2019-FEB-28
FSL version 7.6.98

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

24778 - AVEVA InTouch Edge HMI Multiple Vulnerabilities (LFSEC00000133)

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

Risk Level: High

CVE: CVE-2019-6543, CVE-2019-6545

Description

Multiple vulnerabilities are present in some versions of AVEVA InTouch Edge HMI.

Observation

AVEVA InTouch EDge HMI is a tool to build SCADA, HMI applications.

Multiple vulnerabilities are present in some versions of AVEVA InTouch Edge HMI. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

24785 - AVEVA InduSoft Web Studio Multiple Vulnerabilities (ICSA-19-036-01)

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

Risk Level: High

CVE: CVE-2019-6543, CVE-2019-6545

Description

Multiple vulnerabilities are present in some versions of Aveva InduSoft Web Studio.

Observation

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

Multiple vulnerabilities are present in some versions of Aveva InduSoft Web Studio. The flaws lie in multiple components. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

24788 - (APSB19-10) Vulnerabilities In ColdFusion

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

Risk Level: High

CVE: CVE-2019-7091, CVE-2019-7092

Description

Multiple vulnerabilities are present in some versions of Adobe ColdFusion.

Observation

Adobe ColdFusion is a web application development platform.

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

The update provided by Adobe bulletin APSB19-10 resolves these issues. The target system appears to be missing this update.

194810 - Fedora Linux 28 FEDORA-2019-16de0047d4 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-16de0047d4

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

Fedora Core 28

kernel-tools-4.20.11-100.fc28
kernel-headers-4.20.11-100.fc28
kernel-4.20.11-100.fc28

194826 - Fedora Linux 29 FEDORA-2019-8434288a24 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15686, CVE-2018-15687, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2018-16866, CVE-2019-6454

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8434288a24

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

Fedora Core 29

systemd-239-12.git8bca462.fc29

194805 - Fedora Linux 28 FEDORA-2019-963ea958f9 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-963ea958f9

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/2019/2/?count=200&page=3

Fedora Core 28

runc-1.0.0-68.dev.git6635b4f.fc28

194811 - Fedora Linux 29 FEDORA-2019-4dc1e39b34 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20699, CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-4dc1e39b34

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

Fedora Core 29

docker-latest-1.13.1-42.git1185cfd.fc29

194817 - Fedora Linux 28 FEDORA-2019-f455ef79b8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10892, CVE-2018-20699, CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f455ef79b8

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/2019/2/?count=200&page=3

Fedora Core 28

docker-1.13.1-65.git1185cfd.fc28

194819 - Fedora Linux 29 FEDORA-2019-1fccede810 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10897

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1fccede810

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

Fedora Core 29

createrepo_c-0.12.1-1.fc29
dnf-plugins-extras-4.0.2-1.fc29
dnf-plugins-core-4.0.4-1.fc29
librepo-1.9.4-1.fc29
libdnf-0.26.0-1.fc29
dnf-4.1.0-1.fc29
libcomps-0.1.10-2.fc29

24786 - Advantech WebAccess Multiple Vulnerabilities (ICSA-19-024-01)

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

Risk Level: High

CVE: CVE-2019-6519, CVE-2019-6521, CVE-2019-6523

Description

Multiple vulnerabilities are present in some versions of Advantech WebAccess.

Observation

Advantech WebAccess is a web-based HMI software application used in energy, manufacturing, and building automation systems.

Multiple vulnerabilities are present in some versions of Advantech WebAccess. The flaws lie in multiple components. Successful exploitation could allow a remote attacker to bypass security or to obtain and manipulate sensitive information.

24793 - (JSA10900) Juniper Junos OS MX Series Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-0001

Description

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

Observation

Juniper Junos is an operating system used in the Juniper device.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw lies in Broadband Edge subscriber management daemon. Successful exploitation could allow an attacker to cause a denial of service condition on the targeted system.

24794 - (JSA10898) Juniper Junos OS NTP Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-7704, CVE-2016-1549, CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185

Description

Multiple vulnerabilities are present in some versions of Juniper Junos.

Observation

Juniper Junos is the operating system used in Juniper device.

Multiple vulnerabilities are present in some versions of Juniper Junos. The flaws lie in the NTP service. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

147665 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0450-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0450-1

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-February/005142.html

SuSE SLED 12 SP3
x86_64
procps-3.3.9-11.18.1
libprocps3-debuginfo-3.3.9-11.18.1
libprocps3-3.3.9-11.18.1
procps-debuginfo-3.3.9-11.18.1
procps-debugsource-3.3.9-11.18.1

SuSE SLED 12 SP4
x86_64
procps-3.3.9-11.18.1
libprocps3-debuginfo-3.3.9-11.18.1

libprocps3-3.3.9-11.18.1
procps-debuginfo-3.3.9-11.18.1
procps-debugsource-3.3.9-11.18.1

SuSE SLES 12 SP4
x86_64
procps-3.3.9-11.18.1
libprocps3-debuginfo-3.3.9-11.18.1
libprocps3-3.3.9-11.18.1
procps-debuginfo-3.3.9-11.18.1
procps-debugsource-3.3.9-11.18.1

SuSE SLES 12 SP3
x86_64
procps-3.3.9-11.18.1
libprocps3-debuginfo-3.3.9-11.18.1
libprocps3-3.3.9-11.18.1
procps-debuginfo-3.3.9-11.18.1
procps-debugsource-3.3.9-11.18.1

147669 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0242-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-7443

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0242-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00133.html
https://lists.opensuse.org/opensuse-updates/2019-02/msg00137.html

SuSE Linux 15.0
i586
libKF5Auth5-5.45.0-lp150.3.3.1
kauth-debugsource-5.45.0-lp150.3.3.1
kauth-devel-5.45.0-lp150.3.3.1
libKF5Auth5-debuginfo-5.45.0-lp150.3.3.1

noarch
libKF5Auth5-lang-5.45.0-lp150.3.3.1

x86_64
libKF5Auth5-5.20.0-10.1
kauth-devel-32bit-5.45.0-lp150.3.3.1
libKF5Auth5-64bit-5.32.0-5.2
libpolkit-qt5-1-devel-64bit-0.112.0-4.1
kcoreaddons-devel-debuginfo-64bit-5.32.0-7.1
kcoreaddons-devel-5.20.0-8.1
kcoreaddons-5.20.0-8.1
libKF5CoreAddons5-debuginfo-64bit-5.32.0-7.1
libKF5CoreAddons5-debuginfo-5.20.0-8.1
libKF5CoreAddons5-64bit-5.32.0-7.1

libKF5Auth5-debuginfo-64bit-5.32.0-5.2
libpolkit-qt5-1-1-debuginfo-0.112.0-2.1
kauth-debugsource-5.26.0-9.2
libpolkit-qt5-1-devel-0.112.0-2.1
libKF5Auth5-32bit-debuginfo-5.45.0-lp150.3.3.1
kauth-devel-64bit-5.32.0-5.2
libpolkit-qt5-1-1-0.112.0-2.1
libKF5Auth5-64bit-debuginfo-5.45.0-bp150.3.3.1
libKF5Auth5-debuginfo-5.26.0-9.2
libKF5Auth5-32bit-5.45.0-lp150.3.3.1
kcoreaddons-debugsource-5.20.0-8.1
kcoreaddons-devel-64bit-5.32.0-7.1
kcoreaddons-lang-5.20.0-8.1
libKF5Auth5-lang-5.20.0-10.1
kcoreaddons-devel-debuginfo-5.20.0-8.1
polkit-qt5-1-debugsource-0.112.0-2.1
libKF5CoreAddons5-5.20.0-8.1
libpolkit-qt5-1-1-64bit-0.112.0-4.1
libpolkit-qt5-1-1-debuginfo-64bit-0.112.0-4.1
kauth-devel-5.20.0-10.1

SuSE Linux 42.3
i586
libKF5Auth5-5.32.0-3.3.1
kauth-devel-5.32.0-3.3.1
kauth-debugsource-5.32.0-3.3.1
libKF5Auth5-debuginfo-5.32.0-3.3.1

noarch
libKF5Auth5-lang-5.32.0-3.3.1

x86_64
libKF5Auth5-5.32.0-3.3.1
kauth-debugsource-5.32.0-3.3.1
libKF5Auth5-32bit-5.32.0-3.3.1
kauth-devel-32bit-5.32.0-3.3.1
kauth-devel-5.32.0-3.3.1
libKF5Auth5-debuginfo-5.32.0-3.3.1
libKF5Auth5-debuginfo-32bit-5.32.0-3.3.1

147672 - SuSE Linux 15.0 openSUSE-SU-2019:0243-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3814

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0243-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00135.html

SuSE Linux 15.0
x86_64

dovecot23-fts-solr-debuginfo-2.3.3-lp150.3.3.1
dovecot23-fts-debuginfo-2.3.3-lp150.3.3.1
dovecot23-fts-squat-debuginfo-2.3.3-lp150.3.3.1
dovecot23-debuginfo-2.3.3-lp150.3.3.1
dovecot23-fts-squat-2.3.3-lp150.3.3.1
dovecot23-backend-pgsql-2.3.3-lp150.3.3.1
dovecot23-devel-2.3.3-lp150.3.3.1
dovecot23-backend-sqlite-2.3.3-lp150.3.3.1
dovecot23-2.3.3-lp150.3.3.1
dovecot23-fts-solr-2.3.3-lp150.3.3.1
dovecot23-backend-pgsql-debuginfo-2.3.3-lp150.3.3.1
dovecot23-fts-2.3.3-lp150.3.3.1
dovecot23-debugsource-2.3.3-lp150.3.3.1
dovecot23-fts-lucene-debuginfo-2.3.3-lp150.3.3.1
dovecot23-backend-mysql-debuginfo-2.3.3-lp150.3.3.1
dovecot23-backend-mysql-2.3.3-lp150.3.3.1
dovecot23-backend-sqlite-debuginfo-2.3.3-lp150.3.3.1
dovecot23-fts-lucene-2.3.3-lp150.3.3.1

147674 - SuSE Linux 15.0 openSUSE-SU-2019:0245-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6446

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0245-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00134.html

SuSE Linux 15.0
x86_64
python-numpy_1_14_0-gnu-hpc-debugsource-1.14.0-lp150.3.3.1
python3-numpy-debuginfo-1.14.0-lp150.3.3.1
python2-numpy_1_14_0-gnu-hpc-debuginfo-1.14.0-lp150.3.3.1
python2-numpy-gnu-hpc-devel-1.14.0-lp150.3.3.1
python-numpy_1_14_0-gnu-hpc-debuginfo-1.14.0-lp150.3.3.1
python-numpy-debugsource-1.14.0-lp150.3.3.1
python2-numpy-1.14.0-lp150.3.3.1
python2-numpy-gnu-hpc-1.14.0-lp150.3.3.1
python3-numpy-gnu-hpc-devel-1.14.0-lp150.3.3.1
python3-numpy_1_14_0-gnu-hpc-1.14.0-lp150.3.3.1
python2-numpy_1_14_0-gnu-hpc-devel-1.14.0-lp150.3.3.1
python3-numpy_1_14_0-gnu-hpc-devel-1.14.0-lp150.3.3.1
python2-numpy_1_14_0-gnu-hpc-1.14.0-lp150.3.3.1
python3-numpy-devel-1.14.0-lp150.3.3.1
python2-numpy-devel-1.14.0-lp150.3.3.1
python3-numpy-1.14.0-lp150.3.3.1
python3-numpy_1_14_0-gnu-hpc-debuginfo-1.14.0-lp150.3.3.1
python-numpy-debuginfo-1.14.0-lp150.3.3.1
python3-numpy-gnu-hpc-1.14.0-lp150.3.3.1
python2-numpy-debuginfo-1.14.0-lp150.3.3.1

160523 - CentOS 7 CESA-2019-0368 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6454

Description

The scan detected that the host is missing the following update:
CESA-2019-0368

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023202.html

CentOS 7
x86_64
libgudev1-devel-219-62.el7_6.5
systemd-sysv-219-62.el7_6.5
systemd-journal-gateway-219-62.el7_6.5
systemd-networkd-219-62.el7_6.5
systemd-devel-219-62.el7_6.5
libgudev1-219-62.el7_6.5
systemd-219-62.el7_6.5
systemd-python-219-62.el7_6.5
systemd-libs-219-62.el7_6.5
systemd-resolved-219-62.el7_6.5

i686
systemd-devel-219-62.el7_6.5
libgudev1-devel-219-62.el7_6.5
libgudev1-219-62.el7_6.5
systemd-resolved-219-62.el7_6.5
systemd-libs-219-62.el7_6.5

182917 - FreeBSD Rdesktop - Critical - Remote Code Execution (3e2c9b63-223c-4575-af5c-816acb14e445)

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

Risk Level: High

CVE: CVE-2018-20174, CVE-2018-20175, CVE-2018-20176, CVE-2018-20177, CVE-2018-20178, CVE-2018-20179, CVE-2018-20180, CVE-2018-20181, CVE-2018-20182, CVE-2018-8791, CVE-2018-8792, CVE-2018-8793, CVE-2018-8794, CVE-2018-8795, CVE-2018-8796, CVE-2018-8797, CVE-2018-8798, CVE-2018-8799, CVE-2018-8800

Description

The scan detected that the host is missing the following update:
rdesktop - critical - Remote Code Execution (3e2c9b63-223c-4575-af5c-816acb14e445)

Observation

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

http://www.vuxml.org/freebsd/3e2c9b63-223c-4575-af5c-816acb14e445.html

Affected packages:
rdesktop < 1.8.4

194803 - Fedora Linux 28 FEDORA-2019-6cf96757fe Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6cf96757fe

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/2019/2/?count=200&page=3

Fedora Core 28

golang-1.10.8-1.fc28

194813 - Fedora Linux 28 FEDORA-2019-3d38ab031e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16741, CVE-2018-16744, CVE-2018-16745

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3d38ab031e

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

Fedora Core 28

mgetty-1.1.37-10.fc28

194815 - Fedora Linux 29 FEDORA-2019-7bdeed7fc5 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7bdeed7fc5

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

Fedora Core 29

kernel-tools-4.20.11-200.fc29
kernel-headers-4.20.11-200.fc29
kernel-4.20.11-200.fc29

194820 - Fedora Linux 29 FEDORA-2019-da586db907 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16741, CVE-2018-16744, CVE-2018-16745

Description

The scan detected that the host is missing the following update:
FEDORA-2019-da586db907

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

Fedora Core 29

mgetty-1.1.37-11.fc29

89006 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-054-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-8906, CVE-2019-8907

Description

The scan detected that the host is missing the following update:
SSA:2019-054-01

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.415561

Slackware 14.0
x86_64
file-5.36-x86_64-1

Slackware 14.2
x86_64
file-5.36-x86_64-1

i586
file-5.36-i586-1

Slackware 14.1
x86_64
file-5.36-x86_64-1

147661 - SuSE Linux 42.3 openSUSE-SU-2019:0234-1 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-2019:0234-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00123.html

SuSE Linux 42.3
i586
npm6-6.16.0-18.1
nodejs6-6.16.0-18.1
nodejs6-devel-6.16.0-18.1
nodejs6-debugsource-6.16.0-18.1
nodejs6-debuginfo-6.16.0-18.1

noarch
nodejs6-docs-6.16.0-18.1

x86_64
npm6-6.16.0-18.1
nodejs6-6.16.0-18.1
nodejs6-devel-6.16.0-18.1
nodejs6-debugsource-6.16.0-18.1
nodejs6-debuginfo-6.16.0-18.1

147663 - SuSE SLED 15 SUSE-SU-2019:0469-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18335, CVE-2018-18356, CVE-2018-18509, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0469-1

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-February/005148.html

SuSE SLED 15
x86_64
MozillaThunderbird-60.5.1-3.24.1
MozillaThunderbird-debugsource-60.5.1-3.24.1
MozillaThunderbird-debuginfo-60.5.1-3.24.1
MozillaThunderbird-translations-common-60.5.1-3.24.1
MozillaThunderbird-translations-other-60.5.1-3.24.1

147666 - SuSE Linux 15.0 openSUSE-SU-2019:0248-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0248-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00141.html

SuSE Linux 15.0
x86_64
MozillaFirefox-branding-upstream-60.5.1-lp150.3.39.2
MozillaFirefox-buildsymbols-60.5.1-lp150.3.39.2
MozillaFirefox-devel-60.5.1-lp150.3.39.2
MozillaFirefox-translations-common-60.5.1-lp150.3.39.2
MozillaFirefox-debuginfo-60.5.1-lp150.3.39.2
MozillaFirefox-translations-other-60.5.1-lp150.3.39.2
MozillaFirefox-debugsource-60.5.1-lp150.3.39.2
MozillaFirefox-60.5.1-lp150.3.39.2

147675 - SuSE Linux 42.3 openSUSE-SU-2019:0250-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18335, CVE-2018-18356, CVE-2018-18509, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0250-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00140.html

SuSE Linux 42.3
x86_64
MozillaThunderbird-60.5.1-86.1
MozillaThunderbird-translations-common-60.5.1-86.1
MozillaThunderbird-translations-other-60.5.1-86.1

MozillaThunderbird-buildsymbols-60.5.1-86.1
MozillaThunderbird-debuginfo-60.5.1-86.1
MozillaThunderbird-debugsource-60.5.1-86.1

160519 - CentOS 6 CESA-2019-0373 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
CESA-2019-0373

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023194.html

CentOS 6
x86_64
firefox-60.5.1-1.el6.centos

i686
firefox-60.5.1-1.el6.centos

160520 - CentOS 7 CESA-2019-0374 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18356, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
CESA-2019-0374

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023195.html

CentOS 7
x86_64
firefox-60.5.1-1.el7.centos

i686
firefox-60.5.1-1.el7.centos

182919 - FreeBSD drupal Drupal Core - Highly Critical - Remote Code Execution (002b4b05-35dd-11e9-94a8-000ffec0b3e1)

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

Risk Level: Medium

CVE: CVE-2019-6340

Description

The scan detected that the host is missing the following update:
drupal -- Drupal core - Highly critical - Remote Code Execution (002b4b05-35dd-11e9-94a8-000ffec0b3e1)

Observation

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

http://www.vuxml.org/freebsd/002b4b05-35dd-11e9-94a8-000ffec0b3e1.html

Affected packages:
drupal8 < 8.6.10

194807 - Fedora Linux 29 FEDORA-2019-387e017332 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20662, CVE-2019-7310

Description

The scan detected that the host is missing the following update:
FEDORA-2019-387e017332

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

Fedora Core 29

poppler-0.67.0-12.fc29

194824 - Fedora Linux 29 FEDORA-2019-7a554204c1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7a554204c1

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

Fedora Core 29

SDL-1.2.15-36.fc29

24638 - (JSA10892) Juniper Junos OS Authd Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0057

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 IP address assignment for DHCP subscriber logging in with option 50. Successful exploitation could allow an attacker to retrieve sensitive information from the target system or cause denial of service condition.

147662 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0499-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14662, CVE-2018-16846, CVE-2018-16889

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0499-1

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-February/005154.html

SuSE SLED 12 SP3
x86_64
librados2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rgw-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-common-12.2.10+git.1549630712.bb089269ea-2.27.2
librados2-12.2.10+git.1549630712.bb089269ea-2.27.2
libradosstriper1-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
libradosstriper1-12.2.10+git.1549630712.bb089269ea-2.27.2
librgw2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rbd-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-common-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
libcephfs2-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rados-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-cephfs-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
librbd1-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-debugsource-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rgw-12.2.10+git.1549630712.bb089269ea-2.27.2
librbd1-12.2.10+git.1549630712.bb089269ea-2.27.2
python-cephfs-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rbd-12.2.10+git.1549630712.bb089269ea-2.27.2
librgw2-12.2.10+git.1549630712.bb089269ea-2.27.2
libcephfs2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rados-12.2.10+git.1549630712.bb089269ea-2.27.2

SuSE SLED 12 SP4
x86_64
librados2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rgw-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-common-12.2.10+git.1549630712.bb089269ea-2.27.2
librados2-12.2.10+git.1549630712.bb089269ea-2.27.2
libradosstriper1-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
libradosstriper1-12.2.10+git.1549630712.bb089269ea-2.27.2
librgw2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rbd-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-common-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
libcephfs2-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rados-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-cephfs-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
librbd1-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-debugsource-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rgw-12.2.10+git.1549630712.bb089269ea-2.27.2
librbd1-12.2.10+git.1549630712.bb089269ea-2.27.2
python-cephfs-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rbd-12.2.10+git.1549630712.bb089269ea-2.27.2
librgw2-12.2.10+git.1549630712.bb089269ea-2.27.2
libcephfs2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rados-12.2.10+git.1549630712.bb089269ea-2.27.2

SuSE SLES 12 SP4
x86_64
librados2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rgw-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-common-12.2.10+git.1549630712.bb089269ea-2.27.2
librados2-12.2.10+git.1549630712.bb089269ea-2.27.2
libradosstriper1-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
libradosstriper1-12.2.10+git.1549630712.bb089269ea-2.27.2
librgw2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rbd-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-common-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
libcephfs2-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rados-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-cephfs-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
librbd1-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-debugsource-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rgw-12.2.10+git.1549630712.bb089269ea-2.27.2
librbd1-12.2.10+git.1549630712.bb089269ea-2.27.2
python-cephfs-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rbd-12.2.10+git.1549630712.bb089269ea-2.27.2
librgw2-12.2.10+git.1549630712.bb089269ea-2.27.2
libcephfs2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rados-12.2.10+git.1549630712.bb089269ea-2.27.2

SuSE SLES 12 SP3
x86_64
librados2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rgw-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-common-12.2.10+git.1549630712.bb089269ea-2.27.2
librados2-12.2.10+git.1549630712.bb089269ea-2.27.2
libradosstriper1-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
libradosstriper1-12.2.10+git.1549630712.bb089269ea-2.27.2
librgw2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rbd-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-common-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2

libcephfs2-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rados-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-cephfs-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
librbd1-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
ceph-debugsource-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rgw-12.2.10+git.1549630712.bb089269ea-2.27.2
librbd1-12.2.10+git.1549630712.bb089269ea-2.27.2
python-cephfs-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rbd-12.2.10+git.1549630712.bb089269ea-2.27.2
librgw2-12.2.10+git.1549630712.bb089269ea-2.27.2
libcephfs2-debuginfo-12.2.10+git.1549630712.bb089269ea-2.27.2
python-rados-12.2.10+git.1549630712.bb089269ea-2.27.2

147668 - SuSE Linux 15.0 openSUSE-SU-2019:0232-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14804

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0232-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00124.html

SuSE Linux 15.0
noarch
build-mkbaselibs-20190128-lp150.2.3.1
build-mkdrpms-20190128-lp150.2.3.1
build-20190128-lp150.2.3.1
build-initvm-i586-20190128-lp150.2.3.1
build-initvm-x86_64-20190128-lp150.2.3.1

147670 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0482-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
SUSE-SU-2019:0482-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005150.html

SuSE SLES 12 SP3
noarch
python-doc-pdf-2.7.13-28.21.1

python-doc-2.7.13-28.21.1

x86_64
python-base-debuginfo-2.7.13-28.21.1
python-gdbm-debuginfo-2.7.13-28.21.1
libpython2_7-1_0-2.7.13-28.21.1
python-base-32bit-2.7.13-28.21.1
python-xml-2.7.13-28.21.1
python-32bit-2.7.13-28.21.1
libpython2_7-1_0-32bit-2.7.13-28.21.1
libpython2_7-1_0-debuginfo-32bit-2.7.13-28.21.1
python-gdbm-2.7.13-28.21.1
python-demo-2.7.13-28.21.1
python-debuginfo-32bit-2.7.13-28.21.1
python-xml-debuginfo-2.7.13-28.21.1
python-2.7.13-28.21.1
python-curses-debuginfo-2.7.13-28.21.1
libpython2_7-1_0-debuginfo-2.7.13-28.21.1
python-debuginfo-2.7.13-28.21.1
python-base-debugsource-2.7.13-28.21.1
python-base-debuginfo-32bit-2.7.13-28.21.1
python-tk-debuginfo-2.7.13-28.21.1
python-base-2.7.13-28.21.1
python-debugsource-2.7.13-28.21.1
python-tk-2.7.13-28.21.1
python-idle-2.7.13-28.21.1
python-curses-2.7.13-28.21.1

SuSE SLES 12 SP4
noarch
python-doc-pdf-2.7.13-28.21.1
python-doc-2.7.13-28.21.1

x86_64
python-base-debuginfo-2.7.13-28.21.1
python-gdbm-debuginfo-2.7.13-28.21.1
libpython2_7-1_0-2.7.13-28.21.1
python-base-32bit-2.7.13-28.21.1
python-xml-2.7.13-28.21.1
python-32bit-2.7.13-28.21.1
libpython2_7-1_0-32bit-2.7.13-28.21.1
libpython2_7-1_0-debuginfo-32bit-2.7.13-28.21.1
python-gdbm-2.7.13-28.21.1
python-demo-2.7.13-28.21.1
python-debuginfo-32bit-2.7.13-28.21.1
python-xml-debuginfo-2.7.13-28.21.1
python-2.7.13-28.21.1
python-curses-debuginfo-2.7.13-28.21.1
libpython2_7-1_0-debuginfo-2.7.13-28.21.1
python-debuginfo-2.7.13-28.21.1
python-base-debugsource-2.7.13-28.21.1
python-base-debuginfo-32bit-2.7.13-28.21.1
python-tk-debuginfo-2.7.13-28.21.1
python-base-2.7.13-28.21.1
python-debugsource-2.7.13-28.21.1
python-tk-2.7.13-28.21.1
python-idle-2.7.13-28.21.1
python-curses-2.7.13-28.21.1

SuSE SLED 12 SP4

x86_64
python-base-debuginfo-2.7.13-28.21.1
libpython2_7-1_0-2.7.13-28.21.1
python-debugsource-2.7.13-28.21.1
python-devel-2.7.13-28.21.1
libpython2_7-1_0-32bit-2.7.13-28.21.1
libpython2_7-1_0-debuginfo-32bit-2.7.13-28.21.1
python-xml-debuginfo-2.7.13-28.21.1
python-xml-2.7.13-28.21.1
python-base-debuginfo-32bit-2.7.13-28.21.1
python-2.7.13-28.21.1
python-curses-debuginfo-2.7.13-28.21.1
libpython2_7-1_0-debuginfo-2.7.13-28.21.1
python-debuginfo-2.7.13-28.21.1
python-tk-debuginfo-2.7.13-28.21.1
python-base-2.7.13-28.21.1
python-base-debugsource-2.7.13-28.21.1
python-tk-2.7.13-28.21.1
python-curses-2.7.13-28.21.1

SuSE SLED 12 SP3
x86_64
python-base-debuginfo-2.7.13-28.21.1
libpython2_7-1_0-2.7.13-28.21.1
python-debugsource-2.7.13-28.21.1
python-devel-2.7.13-28.21.1
libpython2_7-1_0-32bit-2.7.13-28.21.1
libpython2_7-1_0-debuginfo-32bit-2.7.13-28.21.1
python-xml-debuginfo-2.7.13-28.21.1
python-xml-2.7.13-28.21.1
python-base-debuginfo-32bit-2.7.13-28.21.1
python-2.7.13-28.21.1
python-curses-debuginfo-2.7.13-28.21.1
libpython2_7-1_0-debuginfo-2.7.13-28.21.1
python-debuginfo-2.7.13-28.21.1
python-tk-debuginfo-2.7.13-28.21.1
python-base-2.7.13-28.21.1
python-base-debugsource-2.7.13-28.21.1
python-tk-2.7.13-28.21.1
python-curses-2.7.13-28.21.1

147673 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:0498-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17189, CVE-2018-17199

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0498-1

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-February/005156.html

SuSE SLES 12 SP3

noarch
apache2-doc-2.4.23-29.34.4

x86_64
apache2-debuginfo-2.4.23-29.34.4
apache2-debugsource-2.4.23-29.34.4
apache2-example-pages-2.4.23-29.34.4
apache2-worker-2.4.23-29.34.4
apache2-prefork-2.4.23-29.34.4
apache2-prefork-debuginfo-2.4.23-29.34.4
apache2-utils-2.4.23-29.34.4
apache2-2.4.23-29.34.4
apache2-worker-debuginfo-2.4.23-29.34.4
apache2-utils-debuginfo-2.4.23-29.34.4

SuSE SLES 12 SP4
noarch
apache2-doc-2.4.23-29.34.4

x86_64
apache2-debuginfo-2.4.23-29.34.4
apache2-debugsource-2.4.23-29.34.4
apache2-example-pages-2.4.23-29.34.4
apache2-worker-2.4.23-29.34.4
apache2-prefork-2.4.23-29.34.4
apache2-prefork-debuginfo-2.4.23-29.34.4
apache2-utils-2.4.23-29.34.4
apache2-2.4.23-29.34.4
apache2-worker-debuginfo-2.4.23-29.34.4
apache2-utils-debuginfo-2.4.23-29.34.4

186583 - Ubuntu Linux 14.04, 16.04 USN-3894-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20781

Description

The scan detected that the host is missing the following update:
USN-3894-1

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-February/004780.html

Ubuntu 14.04

gnome-keyring_3.10.1-1ubuntu4.4
libpam-gnome-keyring_3.10.1-1ubuntu4.4

Ubuntu 16.04

libpam-gnome-keyring_3.18.3-0ubuntu2.1
gnome-keyring_3.18.3-0ubuntu2.1

194812 - Fedora Linux 29 FEDORA-2019-6a2e72916a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14662, CVE-2018-16846, CVE-2018-16889

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6a2e72916a

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/2019/2/?count=200&page=3

Fedora Core 29

ceph-12.2.11-1.fc29

194821 - Fedora Linux 29 FEDORA-2019-d0af506401 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16476

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d0af506401

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

Fedora Core 29

rubygem-activejob-5.2.1-2.fc29

194823 - Fedora Linux 28 FEDORA-2019-afade40f3d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3813

Description

The scan detected that the host is missing the following update:
FEDORA-2019-afade40f3d

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

Fedora Core 28

spice-0.14.0-5.fc28

194829 - Fedora Linux 28 FEDORA-2019-31e6f6e545 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16476

Description

The scan detected that the host is missing the following update:
FEDORA-2019-31e6f6e545

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

Fedora Core 28

rubygem-activejob-5.1.5-2.fc28

196255 - Red Hat Enterprise Linux RHSA-2019-0396 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5784

Description

The scan detected that the host is missing the following update:
RHSA-2019-0396

Observation

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

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

RHEL6D
x86_64
chromium-browser-debuginfo-72.0.3626.96-1.el6_10
chromium-browser-72.0.3626.96-1.el6_10

i386
chromium-browser-debuginfo-72.0.3626.96-1.el6_10
chromium-browser-72.0.3626.96-1.el6_10

RHEL6S
x86_64
chromium-browser-debuginfo-72.0.3626.96-1.el6_10
chromium-browser-72.0.3626.96-1.el6_10

i386
chromium-browser-debuginfo-72.0.3626.96-1.el6_10
chromium-browser-72.0.3626.96-1.el6_10

RHEL6WS
x86_64
chromium-browser-debuginfo-72.0.3626.96-1.el6_10
chromium-browser-72.0.3626.96-1.el6_10

i386
chromium-browser-debuginfo-72.0.3626.96-1.el6_10
chromium-browser-72.0.3626.96-1.el6_10

147664 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0466-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5383

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0466-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005145.html

SuSE SLED 12 SP3
noarch
kernel-firmware-20170530-21.28.1
ucode-amd-20170530-21.28.1

SuSE SLES 12 SP3
noarch
kernel-firmware-20170530-21.28.1
ucode-amd-20170530-21.28.1

147671 - SuSE SLES 12 SP3 SUSE-SU-2019:0470-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18249, CVE-2019-3459, CVE-2019-3460

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0470-1

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-February/005147.html

SuSE SLES 12 SP3

x86_64
cluster-md-kmp-rt-debuginfo-4.4.172-3.35.1
kernel-rt-base-debuginfo-4.4.172-3.35.1
kernel-rt-4.4.172-3.35.1
kernel-rt_debug-debugsource-4.4.172-3.35.1
kernel-rt_debug-devel-4.4.172-3.35.1
kernel-rt_debug-devel-debuginfo-4.4.172-3.35.1
kernel-rt-debugsource-4.4.172-3.35.1
ocfs2-kmp-rt-debuginfo-4.4.172-3.35.1
kernel-syms-rt-4.4.172-3.35.1
dlm-kmp-rt-debuginfo-4.4.172-3.35.1
cluster-md-kmp-rt-4.4.172-3.35.1
kernel-rt-base-4.4.172-3.35.1
dlm-kmp-rt-4.4.172-3.35.1
gfs2-kmp-rt-debuginfo-4.4.172-3.35.1
gfs2-kmp-rt-4.4.172-3.35.1
kernel-rt-debuginfo-4.4.172-3.35.1
kernel-rt_debug-debuginfo-4.4.172-3.35.1
kernel-rt-devel-4.4.172-3.35.1
ocfs2-kmp-rt-4.4.172-3.35.1

noarch
kernel-source-rt-4.4.172-3.35.1
kernel-devel-rt-4.4.172-3.35.1

160521 - CentOS 7 CESA-2019-0375 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-8308

Description

The scan detected that the host is missing the following update:
CESA-2019-0375

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023203.html

CentOS 7
x86_64
flatpak-builder-1.0.0-4.el7_6
flatpak-devel-1.0.2-4.el7_6
flatpak-libs-1.0.2-4.el7_6
flatpak-1.0.2-4.el7_6

160522 - CentOS 6 CESA-2019-0415 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10902

Description

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

CESA-2019-0415

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023209.html

CentOS 6
i686
kernel-headers-2.6.32-754.11.1.el6
python-perf-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6

noarch
kernel-firmware-2.6.32-754.11.1.el6
kernel-doc-2.6.32-754.11.1.el6
kernel-abi-whitelists-2.6.32-754.11.1.el6

x86_64
kernel-headers-2.6.32-754.11.1.el6
python-perf-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6

160524 - CentOS 6 CESA-2019-0420 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6133

Description

The scan detected that the host is missing the following update:
CESA-2019-0420

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023210.html

CentOS 6
i686
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

noarch
polkit-desktop-policy-0.96-11.el6_10.1

x86_64
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

160525 - CentOS 6 CESA-2019-0416 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
CESA-2019-0416

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023208.html

CentOS 6
i686
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-1.el6_10

noarch
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-1.el6_10

x86_64
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-1.el6_10

163811 - Oracle Enterprise Linux ELSA-2019-0415 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10902

Description

The scan detected that the host is missing the following update:
ELSA-2019-0415

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-February/008497.html

OEL6
x86_64
kernel-headers-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
kernel-firmware-2.6.32-754.11.1.el6
kernel-doc-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
kernel-abi-whitelists-2.6.32-754.11.1.el6
python-perf-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6

i386
kernel-headers-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
kernel-firmware-2.6.32-754.11.1.el6
kernel-doc-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
kernel-abi-whitelists-2.6.32-754.11.1.el6
python-perf-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6

163812 - Oracle Enterprise Linux ELSA-2019-0420 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6133

Description

The scan detected that the host is missing the following update:
ELSA-2019-0420

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-February/008499.html

OEL6
x86_64
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-desktop-policy-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

i386
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-desktop-policy-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

163813 - Oracle Enterprise Linux ELSA-2019-0416 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-3639, CVE-2019-2422

Description

The scan detected that the host is missing the following update:
ELSA-2019-0416

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-February/008498.html

OEL6
x86_64
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-1.el6_10

i386
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-1.el6_10

194814 - Fedora Linux 29 FEDORA-2019-4e72b179e4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7628

Description

The scan detected that the host is missing the following update:
FEDORA-2019-4e72b179e4

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

Fedora Core 29

pagure-5.3-1.fc29

194816 - Fedora Linux 28 FEDORA-2019-3f9a71578d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3f9a71578d

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

Fedora Core 28

java-1.8.0-openjdk-1.8.0.201.b09-2.fc28

194828 - Fedora Linux 29 FEDORA-2019-307ebe924c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16477

Description

The scan detected that the host is missing the following update:
FEDORA-2019-307ebe924c

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

Fedora Core 29

rubygem-activestorage-5.2.1-3.fc29

196256 - Red Hat Enterprise Linux RHSA-2019-0416 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
RHSA-2019-0416

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-February/msg00028.html

RHEL6D
i386
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-1.el6_10

noarch
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-1.el6_10

x86_64
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-1.8.0.201.b09-1.el6_10

RHEL6S
i386
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-1.el6_10

java-1.8.0-openjdk-demo-1.8.0.201.b09-1.el6_10

noarch
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-1.el6_10

x86_64
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-demo-1.8.0.201.b09-1.el6_10

RHEL6WS
x86_64
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10

i386
java-1.8.0-openjdk-devel-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-headless-1.8.0.201.b09-1.el6_10
java-1.8.0-openjdk-1.8.0.201.b09-1.el6_10

196257 - Red Hat Enterprise Linux RHSA-2019-0415 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10902

Description

The scan detected that the host is missing the following update:
RHSA-2019-0415

Observation

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

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

RHEL6D
i386
kernel-headers-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
kernel-debuginfo-2.6.32-754.11.1.el6
python-perf-debuginfo-2.6.32-754.11.1.el6
python-perf-2.6.32-754.11.1.el6
kernel-debuginfo-common-i686-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
perf-debuginfo-2.6.32-754.11.1.el6

kernel-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
kernel-debug-debuginfo-2.6.32-754.11.1.el6

noarch
kernel-firmware-2.6.32-754.11.1.el6
kernel-doc-2.6.32-754.11.1.el6
kernel-abi-whitelists-2.6.32-754.11.1.el6

x86_64
python-perf-debuginfo-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6
python-perf-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
kernel-debuginfo-common-i686-2.6.32-754.11.1.el6
perf-debuginfo-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
kernel-debuginfo-common-x86_64-2.6.32-754.11.1.el6
kernel-debug-debuginfo-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
kernel-debuginfo-2.6.32-754.11.1.el6
kernel-headers-2.6.32-754.11.1.el6

RHEL6S
i386
kernel-headers-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
kernel-debuginfo-2.6.32-754.11.1.el6
python-perf-debuginfo-2.6.32-754.11.1.el6
python-perf-2.6.32-754.11.1.el6
kernel-debuginfo-common-i686-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
perf-debuginfo-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
kernel-debug-debuginfo-2.6.32-754.11.1.el6

noarch
kernel-firmware-2.6.32-754.11.1.el6
kernel-doc-2.6.32-754.11.1.el6
kernel-abi-whitelists-2.6.32-754.11.1.el6

x86_64
python-perf-debuginfo-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6
python-perf-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
kernel-debuginfo-common-i686-2.6.32-754.11.1.el6
perf-debuginfo-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
kernel-debuginfo-common-x86_64-2.6.32-754.11.1.el6
kernel-debug-debuginfo-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
kernel-debuginfo-2.6.32-754.11.1.el6
kernel-headers-2.6.32-754.11.1.el6

RHEL6WS
i386
kernel-headers-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
kernel-debuginfo-2.6.32-754.11.1.el6
python-perf-debuginfo-2.6.32-754.11.1.el6
kernel-debuginfo-common-i686-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
perf-debuginfo-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
kernel-debug-debuginfo-2.6.32-754.11.1.el6

noarch
kernel-firmware-2.6.32-754.11.1.el6
kernel-doc-2.6.32-754.11.1.el6
kernel-abi-whitelists-2.6.32-754.11.1.el6

x86_64
kernel-headers-2.6.32-754.11.1.el6
kernel-debug-2.6.32-754.11.1.el6
kernel-debuginfo-2.6.32-754.11.1.el6
python-perf-debuginfo-2.6.32-754.11.1.el6
kernel-debuginfo-common-i686-2.6.32-754.11.1.el6
kernel-debug-devel-2.6.32-754.11.1.el6
perf-debuginfo-2.6.32-754.11.1.el6
kernel-debuginfo-common-x86_64-2.6.32-754.11.1.el6
kernel-2.6.32-754.11.1.el6
perf-2.6.32-754.11.1.el6
kernel-devel-2.6.32-754.11.1.el6
kernel-debug-debuginfo-2.6.32-754.11.1.el6

196258 - Red Hat Enterprise Linux RHSA-2019-0420 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6133

Description

The scan detected that the host is missing the following update:
RHSA-2019-0420

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-February/msg00030.html

RHEL6D
i386
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-debuginfo-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

noarch
polkit-desktop-policy-0.96-11.el6_10.1

x86_64
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-debuginfo-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

RHEL6S
i386
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-debuginfo-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

noarch
polkit-desktop-policy-0.96-11.el6_10.1

x86_64
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-debuginfo-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

RHEL6WS
i386
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-debuginfo-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

noarch
polkit-desktop-policy-0.96-11.el6_10.1

x86_64
polkit-devel-0.96-11.el6_10.1
polkit-docs-0.96-11.el6_10.1
polkit-debuginfo-0.96-11.el6_10.1
polkit-0.96-11.el6_10.1

147667 - SuSE Linux 15.0 openSUSE-SU-2019:0233-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12546, CVE-2018-12550, CVE-2018-12551

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0233-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00125.html

SuSE Linux 15.0
x86_64
libmosquittopp1-debuginfo-1.4.15-lp150.2.3.1

libmosquitto1-1.4.15-lp150.2.3.1
libmosquitto1-debuginfo-1.4.15-lp150.2.3.1
mosquitto-1.4.15-lp150.2.3.1
mosquitto-debuginfo-1.4.15-lp150.2.3.1
mosquitto-clients-1.4.15-lp150.2.3.1
libmosquittopp1-1.4.15-lp150.2.3.1
mosquitto-devel-1.4.15-lp150.2.3.1
mosquitto-debugsource-1.4.15-lp150.2.3.1
mosquitto-clients-debuginfo-1.4.15-lp150.2.3.1

182918 - FreeBSD OpenSSL Undisclosed Vulnerability (7700061f-34f7-11e9-b95c-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OpenSSL -- Undisclosed vulnerability (7700061f-34f7-11e9-b95c-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/7700061f-34f7-11e9-b95c-b499baebfeaf.html

Affected packages:
openssl < 1.0.2r,1

182920 - FreeBSD webkit-gtk Multiple Vulnabilities (e3aacd6d-3d01-434c-9330-bc9efd40350f)

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
webkit-gtk -- Multiple vulnabilities (e3aacd6d-3d01-434c-9330-bc9efd40350f)

Observation

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

http://www.vuxml.org/freebsd/e3aacd6d-3d01-434c-9330-bc9efd40350f.html

Affected packages:
webkit2-gtk3 < 2.22.6

186582 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3893-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5744, CVE-2018-5745, CVE-2019-6465

Description

The scan detected that the host is missing the following update:
USN-3893-1

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-February/004777.html

Ubuntu 16.04

bind9_9.10.3.dfsg.P4-8ubuntu1.12

Ubuntu 18.10

bind9_9.11.4+dfsg-3ubuntu5.1

Ubuntu 14.04

bind9_9.9.5.dfsg-3ubuntu0.19

Ubuntu 18.04

bind9_9.11.3+dfsg-1ubuntu1.5

186586 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3866-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3866-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004776.html

Ubuntu 16.04

ghostscript_9.26~dfsg+0-0ubuntu0.16.04.5
libgs9_9.26~dfsg+0-0ubuntu0.16.04.5

Ubuntu 18.10

libgs9_9.26~dfsg+0-0ubuntu0.18.10.5
ghostscript_9.26~dfsg+0-0ubuntu0.18.10.5

Ubuntu 14.04

libgs9_9.26~dfsg+0-0ubuntu0.14.04.5
ghostscript_9.26~dfsg+0-0ubuntu0.14.04.5

Ubuntu 18.04

libgs9_9.26~dfsg+0-0ubuntu0.18.04.5
ghostscript_9.26~dfsg+0-0ubuntu0.18.04.5

186587 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3866-3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3866-3

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004779.html

Ubuntu 16.04

ghostscript_9.26~dfsg+0-0ubuntu0.16.04.7
libgs9_9.26~dfsg+0-0ubuntu0.16.04.7

Ubuntu 18.10

ghostscript_9.26~dfsg+0-0ubuntu0.18.10.7
libgs9_9.26~dfsg+0-0ubuntu0.18.10.7

Ubuntu 14.04

libgs9_9.26~dfsg+0-0ubuntu0.14.04.7
ghostscript_9.26~dfsg+0-0ubuntu0.14.04.7

Ubuntu 18.04

libgs9_9.26~dfsg+0-0ubuntu0.18.04.7
ghostscript_9.26~dfsg+0-0ubuntu0.18.04.7

186588 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3895-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3824

Description

The scan detected that the host is missing the following update:
USN-3895-1

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-February/004781.html

Ubuntu 16.04

libldb1_1.1.24-1ubuntu3.1

Ubuntu 18.10

libldb1_1.4.0+really1.3.5-2ubuntu0.1

Ubuntu 14.04

libldb1_1.1.24-0ubuntu0.14.04.2

Ubuntu 18.04

libldb1_1.2.3-1ubuntu0.1

194804 - Fedora Linux 28 FEDORA-2019-362387a66d 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-2019-362387a66d

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

Fedora Core 28

java-1.8.0-openjdk-aarch32-1.8.0.201.190124-1.fc28

194806 - Fedora Linux 29 FEDORA-2019-b084fa3ea5 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-b084fa3ea5

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

Fedora Core 29

java-1.8.0-openjdk-aarch32-1.8.0.201.190124-1.fc29

194808 - Fedora Linux 29 FEDORA-2019-3b8d06c61e 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-2019-3b8d06c61e

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/2019/2/?count=200&page=3

Fedora Core 29

firefox-65.0.1-1.fc29

194809 - Fedora Linux 29 FEDORA-2019-50ca715929 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1002161

Description

The scan detected that the host is missing the following update:
FEDORA-2019-50ca715929

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

Fedora Core 29

koji-1.16.2-1.fc29

194818 - Fedora Linux 29 FEDORA-2019-e0f5a82082 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20187

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e0f5a82082

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/2019/2/?count=200&page=3

Fedora Core 29

botan2-2.9.0-1.fc29

194822 - Fedora Linux 29 FEDORA-2019-cba0f77eab 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-cba0f77eab

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

Fedora Core 29

thunderbird-60.5.1-1.fc29

194825 - Fedora Linux 29 FEDORA-2019-5396a60397 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5744, CVE-2018-5745, CVE-2019-6465

Description

The scan detected that the host is missing the following update:
FEDORA-2019-5396a60397

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

Fedora Core 29

bind-9.11.5-4.P4.fc29

194827 - Fedora Linux 28 FEDORA-2019-5c54d58073 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6212, CVE-2019-6215

Description

The scan detected that the host is missing the following update:
FEDORA-2019-5c54d58073

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/2019/2/?count=200&page=3

Fedora Core 28

webkit2gtk3-2.22.6-1.fc28

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.