1.el7
perf-3.10.0-957.5.1.el7
kernel-tools-3.10.0-957.5.1.el7
kernel-3.10.0-957.5.1.el7
python-perf-debuginfo-3.10.0-957.5.1.el7

noarch
kernel-doc-3.10.0-957.5.1.el7
kernel-abi-whitelists-3.10.0-957.5.1.el7

196239 - Red Hat Enterprise Linux RHSA-2019-0160 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12405, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498

Description

The scan detected that the host is missing the following update:
RHSA-2019-0160

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00026.html

RHEL7D
x86_64
thunderbird-debuginfo-60.4.0-1.el7_6
thunderbird-60.4.0-1.el7_6

RHEL7S
x86_64
thunderbird-debuginfo-60.4.0-1.el7_6
thunderbird-60.4.0-1.el7_6

RHEL7WS
x86_64
thunderbird-debuginfo-60.4.0-1.el7_6
thunderbird-60.4.0-1.el7_6

24641 - (JSA10919) Juniper Junos OS OpenSSL Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0732, CVE-2018-0737

Description

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

Observation

Juniper Junos OS is an operating system used in Juniper devices.

Multiple vulnerabilities are present in some versions of Juniper Junos OS. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to cause a denial of service condition.

24649 - Oracle MySQL Enterprise Monitor Critical Patch Update January 2019

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

Risk Level: Medium

CVE: CVE-2018-0732

Description

A vulnerability is present in some versions of Oracle MySQL Enterprise Monitor.

Observation

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

A Vulnerability is present in some versions of Oracle MySQL Enterprise Monitor. The flaw lies in OpenSSL component. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

24651 - (JSA10915) Juniper Junos OS SRX Series Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0015

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw is in token caching, allows deleted dynamic VPN connection to establish dynamic VPN connections until the device is rebooted. Successful exploitation could allow an attacker to bypass security restrictions on the target system.

24652 - Oracle MySQL Server Critical Patch Update January 2019

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

Risk Level: Medium

CVE: CVE-2018-0734, CVE-2019-2420, CVE-2019-2434, CVE-2019-2436, CVE-2019-2455, CVE-2019-2481, CVE-2019-2482, CVE-2019-2486, CVE-2019-2494, CVE-2019-2495, CVE-2019-2502, CVE-2019-2503, CVE-2019-2507, CVE-2019-2510, CVE-2019-2513, CVE-2019-2528, CVE-2019-2529, CVE-2019-2530, CVE-2019-2531, CVE-2019-2532, CVE-2019-2533, CVE-2019-2534, CVE-2019-2535, CVE-2019-2536, CVE-2019-2537, CVE-2019-2539

Description

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

Observation

Oracle MySQL Server is a popular open source database.

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

24656 - (CTX240139) Citrix NetScaler Gateway TLS Padding Oracle Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-6485

Description

A vulnerability is present in some versions of Citrix NetScaler Gateway.

Observation

Citrix NetScaler is a widely used product that helps enterprises to protect, control and improve their services.

A vulnerability is present in some versions of Citrix NetScaler Gateway. The flaw lies in the Citrix Application Delivery Controller that using hardware acceleration. Successful exploitation could allow an attacker to decrypt TLS traffic.

24658 - (JSA10913) Juniper Junos OS RPD Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2019-0013

Description

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

Observation

Juniper Junos is an operating system used in Juniper device.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw lies in junos routing protocol daemon process. Successful exploitation could allow an attacker to cause a denial of service condition on the targeted system.

24661 - Cisco Jabber Client Framework Instant Message Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2018-0483

Description

A cross-site scripting vulnerability is present in some versions of Cisco Jabber.

Observation

Cisco Jabber is Cisco unified communication software solution.

A cross-site scripting vulnerability is present in some versions of Cisco Jabber. The flaw is due to insufficient validation of user-

supplied input of an affected client. Successful exploitation could allow an authenticated attacker to execute arbitrary script code in the context of the targeted client.

24664 - Joomla Stored XSS in mod_banners Vulnerability (20190101)

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

Risk Level: Medium

CVE: CVE-2019-6264

Description

A stored xss vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A stored xss vulnerability is present in some versions of Joomla! CMS. The flaw lies in the mod_banners. Successful exploitation could allow a malicious user to conduct xss attack and steal cookie-based authentication credentials.

24665 - (JSA10909) Juniper Junos OS EX2300 and EX3400 Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0009

Description

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

Observation

Juniper Junos OS is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos OS. The flaw is due to high disk I/O operations in virtual chassis deployment disrupting the communications. Successful exploitation could allow an attacker to cause a denial of service condition in the target system.

24666 - Joomla Stored XSS In Com_Contact Vulnerability (20190102)

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

Risk Level: Medium

CVE: CVE-2019-6261

Description

A stored xss vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A stored xss vulnerability is present in some versions of Joomla! CMS. The flaw is due to the Inadequate escaping in com_contact. Successful exploitation could allow a malicious user to conduct xss attack and steal cookie-based authentication credentials.

147586 - SuSE Linux 15.0 openSUSE-SU-2019:0089-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12116, CVE-2018-12121, CVE-2018-12122, CVE-2018-12123

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0089-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00092.html

SuSE Linux 15.0
i586
nodejs8-debugsource-8.15.0-lp150.2.9.1
nodejs8-debuginfo-8.15.0-lp150.2.9.1
nodejs8-devel-8.15.0-lp150.2.9.1
npm8-8.15.0-lp150.2.9.1
nodejs8-8.15.0-lp150.2.9.1

noarch
nodejs8-docs-8.15.0-lp150.2.9.1

x86_64
nodejs8-debugsource-8.15.0-lp150.2.9.1
nodejs8-debuginfo-8.15.0-lp150.2.9.1
nodejs8-devel-8.15.0-lp150.2.9.1
npm8-8.15.0-lp150.2.9.1
nodejs8-8.15.0-lp150.2.9.1

171065 - Amazon Linux AMI ALAS-2018-1127 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10852

Description

The scan detected that the host is missing the following update:
ALAS-2018-1127

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1127.html

Amazon Linux AMI
i686
python27-sss-1.16.2-13.amzn1
libsss_nss_idmap-1.16.2-13.amzn1
libsss_nss_idmap-devel-1.16.2-13.amzn1
sssd-tools-1.16.2-13.amzn1
sssd-client-1.16.2-13.amzn1
sssd-ldap-1.16.2-13.amzn1
sssd-common-1.16.2-13.amzn1
sssd-proxy-1.16.2-13.amzn1
libsss_idmap-devel-1.16.2-13.amzn1

libsss_certmap-devel-1.16.2-13.amzn1
libsss_simpleifp-1.16.2-13.amzn1
libipa_hbac-devel-1.16.2-13.amzn1
python27-sss-murmur-1.16.2-13.amzn1
sssd-krb5-1.16.2-13.amzn1
python27-libipa_hbac-1.16.2-13.amzn1
libsss_sudo-1.16.2-13.amzn1
sssd-debuginfo-1.16.2-13.amzn1
sssd-libwbclient-1.16.2-13.amzn1
sssd-1.16.2-13.amzn1
sssd-dbus-1.16.2-13.amzn1
sssd-ipa-1.16.2-13.amzn1
libsss_certmap-1.16.2-13.amzn1
sssd-winbind-idmap-1.16.2-13.amzn1
sssd-libwbclient-devel-1.16.2-13.amzn1
libsss_idmap-1.16.2-13.amzn1
sssd-ad-1.16.2-13.amzn1
libsss_simpleifp-devel-1.16.2-13.amzn1
libipa_hbac-1.16.2-13.amzn1
python27-libsss_nss_idmap-1.16.2-13.amzn1
libsss_autofs-1.16.2-13.amzn1
sssd-common-pac-1.16.2-13.amzn1
sssd-krb5-common-1.16.2-13.amzn1

noarch
python27-sssdconfig-1.16.2-13.amzn1

x86_64
python27-sss-1.16.2-13.amzn1
sssd-debuginfo-1.16.2-13.amzn1
libsss_nss_idmap-devel-1.16.2-13.amzn1
python27-libsss_nss_idmap-1.16.2-13.amzn1
sssd-tools-1.16.2-13.amzn1
sssd-client-1.16.2-13.amzn1
sssd-ldap-1.16.2-13.amzn1
sssd-proxy-1.16.2-13.amzn1
libsss_idmap-devel-1.16.2-13.amzn1
libsss_certmap-devel-1.16.2-13.amzn1
libsss_simpleifp-1.16.2-13.amzn1
python27-sss-murmur-1.16.2-13.amzn1
sssd-krb5-1.16.2-13.amzn1
python27-libipa_hbac-1.16.2-13.amzn1
libsss_sudo-1.16.2-13.amzn1
sssd-libwbclient-1.16.2-13.amzn1
sssd-1.16.2-13.amzn1
sssd-dbus-1.16.2-13.amzn1
sssd-ipa-1.16.2-13.amzn1
libsss_certmap-1.16.2-13.amzn1
libsss_simpleifp-devel-1.16.2-13.amzn1
sssd-winbind-idmap-1.16.2-13.amzn1
sssd-libwbclient-devel-1.16.2-13.amzn1
libsss_idmap-1.16.2-13.amzn1
sssd-ad-1.16.2-13.amzn1
sssd-common-1.16.2-13.amzn1
libipa_hbac-1.16.2-13.amzn1
libipa_hbac-devel-1.16.2-13.amzn1
libsss_autofs-1.16.2-13.amzn1
libsss_nss_idmap-1.16.2-13.amzn1
sssd-common-pac-1.16.2-13.amzn1
sssd-krb5-common-1.16.2-13.amzn1

182892 - FreeBSD MySQL Multiple Vulnerabilities (d3d02d3a-2242-11e9-b95c-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2019-2420, CVE-2019-2434, CVE-2019-2436, CVE-2019-2455, CVE-2019-2481, CVE-2019-2482, CVE-2019-2486, CVE-2019-2494, CVE-2019-2495, CVE-2019-2502, CVE-2019-2503, CVE-2019-2507, CVE-2019-2510, CVE-2019-2513, CVE-2019-2528, CVE-2019-2529, CVE-2019-2530, CVE-2019-2531, CVE-2019-2532, CVE-2019-2533, CVE-2019-2534, CVE-2019-2535, CVE-2019-2536, CVE-2019-2537, CVE-2019-2539

Description

The scan detected that the host is missing the following update:
MySQL -- multiple vulnerabilities (d3d02d3a-2242-11e9-b95c-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/d3d02d3a-2242-11e9-b95c-b499baebfeaf.html

Affected packages:
mariadb55-server < 5.5.63
mariadb100-server < 10.0.38
mariadb101-server < 10.1.38
mariadb102-server < 10.2.22
mariadb103-server < 10.3.13
mysql55-server < 5.5.63
mysql56-server < 5.6.43
mysql57-server < 5.7.25
mysql80-server < 8.0.14
percona55-server < 5.5.63
percona56-server < 5.6.43
percona57-server < 5.7.25

186544 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3867-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2420, CVE-2019-2434, CVE-2019-2455, CVE-2019-2481, CVE-2019-2482, CVE-2019-2486, CVE-2019-2503, CVE-2019-2507, CVE-2019-2510, CVE-2019-2528, CVE-2019-2529, CVE-2019-2531, CVE-2019-2532, CVE-2019-2534, CVE-2019-2537

Description

The scan detected that the host is missing the following update:
USN-3867-1

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-January/004740.html

Ubuntu 16.04

mysql-server-5.7_5.7.25-0ubuntu0.16.04.2

Ubuntu 18.10

mysql-server-5.7_5.7.25-0ubuntu0.18.10.2

Ubuntu 18.04

mysql-server-5.7_5.7.25-0ubuntu0.18.04.2

194720 - Fedora Linux 29 FEDORA-2019-ee57bda7ae Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6706

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ee57bda7ae

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

Fedora Core 29

lua-5.3.5-3.fc29

194721 - Fedora Linux 29 FEDORA-2019-866b01407a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16056, CVE-2018-16057, CVE-2018-16058, CVE-2018-19622, CVE-2018-19623, CVE-2018-19624, CVE-2018-19625, CVE-2018-19626, CVE-2018-19627, CVE-2018-19628, CVE-2019-5716, CVE-2019-5717, CVE-2019-5718, CVE-2019-5719

Description

The scan detected that the host is missing the following update:
FEDORA-2019-866b01407a

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/2019/1/?count=200&page=2

Fedora Core 29

wireshark-2.6.6-1.fc29

194725 - Fedora Linux 28 FEDORA-2019-b8ffb3768d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14647, CVE-2019-5010

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b8ffb3768d

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

Fedora Core 28

python37-3.7.2-2.fc28

196236 - Red Hat Enterprise Linux RHSA-2019-0194 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5742

Description

The scan detected that the host is missing the following update:
RHSA-2019-0194

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00032.html

RHEL7D
x86_64
bind-debuginfo-9.9.4-73.el7_6
bind-utils-9.9.4-73.el7_6
bind-pkcs11-9.9.4-73.el7_6
bind-9.9.4-73.el7_6
bind-pkcs11-utils-9.9.4-73.el7_6
bind-libs-lite-9.9.4-73.el7_6
bind-sdb-chroot-9.9.4-73.el7_6
bind-libs-9.9.4-73.el7_6
bind-chroot-9.9.4-73.el7_6
bind-pkcs11-libs-9.9.4-73.el7_6
bind-lite-devel-9.9.4-73.el7_6
bind-sdb-9.9.4-73.el7_6
bind-devel-9.9.4-73.el7_6
bind-pkcs11-devel-9.9.4-73.el7_6

noarch
bind-license-9.9.4-73.el7_6

RHEL7S
noarch
bind-license-9.9.4-73.el7_6

x86_64
bind-debuginfo-9.9.4-73.el7_6
bind-utils-9.9.4-73.el7_6
bind-pkcs11-9.9.4-73.el7_6

bind-9.9.4-73.el7_6
bind-pkcs11-utils-9.9.4-73.el7_6
bind-libs-lite-9.9.4-73.el7_6
bind-sdb-chroot-9.9.4-73.el7_6
bind-libs-9.9.4-73.el7_6
bind-chroot-9.9.4-73.el7_6
bind-pkcs11-libs-9.9.4-73.el7_6
bind-lite-devel-9.9.4-73.el7_6
bind-sdb-9.9.4-73.el7_6
bind-devel-9.9.4-73.el7_6
bind-pkcs11-devel-9.9.4-73.el7_6

RHEL7WS
x86_64
bind-debuginfo-9.9.4-73.el7_6
bind-utils-9.9.4-73.el7_6
bind-pkcs11-9.9.4-73.el7_6
bind-9.9.4-73.el7_6
bind-pkcs11-utils-9.9.4-73.el7_6
bind-libs-lite-9.9.4-73.el7_6
bind-sdb-chroot-9.9.4-73.el7_6
bind-libs-9.9.4-73.el7_6
bind-chroot-9.9.4-73.el7_6
bind-pkcs11-libs-9.9.4-73.el7_6
bind-lite-devel-9.9.4-73.el7_6
bind-sdb-9.9.4-73.el7_6
bind-devel-9.9.4-73.el7_6
bind-pkcs11-devel-9.9.4-73.el7_6

noarch
bind-license-9.9.4-73.el7_6

24637 - Wireshark Multiple Vulnerabilities Prior To 2.4.12

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

Risk Level: Medium

CVE: CVE-2019-5717, CVE-2019-5718, CVE-2019-5719

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

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

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

24654 - Joomla Stored XSS Issue In The Global Configuration Help URL Vulnerability (20190104)

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

Risk Level: Medium

CVE: CVE-2019-6262

Description

A stored xss vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A stored xss vulnerability is present in some versions of Joomla! CMS. The flaw lies in the Global Configuration help url. Successful exploitation could allow a malicious user to bypass security and steal cookie-based authentication credentials.

147584 - SuSE Linux 15.0 openSUSE-SU-2019:0092-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5717, CVE-2019-5718, CVE-2019-5719, CVE-2019-5721

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0092-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00090.html

SuSE Linux 15.0
x86_64
libwsutil8-2.4.12-lp150.2.19.1
libwiretap7-debuginfo-2.4.12-lp150.2.19.1
wireshark-devel-2.4.12-lp150.2.19.1
wireshark-debugsource-2.4.12-lp150.2.19.1
libwscodecs1-debuginfo-2.4.12-lp150.2.19.1
libwiretap7-2.4.12-lp150.2.19.1
libwireshark9-2.4.12-lp150.2.19.1
libwscodecs1-2.4.12-lp150.2.19.1
wireshark-ui-qt-2.4.12-lp150.2.19.1
wireshark-ui-qt-debuginfo-2.4.12-lp150.2.19.1
wireshark-debuginfo-2.4.12-lp150.2.19.1
libwsutil8-debuginfo-2.4.12-lp150.2.19.1
wireshark-2.4.12-lp150.2.19.1
libwireshark9-debuginfo-2.4.12-lp150.2.19.1

i586
libwsutil8-2.4.12-lp150.2.19.1
libwiretap7-debuginfo-2.4.12-lp150.2.19.1
wireshark-devel-2.4.12-lp150.2.19.1
wireshark-debugsource-2.4.12-lp150.2.19.1
libwscodecs1-debuginfo-2.4.12-lp150.2.19.1
libwiretap7-2.4.12-lp150.2.19.1
libwireshark9-2.4.12-lp150.2.19.1
libwscodecs1-2.4.12-lp150.2.19.1
wireshark-ui-qt-2.4.12-lp150.2.19.1
wireshark-ui-qt-debuginfo-2.4.12-lp150.2.19.1
wireshark-debuginfo-2.4.12-lp150.2.19.1
libwsutil8-debuginfo-2.4.12-lp150.2.19.1
wireshark-2.4.12-lp150.2.19.1
libwireshark9-debuginfo-2.4.12-lp150.2.19.1

186547 - Ubuntu Linux 18.04 USN-3872-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14625, CVE-2018-16882, CVE-2018-19407, CVE-2018-19854

Description

The scan detected that the host is missing the following update:
USN-3872-1

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-January/004745.html

Ubuntu 18.04

linux-image-generic-lpae-hwe-18.04_4.18.0.14.64
linux-image-4.18.0-14-generic-lpae_4.18.0-14.15~18.04.1
linux-image-snapdragon-hwe-18.04_4.18.0.14.64
linux-image-4.18.0-14-lowlatency_4.18.0-14.15~18.04.1
linux-image-lowlatency-hwe-18.04_4.18.0.14.64
linux-image-4.18.0-14-snapdragon_4.18.0-14.15~18.04.1
linux-image-4.18.0-14-generic_4.18.0-14.15~18.04.1
linux-image-generic-hwe-18.04_4.18.0.14.64

194723 - Fedora Linux 29 FEDORA-2019-7ff7f5093e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18897, CVE-2018-20481, CVE-2018-20551, CVE-2018-20650

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7ff7f5093e

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/2019/1/?count=200&page=2

Fedora Core 29

poppler-0.67.0-10.fc29

88997 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-022-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-17189, CVE-2018-17199, CVE-2019-0190

Description

The scan detected that the host is missing the following update:
SSA:2019-022-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.478594

Slackware 14.0
x86_64
httpd-2.4.38-x86_64-1

Slackware 14.2
x86_64
httpd-2.4.38-x86_64-1

i586
httpd-2.4.38-i586-1

Slackware 14.1
x86_64
httpd-2.4.38-x86_64-1

131278 - Debian Linux 9.0 DSA-4372-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6116

Description

The scan detected that the host is missing the following update:
DSA-4372-1

Observation

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

http://www.debian.org/security/2019/dsa-4372

Debian 9.0
all
ghostscript_9.26a~dfsg-0+deb9u1

131279 - Debian Linux 9.0 DSA-4373-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-4056, CVE-2018-4058, CVE-2018-4059

Description

The scan detected that the host is missing the following update:
DSA-4373-1

Observation

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

http://www.debian.org/security/2019/dsa-4373

Debian 9.0
all
coturn_4.5.0.5-1+deb9u1

131281 - Debian Linux 9.0 DSA-4375-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3813

Description

The scan detected that the host is missing the following update:
DSA-4375-1

Observation

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

http://www.debian.org/security/2019/dsa-4375

Debian 9.0
all
libspice-server-dev_0.12.8-2.1+deb9u3
libspice-server1_0.12.8-2.1+deb9u3

182894 - FreeBSD Apache Vulnerability (eb888ce5-1f19-11e9-be05-4c72b94353b5)

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

Risk Level: Low

CVE: CVE-2018-17189, CVE-2018-17199, CVE-2019-0190

Description

The scan detected that the host is missing the following update:
Apache -- vulnerability (eb888ce5-1f19-11e9-be05-4c72b94353b5)

Observation

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

http://www.vuxml.org/freebsd/eb888ce5-1f19-11e9-be05-4c72b94353b5.html

Affected packages:
apache24 < 2.4.38

182895 - FreeBSD gitea Multiple Vulnerabilities (7f6146aa-2157-11e9-9ba0-4c72b94353b5)

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:

gitea -- multiple vulnerabilities (7f6146aa-2157-11e9-9ba0-4c72b94353b5)

Observation

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

http://www.vuxml.org/freebsd/7f6146aa-2157-11e9-9ba0-4c72b94353b5.html

Affected packages:
gitea < 1.7.0

182896 - FreeBSD phpMyAdmin File Disclosure And SQL Injection (111aefca-2213-11e9-9c8d-6805ca0b3d42)

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:
phpMyAdmin -- File disclosure and SQL injection (111aefca-2213-11e9-9c8d-6805ca0b3d42)

Observation

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

http://www.vuxml.org/freebsd/111aefca-2213-11e9-9c8d-6805ca0b3d42.html

Affected packages:
phpMyAdmin < 4.8.5
phpMyAdmin-php56 < 4.8.5
phpMyAdmin-php70 < 4.8.5
phpMyAdmin-php71 < 4.8.5
phpMyAdmin-php72 < 4.8.5

182898 - FreeBSD botan2 Side Channel During ECC Key Generation (d8e7e854-17fa-11e9-bef6-6805ca2fa271)

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

Risk Level: Low

CVE: CVE-2018-20187

Description

The scan detected that the host is missing the following update:
botan2 -- Side channel during ECC key generation (d8e7e854-17fa-11e9-bef6-6805ca2fa271)

Observation

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

http://www.vuxml.org/freebsd/d8e7e854-17fa-11e9-bef6-6805ca2fa271.html

Affected packages:
botan2 < 2.9.0

182899 - FreeBSD mozilla Multiple Vulnerabilities (b1f7d52f-fc42-48e8-8403-87d4c9d26229)

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

Risk Level: Low

CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18502, CVE-2018-18503, CVE-2018-18504, CVE-2018-18505, CVE-2018-18506

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (b1f7d52f-fc42-48e8-8403-87d4c9d26229)

Observation

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

http://www.vuxml.org/freebsd/b1f7d52f-fc42-48e8-8403-87d4c9d26229.html

Affected packages:
firefox < 65.0_1,1
waterfox < 56.2.7
seamonkey < 2.49.5
linux-seamonkey < 2.49.5
firefox-esr < 60.5.0_1,1
linux-firefox < 60.5.0,2
libxul < 60.5.0
thunderbird < 60.5.0
linux-thunderbird < 60.5.0

182900 - FreeBSD www/mod_dav_svn Malicious SVN Clients Can Crash Mod_dav_svn. (4af3241d-1f0c-11e9-b4bd-d43d7eed0ce2)

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:
www/mod_dav_svn -- Malicious SVN clients can crash mod_dav_svn. (4af3241d-1f0c-11e9-b4bd-d43d7eed0ce2)

Observation

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

http://www.vuxml.org/freebsd/4af3241d-1f0c-11e9-b4bd-d43d7eed0ce2.html

Affected packages:
1.10.0 <= mod_dav_svn < 1.10.3
mod_dav_svn == 1.11.0

186546 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3870-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3813

Description

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

USN-3870-1

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-January/004743.html

Ubuntu 16.04

libspice-server1_0.12.6-4ubuntu0.4

Ubuntu 18.10

libspice-server1_0.14.0-1ubuntu4.2

Ubuntu 14.04

libspice-server1_0.12.4-0nocelt2ubuntu1.8

Ubuntu 18.04

libspice-server1_0.14.0-1ubuntu2.4

186548 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3866-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6116

Description

The scan detected that the host is missing the following update:
USN-3866-1

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-January/004739.html

Ubuntu 16.04

libgs9_9.26~dfsg+0-0ubuntu0.16.04.4
ghostscript_9.26~dfsg+0-0ubuntu0.16.04.4

Ubuntu 18.10

ghostscript_9.26~dfsg+0-0ubuntu0.18.10.4
libgs9_9.26~dfsg+0-0ubuntu0.18.10.4

Ubuntu 14.04

ghostscript_9.26~dfsg+0-0ubuntu0.14.04.4
libgs9_9.26~dfsg+0-0ubuntu0.14.04.4

Ubuntu 18.04

ghostscript_9.26~dfsg+0-0ubuntu0.18.04.4
libgs9_9.26~dfsg+0-0ubuntu0.18.04.4

194713 - Fedora Linux 28 FEDORA-2019-0398d1b049 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20102, CVE-2018-20103, CVE-2018-20615

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0398d1b049

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/2019/1/?count=200&page=2

Fedora Core 28

haproxy-1.8.17-1.fc28

194714 - Fedora Linux 29 FEDORA-2019-9790f1867a 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-2019-9790f1867a

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

Fedora Core 29

radvd-2.17-17.fc29

194715 - Fedora Linux 29 FEDORA-2019-b4356521ba 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-b4356521ba

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/2019/1/?count=200&page=2

Fedora Core 29

runc-1.0.0-67.dev.git12f6a99.fc29

194716 - Fedora Linux 29 FEDORA-2019-c7da53319c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20102, CVE-2018-20103, CVE-2018-20615

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c7da53319c

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/2019/1/?count=200&page=2

Fedora Core 29

haproxy-1.8.17-1.fc29

194717 - Fedora Linux 29 FEDORA-2019-00870e8bfc Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-5010

Description

The scan detected that the host is missing the following update:
FEDORA-2019-00870e8bfc

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/2019/1/?count=200&page=2

Fedora Core 29

anaconda-29.24.7-2.fc29
python3-3.7.2-4.fc29

194718 - Fedora Linux 28 FEDORA-2019-93b4b78e58 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-2019-93b4b78e58

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/2019/1/?count=200&page=2

Fedora Core 28

runc-1.0.0-67.dev.git12f6a99.fc28

194722 - Fedora Linux 28 FEDORA-2019-596813cc59 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-2019-596813cc59

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/2019/1/?count=200&page=2

Fedora Core 28

electrum-3.2.4-2.fc28

196238 - Red Hat Enterprise Linux RHSA-2019-0201 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-16864, CVE-2019-3815

Description

The scan detected that the host is missing the following update:
RHSA-2019-0201

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00029.html

RHEL7D
x86_64
libgudev1-219-62.el7_6.3
systemd-journal-gateway-219-62.el7_6.3

systemd-resolved-219-62.el7_6.3
systemd-devel-219-62.el7_6.3
systemd-sysv-219-62.el7_6.3
libgudev1-devel-219-62.el7_6.3
systemd-219-62.el7_6.3
systemd-libs-219-62.el7_6.3
systemd-debuginfo-219-62.el7_6.3
systemd-python-219-62.el7_6.3
systemd-networkd-219-62.el7_6.3

RHEL7S
x86_64
libgudev1-219-62.el7_6.3
systemd-journal-gateway-219-62.el7_6.3
systemd-python-219-62.el7_6.3
systemd-sysv-219-62.el7_6.3
systemd-devel-219-62.el7_6.3
libgudev1-devel-219-62.el7_6.3
systemd-219-62.el7_6.3
systemd-debuginfo-219-62.el7_6.3
systemd-libs-219-62.el7_6.3
systemd-resolved-219-62.el7_6.3
systemd-networkd-219-62.el7_6.3

RHEL7WS
x86_64
libgudev1-219-62.el7_6.3
systemd-journal-gateway-219-62.el7_6.3
systemd-python-219-62.el7_6.3
systemd-sysv-219-62.el7_6.3
systemd-devel-219-62.el7_6.3
libgudev1-devel-219-62.el7_6.3
systemd-219-62.el7_6.3
systemd-debuginfo-219-62.el7_6.3
systemd-libs-219-62.el7_6.3
systemd-resolved-219-62.el7_6.3
systemd-networkd-219-62.el7_6.3

147575 - SuSE Linux 42.3 openSUSE-SU-2019:0093-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0093-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00094.html

SuSE Linux 42.3
x86_64
openssh-7.2p2-29.1
openssh-askpass-gnome-debuginfo-7.2p2-29.1

openssh-cavs-7.2p2-29.1
openssh-debuginfo-7.2p2-29.1
openssh-helpers-debuginfo-7.2p2-29.1
openssh-debugsource-7.2p2-29.1
openssh-helpers-7.2p2-29.1
openssh-fips-7.2p2-29.1
openssh-cavs-debuginfo-7.2p2-29.1
openssh-askpass-gnome-7.2p2-29.1

i586
openssh-7.2p2-29.1
openssh-askpass-gnome-debuginfo-7.2p2-29.1
openssh-cavs-7.2p2-29.1
openssh-debuginfo-7.2p2-29.1
openssh-helpers-debuginfo-7.2p2-29.1
openssh-debugsource-7.2p2-29.1
openssh-helpers-7.2p2-29.1
openssh-fips-7.2p2-29.1
openssh-cavs-debuginfo-7.2p2-29.1
openssh-askpass-gnome-7.2p2-29.1

147589 - SuSE Linux 15.0 openSUSE-SU-2019:0091-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0091-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00089.html

SuSE Linux 15.0
x86_64
openssh-askpass-gnome-debuginfo-7.6p1-lp150.8.9.1
openssh-debuginfo-7.6p1-lp150.8.9.1
openssh-cavs-7.6p1-lp150.8.9.1
openssh-helpers-7.6p1-lp150.8.9.1
openssh-fips-7.6p1-lp150.8.9.1
openssh-askpass-gnome-7.6p1-lp150.8.9.1
openssh-7.6p1-lp150.8.9.1
openssh-cavs-debuginfo-7.6p1-lp150.8.9.1
openssh-helpers-debuginfo-7.6p1-lp150.8.9.1
openssh-debugsource-7.6p1-lp150.8.9.1

i586
openssh-debuginfo-7.6p1-lp150.8.9.1
openssh-cavs-7.6p1-lp150.8.9.1
openssh-helpers-7.6p1-lp150.8.9.1
openssh-fips-7.6p1-lp150.8.9.1
openssh-7.6p1-lp150.8.9.1
openssh-cavs-debuginfo-7.6p1-lp150.8.9.1
openssh-helpers-debuginfo-7.6p1-lp150.8.9.1

openssh-debugsource-7.6p1-lp150.8.9.1

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.

24510 - (APSB18-42) Vulnerability In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2018-15982, CVE-2018-15983

Update Details

Risk is updated

24511 - (APSB18-42) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-15982, CVE-2018-15983

Update Details

Risk is updated

182864 - FreeBSD Flash Player Multiple Vulnerabilities (49cbe200-f92a-11e8-a89d-d43d7ef03aa6)

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

Risk Level: High

CVE: CVE-2018-15982, CVE-2018-15983

Update Details

Risk is updated

196215 - Red Hat Enterprise Linux RHSA-2018-3795 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15982

Update Details

Risk is updated

131270 - Debian Linux 9.0 DSA-4368-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6250

Update Details

Risk is updated

147551 - SuSE Linux 42.3 openSUSE-SU-2019:0064-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2019-6250

Update Details
Risk is updated

131235 - Debian Linux 9.0 DSA-4328-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-14665

Update Details
Risk is updated

131249 - Debian Linux 9.0 DSA-4343-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-4013

Update Details
Risk is updated

182825 - FreeBSD liveMedia Potential Remote Code Execution (fa194483-dabd-11e8-bf39-5404a68ad561)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-4013

Update Details
Risk is updated

186448 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3802-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-14665

Update Details
Risk is updated

192844 - Fedora Linux 26 FEDORA-2017-94a173c491 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1002157

Update Details

Risk is updated

192854 - Fedora Linux 25 FEDORA-2017-8258f76154 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1002157

Update Details

Risk is updated

192879 - Fedora Linux 27 FEDORA-2017-cc316727f5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1002157

Update Details

Risk is updated

194378 - Fedora Linux 29 FEDORA-2018-a24754252a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18883

Update Details

Risk is updated

194389 - Fedora Linux 29 FEDORA-2018-4ab08fedd6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14665

Update Details

Risk is updated

194430 - Fedora Linux 28 FEDORA-2018-839720583a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14665

Update Details

Risk is updated

194450 - Fedora Linux 29 FEDORA-2018-8e457298ce Update Is Not Installed

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

Risk Level: High
CVE: CVE-2018-18883

Update Details
Risk is updated

194495 - Fedora Linux 29 FEDORA-2018-2fde555d91 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-18883

Update Details
Risk is updated

88835 - Slackware Linux 14.2 SSA:2016-363-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2123, CVE-2016-2125

Update Details
Risk is updated

131240 - Debian Linux 9.0 DSA-4333-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18820

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-6056

Update Details
Risk is updated

145111 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:3271-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2123, CVE-2016-2125

Update Details
Risk is updated

145112 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3272-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2123, CVE-2016-2125

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-6056

Update Details
Risk is updated

147262 - SuSE Linux 15.0 openSUSE-SU-2018:3537-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-17095

Update Details
Risk is updated

147310 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:3588-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-17095

Update Details
Risk is updated

147332 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:3754-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18820

Update Details
Risk is updated

147339 - SuSE Linux 42.3 openSUSE-SU-2018:3694-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-17095

Update Details

Risk is updated

147344 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:3819-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-4022

Update Details

Risk is updated

147430 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2018:3588-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17095

Update Details

Risk is updated

182235 - FreeBSD samba Multiple Vulnerabilities (e4bc323f-cc73-11e6-b704-000c292e4fd8)

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

Risk Level: Medium

CVE: CVE-2016-2123, CVE-2016-2125

Update Details

Risk is updated

182624 - FreeBSD chromium Vulnerability (abfc932e-1ba8-11e8-a944-54ee754af08e)

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

Risk Level: Medium

CVE: CVE-2018-6056

Update Details

Risk is updated

185525 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3158-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2123, CVE-2016-2125

Update Details

Risk is updated

194195 - Fedora Linux 29 FEDORA-2018-be6e73f746 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2018-16515

Update Details
Risk is updated

194401 - Fedora Linux 28 FEDORA-2018-d4349a7ba3 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18820

Update Details
Risk is updated

194407 - Fedora Linux 29 FEDORA-2018-b881073c43 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18820

Update Details
Risk is updated

194410 - Fedora Linux 27 FEDORA-2018-f3d995c6a8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18820

Update Details
Risk is updated

194425 - Fedora Linux 28 FEDORA-2018-317ecbb54f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-4022

Update Details
Risk is updated

194435 - Fedora Linux 29 FEDORA-2018-44ea020814 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-4022

Update Details
Risk is updated

194437 - Fedora Linux 27 FEDORA-2018-8587111c5a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-4022

Update Details
Risk is updated

131233 - Debian Linux 9.0 DSA-4329-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18541

Update Details
Risk is updated

147455 - SuSE Linux 42.3 openSUSE-SU-2018:4148-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-17204, CVE-2018-17205, CVE-2018-17206

Update Details
Risk is updated

147457 - SuSE SLES 12 SP3 SUSE-SU-2018:4128-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-17204, CVE-2018-17205, CVE-2018-17206

Update Details
Risk is updated

194379 - Fedora Linux 29 FEDORA-2018-5702dc9bdf Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18541

Update Details
Risk is updated

194384 - Fedora Linux 28 FEDORA-2018-63465e1846 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18541

Update Details

Risk is updated

194385 - Fedora Linux 27 FEDORA-2018-b24201fc50 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18541

Update Details

Risk is updated

147373 - SuSE Linux 15.0 openSUSE-SU-2018:3890-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-0734, CVE-2018-0735

Update Details

Risk is updated

182829 - FreeBSD OpenSSL Multiple Vulnerabilities In 1.1 Branch (238ae7de-dba2-11e8-b713-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2018-0734, CVE-2018-0735

Update Details

Risk is updated

182887 - FreeBSD www/py-requests Information Disclosure Vulnerability (50ad9a9a-1e28-11e9-98d7-0050562a4d7b)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

147549 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0132-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111

Update Details

Risk is updated

147555 - SuSE SLES 11 SP4 SUSE-SU-2019:13931-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111

Update Details

Risk is updated

194679 - Fedora Linux 28 FEDORA-2019-9eb0ae6296 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20685

Update Details

Risk is updated

194696 - Fedora Linux 29 FEDORA-2019-f6ff819834 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20685

Update Details

Risk is updated

14411 - PHP Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14412 - Fedora Obsolete Version Detection

Category: SSH Module -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14413 - VMware ESX Obsolete Version Detection

Category: SSH Module -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14460 - Adobe Reader Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14519 - Cisco IOS Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14541 - HP Systems Insight Manager Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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