2019-MAR-27
FSL version 7.6.103

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

24744 - Mozilla Firefox Multiple Vulnerabilities Prior To 65

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

Risk Level: High

CVE: CVE-2011-3079, CVE-2018-18500, CVE-2018-18501, CVE-2018-18502, CVE-2018-18503, CVE-2018-18504, CVE-2018-18505, CVE-2018-18506

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

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

24750 - Mozilla Firefox ESR Vulnerabilities Prior To ESR 60.5

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

Risk Level: High

CVE: CVE-2011-3079, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Description

Multiple Vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple Vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to remotely execute arbitrary code, gain elevated privileges and cause a denial of service condition.

24898 - (APSB19-16) Vulnerability In Adobe Digital Editions

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

Risk Level: High

CVE: CVE-2019-7095

Description

A vulnerability is present in some versions of Adobe Digital Editions.

Observation

Adobe Digital Editions is the Adobe's eBook reader software.

A vulnerability is present in some versions of Adobe Digital Editions. The flaw is due to the application fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer. Successful exploitation could allow an attacker to execute arbitrary code.

24861 - (APSB19-14) Vulnerabilities In Adobe ColdFusion

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

Risk Level: High

CVE: CVE-2019-7816

Description

A vulnerability is present in some versions of Adobe ColdFusion.

Observation

Adobe ColdFusion is a web application development platform.

A vulnerability is present in some versions of Adobe ColdFusion. The flaw is due to improper restriction of file uploading. Successful exploitation could allow an attacker to gain arbitrary code execution.

The update provided by Adobe bulletin APSB19-14 resolves these issues. The target system appears to be missing this update.

24893 - (SB10276) McAfee Web Gateway Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4463, CVE-2017-16997, CVE-2018-0494, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301, CVE-2018-1060, CVE-2018-1061, CVE-2018-10897, CVE-2018-11236, CVE-2018-11237, CVE-2018-16864, CVE-2018-16865, CVE-2018-18311, CVE-2018-6485

Description

Multiple vulnerabilities are present in some versions of McAfee Web Gateway.

Observation

McAfee Web Gateway is a web based security control system designed to prevent web application attacks.

Multiple vulnerabilities are present in some versions of McAfee Web Gateway. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or execute arbitrary code.

147729 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0655-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Description

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

SUSE-SU-2019:0655-1

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-March/005210.html

SuSE SLED 12 SP3
x86_64
libssh2-1-debuginfo-32bit-1.4.3-20.3.1
libssh2_org-debugsource-1.4.3-20.3.1
libssh2-1-debuginfo-1.4.3-20.3.1
libssh2-1-32bit-1.4.3-20.3.1
libssh2-1-1.4.3-20.3.1

SuSE SLED 12 SP4
x86_64
libssh2-1-debuginfo-32bit-1.4.3-20.3.1
libssh2_org-debugsource-1.4.3-20.3.1
libssh2-1-debuginfo-1.4.3-20.3.1
libssh2-1-32bit-1.4.3-20.3.1
libssh2-1-1.4.3-20.3.1

SuSE SLES 12 SP4
x86_64
libssh2-1-debuginfo-32bit-1.4.3-20.3.1
libssh2-1-32bit-1.4.3-20.3.1
libssh2_org-debugsource-1.4.3-20.3.1
libssh2-1-debuginfo-1.4.3-20.3.1
libssh2-1-1.4.3-20.3.1

SuSE SLES 12 SP3
x86_64
libssh2-1-debuginfo-32bit-1.4.3-20.3.1
libssh2-1-32bit-1.4.3-20.3.1
libssh2_org-debugsource-1.4.3-20.3.1
libssh2-1-debuginfo-1.4.3-20.3.1
libssh2-1-1.4.3-20.3.1

194908 - Fedora Linux 29 FEDORA-2019-f31c14682f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f31c14682f

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/2019/3/?count=200&page=1

Fedora Core 29

libssh2-1.8.1-1.fc29

24767 - LibreOffice Directory Traversal Vulnerability (CVE-2018-16858)

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

Risk Level: High

CVE: CVE-2018-16858

Description

A vulnerability is present in some versions of LibreOffice.

Observation

LibreOffice is an open source office suite.

A vulnerability is present in some versions of LibreOffice. The flaw lies in pre-installed macros execution feature. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

24900 - Cisco NX-OS Software Privilege Escalation Vulnerability (CVE-2019-1604)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1604

Description

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

Observation

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

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to insufficient authorization check of user accounts. Successful exploitation could allow an authenticated attacker to gain elevated privileges.

24746 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 60.5

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

Risk Level: High

CVE: CVE-2016-5824, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505, CVE-2018-18512, CVE-2018-18513

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

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

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, bypass security access restrictions or remotely execute arbitrary code on the target system.

24781 - Mozilla Firefox ESR Vulnerabilities Prior To 60.5.1

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

Risk Level: High

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

Description

Multiple Vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple Vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition.

24789 - Mozilla Firefox Vulnerabilities Prior To 65.0.1

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

Risk Level: High

CVE: CVE-2018-18356, CVE-2018-18511, CVE-2019-5785

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

24879 - Google Chrome Vulnerability Prior To 72.0.3626.121

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

Risk Level: High

CVE: CVE-2019-5786

Description

A Vulnerability is present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

A Vulnerability is present in some versions of Google Chrome. The flaw is due to use-after-free condition in FileReader. Successful exploitation could allow an attacker to execute remote code on the targeted system.

24890 - IBM DB2 Java Vulnerability (ibm10741443)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-3180

Description

A vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw lies in JDK. Successful exploitation could allow an attacker to cause low confidentiality impact, low integrity impact, and low availability impact.

24897 - (K95343321) F5 BIG-IP Linux kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2018-5390

Description

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

Observation

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

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

24912 - IBM DB2 Multiple Java Vulnerabilities (ibm10875132)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-12547, CVE-2018-1890, CVE-2019-2426

Description

Multiple vulnerabilities are present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

Multiple vulnerabilities are present in some versions of IBM DB2. The flaws lie in JDK. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or execute arbitrary code.

24913 - Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1608)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1608

Description

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

Observation

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

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

24914 - Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1612)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1612

Description

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

Observation

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

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

24918 - (VMSA-2019-0002) VMware Workstation Player Multiple Elevation Of Privilege Vulnerabilities

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

Risk Level: High

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

Description

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

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in multiple components. Successful exploitation could allow a malicious attacker to gain elevated privileges on the target system.

147728 - SuSE SLES 12 SP3 SUSE-SU-2019:0738-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12181

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0738-1

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-March/005234.html

SuSE SLES 12 SP3
noarch
qemu-ovmf-x86_64-2017+git1492060560.b6d11d7c46-4.23.1
qemu-uefi-aarch64-2017+git1492060560.b6d11d7c46-4.23.1

x86_64
ovmf-2017+git1492060560.b6d11d7c46-4.23.1
ovmf-tools-2017+git1492060560.b6d11d7c46-4.23.1

147730 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0765-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5753, CVE-2018-20669, CVE-2019-2024, CVE-2019-3459, CVE-2019-3460, CVE-2019-3819, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0765-1

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-March/005243.html
http://lists.suse.com/pipermail/sle-security-updates/2019-March/005240.html

SuSE SLED 12 SP4
x86_64
kernel-default-extra-4.12.14-95.13.1
kernel-default-devel-4.12.14-95.13.1
kernel-default-extra-debuginfo-4.12.14-95.13.1
kernel-default-debugsource-4.12.14-95.13.1
kernel-syms-4.12.14-95.13.1
kernel-default-4.12.14-95.13.1
kernel-default-debuginfo-4.12.14-95.13.1
kernel-default-devel-debuginfo-4.12.14-95.13.1

noarch
kernel-devel-4.12.14-95.13.1
kernel-source-4.12.14-95.13.1
kernel-macros-4.12.14-95.13.1

SuSE SLES 12 SP4
noarch
kernel-devel-4.12.14-95.13.1
kernel-source-4.12.14-95.13.1
kernel-macros-4.12.14-95.13.1

x86_64
kernel-syms-4.12.14-95.13.1
kernel-default-devel-4.12.14-95.13.1
kernel-default-base-debuginfo-4.12.14-95.13.1
kernel-default-debugsource-4.12.14-95.13.1
kernel-default-4.12.14-95.13.1
kernel-default-debuginfo-4.12.14-95.13.1
kernel-default-base-4.12.14-95.13.1
kernel-default-devel-debuginfo-4.12.14-95.13.1

147735 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0736-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0736-1

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-March/005233.html
http://lists.suse.com/pipermail/sle-security-updates/2019-March/005232.html

SuSE SLED 12 SP3
x86_64
ucode-intel-debuginfo-20190312-13.38.1
ucode-intel-debugsource-20190312-13.38.1
ucode-intel-20190312-13.38.1

SuSE SLED 12 SP4
x86_64
ucode-intel-debuginfo-20190312-13.38.1
ucode-intel-debugsource-20190312-13.38.1
ucode-intel-20190312-13.38.1

SuSE SLES 12 SP4
x86_64
ucode-intel-debuginfo-20190312-13.38.1
ucode-intel-debugsource-20190312-13.38.1
ucode-intel-20190312-13.38.1

SuSE SLES 12 SP3
x86_64
ucode-intel-debuginfo-20190312-13.38.1
ucode-intel-debugsource-20190312-13.38.1
ucode-intel-20190312-13.38.1

147736 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0747-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6977, CVE-2019-6978

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0747-1

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-March/005236.html

SuSE SLES 12 SP3
x86_64
gd-debugsource-2.1.0-24.12.1

gd-debuginfo-2.1.0-24.12.1
gd-2.1.0-24.12.1

SuSE SLES 12 SP4
x86_64
gd-debugsource-2.1.0-24.12.1
gd-debuginfo-2.1.0-24.12.1
gd-2.1.0-24.12.1

SuSE SLED 12 SP4
x86_64
gd-32bit-2.1.0-24.12.1
gd-debuginfo-2.1.0-24.12.1
gd-2.1.0-24.12.1
gd-debugsource-2.1.0-24.12.1
gd-debuginfo-32bit-2.1.0-24.12.1

SuSE SLED 12 SP3
x86_64
gd-32bit-2.1.0-24.12.1
gd-debuginfo-2.1.0-24.12.1
gd-2.1.0-24.12.1
gd-debugsource-2.1.0-24.12.1
gd-debuginfo-32bit-2.1.0-24.12.1

147737 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0719-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3838

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0719-1

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-March/005228.html

SuSE SLED 12 SP3
x86_64
ghostscript-9.26a-23.22.1
ghostscript-debugsource-9.26a-23.22.1
ghostscript-debuginfo-9.26a-23.22.1
ghostscript-x11-debuginfo-9.26a-23.22.1
ghostscript-x11-9.26a-23.22.1

SuSE SLED 12 SP4
x86_64
ghostscript-9.26a-23.22.1
ghostscript-debugsource-9.26a-23.22.1
ghostscript-debuginfo-9.26a-23.22.1
ghostscript-x11-debuginfo-9.26a-23.22.1
ghostscript-x11-9.26a-23.22.1

SuSE SLES 12 SP4

x86_64
ghostscript-9.26a-23.22.1
ghostscript-debugsource-9.26a-23.22.1
ghostscript-debuginfo-9.26a-23.22.1
ghostscript-x11-debuginfo-9.26a-23.22.1
ghostscript-x11-9.26a-23.22.1

SuSE SLES 12 SP3
x86_64
ghostscript-9.26a-23.22.1
ghostscript-debugsource-9.26a-23.22.1
ghostscript-debuginfo-9.26a-23.22.1
ghostscript-x11-debuginfo-9.26a-23.22.1
ghostscript-x11-9.26a-23.22.1

160535 - CentOS 7 CESA-2019-0633 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
CESA-2019-0633

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-March/023251.html

CentOS 7
i686
ghostscript-devel-9.07-31.el7_6.10
ghostscript-9.07-31.el7_6.10

noarch
ghostscript-doc-9.07-31.el7_6.10

x86_64
ghostscript-9.07-31.el7_6.10
ghostscript-devel-9.07-31.el7_6.10
ghostscript-gtk-9.07-31.el7_6.10
ghostscript-cups-9.07-31.el7_6.10

163830 - Oracle Enterprise Linux ELSA-2019-0633 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2019-0633

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008596.html
http://oss.oracle.com/pipermail/el-errata/2019-March/008595.html

OEL7
x86_64
ghostscript-gtk-9.07-31.el7_6.10
ghostscript-9.07-31.el7_6.10
ghostscript-devel-9.07-31.el7_6.10
ghostscript-doc-9.07-31.el7_6.10
ghostscript-cups-9.07-31.el7_6.10

171076 - Amazon Linux AMI ALAS-2019-1174 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6978

Description

The scan detected that the host is missing the following update:
ALAS-2019-1174

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1174.html

Amazon Linux AMI
x86_64
libwmf-debuginfo-0.2.8.4-41.13.amzn1
libwmf-0.2.8.4-41.13.amzn1
libwmf-devel-0.2.8.4-41.13.amzn1
libwmf-lite-0.2.8.4-41.13.amzn1

i686
libwmf-0.2.8.4-41.13.amzn1
libwmf-debuginfo-0.2.8.4-41.13.amzn1
libwmf-devel-0.2.8.4-41.13.amzn1
libwmf-lite-0.2.8.4-41.13.amzn1

171077 - Amazon Linux AMI ALAS-2019-1180 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18311

Description

The scan detected that the host is missing the following update:
ALAS-2019-1180

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1180.html

Amazon Linux AMI
i686
perl-Time-Piece-1.20.1-294.43.amzn1
perl-debuginfo-5.16.3-294.43.amzn1
perl-core-5.16.3-294.43.amzn1
perl-macros-5.16.3-294.43.amzn1
perl-devel-5.16.3-294.43.amzn1
perl-tests-5.16.3-294.43.amzn1
perl-libs-5.16.3-294.43.amzn1
perl-5.16.3-294.43.amzn1

noarch
perl-CPAN-1.9800-294.43.amzn1
perl-Locale-Maketext-Simple-0.21-294.43.amzn1
perl-Package-Constants-0.02-294.43.amzn1
perl-IO-Zlib-1.10-294.43.amzn1
perl-Pod-Escapes-1.04-294.43.amzn1
perl-Object-Accessor-0.42-294.43.amzn1
perl-ExtUtils-CBuilder-0.28.2.6-294.43.amzn1
perl-Module-Loaded-0.08-294.43.amzn1
perl-ExtUtils-Install-1.58-294.43.amzn1
perl-Module-CoreList-2.76.02-294.43.amzn1
perl-ExtUtils-Embed-1.30-294.43.amzn1

x86_64
perl-macros-5.16.3-294.43.amzn1
perl-debuginfo-5.16.3-294.43.amzn1
perl-Time-Piece-1.20.1-294.43.amzn1
perl-core-5.16.3-294.43.amzn1
perl-devel-5.16.3-294.43.amzn1
perl-tests-5.16.3-294.43.amzn1
perl-libs-5.16.3-294.43.amzn1
perl-5.16.3-294.43.amzn1

171084 - Amazon Linux AMI ALAS-2019-1179 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8980, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
ALAS-2019-1179

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1179.html

Amazon Linux AMI
x86_64
kernel-headers-4.14.106-79.86.amzn1
kernel-4.14.106-79.86.amzn1
perf-debuginfo-4.14.106-79.86.amzn1

kernel-debuginfo-4.14.106-79.86.amzn1
kernel-devel-4.14.106-79.86.amzn1
kernel-tools-4.14.106-79.86.amzn1
kernel-debuginfo-common-x86_64-4.14.106-79.86.amzn1
perf-4.14.106-79.86.amzn1
kernel-tools-devel-4.14.106-79.86.amzn1
kernel-tools-debuginfo-4.14.106-79.86.amzn1

i686
kernel-headers-4.14.106-79.86.amzn1
kernel-tools-4.14.106-79.86.amzn1
kernel-4.14.106-79.86.amzn1
kernel-devel-4.14.106-79.86.amzn1
kernel-debuginfo-common-i686-4.14.106-79.86.amzn1
kernel-debuginfo-4.14.106-79.86.amzn1
perf-4.14.106-79.86.amzn1
kernel-tools-devel-4.14.106-79.86.amzn1
kernel-tools-debuginfo-4.14.106-79.86.amzn1
perf-debuginfo-4.14.106-79.86.amzn1

194890 - Fedora Linux 28 FEDORA-2019-779a9db46a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18342

Description

The scan detected that the host is missing the following update:
FEDORA-2019-779a9db46a

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/2019/3/?count=200&page=1

Fedora Core 28

PyYAML-5.1-1.fc28

194903 - Fedora Linux 28 FEDORA-2019-a9c08d4b40 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18407, CVE-2018-18408, CVE-2019-8376, CVE-2019-8377, CVE-2019-8381

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a9c08d4b40

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/2019/3/?count=200&page=1

Fedora Core 28

tcpreplay-4.3.2-1.fc28

194906 - Fedora Linux 29 FEDORA-2019-88a98ce795 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10839, CVE-2018-15746, CVE-2018-16867, CVE-2018-16872, CVE-2018-17958, CVE-2018-17962, CVE-2018-17963, CVE-2018-18849, CVE-2018-18954, CVE-2018-19364, CVE-2018-19489, CVE-2018-20191, CVE-2019-3812, CVE-2019-6778

Description

The scan detected that the host is missing the following update:
FEDORA-2019-88a98ce795

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/2019/3/?count=200&page=1

Fedora Core 29

qemu-3.0.0-4.fc29

194911 - Fedora Linux 29 FEDORA-2019-bed9afe622 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18342

Description

The scan detected that the host is missing the following update:
FEDORA-2019-bed9afe622

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

Fedora Core 29

PyYAML-5.1-1.fc29

194913 - Fedora Linux 29 FEDORA-2019-e40253f67e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18407, CVE-2018-18408, CVE-2019-8376, CVE-2019-8377, CVE-2019-8381

Description

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

FEDORA-2019-e40253f67e

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/2019/3/?count=200&page=1

Fedora Core 29

tcpreplay-4.3.2-1.fc29

194914 - Fedora Linux 28 FEDORA-2019-bce6498890 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10471, CVE-2018-10472, CVE-2018-10981, CVE-2018-10982, CVE-2018-12891, CVE-2018-12892, CVE-2018-12893, CVE-2018-15468, CVE-2018-15469, CVE-2018-15470, CVE-2018-18883, CVE-2018-19961, CVE-2018-19962, CVE-2018-19965, CVE-2018-19966, CVE-2018-19967, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-3665, CVE-2018-8897

Description

The scan detected that the host is missing the following update:
FEDORA-2019-bce6498890

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

Fedora Core 28

xen-4.10.3-2.fc28

196274 - Red Hat Enterprise Linux RHSA-2019-0633 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2019-0633

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00034.html

RHEL7D
x86_64
ghostscript-gtk-9.07-31.el7_6.10
ghostscript-9.07-31.el7_6.10
ghostscript-devel-9.07-31.el7_6.10

ghostscript-debuginfo-9.07-31.el7_6.10
ghostscript-cups-9.07-31.el7_6.10

noarch
ghostscript-doc-9.07-31.el7_6.10

RHEL7S
noarch
ghostscript-doc-9.07-31.el7_6.10

x86_64
ghostscript-gtk-9.07-31.el7_6.10
ghostscript-9.07-31.el7_6.10
ghostscript-devel-9.07-31.el7_6.10
ghostscript-debuginfo-9.07-31.el7_6.10
ghostscript-cups-9.07-31.el7_6.10

RHEL7WS
x86_64
ghostscript-gtk-9.07-31.el7_6.10
ghostscript-9.07-31.el7_6.10
ghostscript-devel-9.07-31.el7_6.10
ghostscript-debuginfo-9.07-31.el7_6.10
ghostscript-cups-9.07-31.el7_6.10

noarch
ghostscript-doc-9.07-31.el7_6.10

24798 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 60.5.1

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

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

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

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

147734 - SuSE SLES 11 SP4 SUSE-SU-2019:13985-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9318, CVE-2018-14404

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13985-1

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-March/005217.html

SuSE SLES 11 SP4
i586
libxml2-doc-2.7.6-0.77.15.1
libxml2-2.7.6-0.77.15.1
libxml2-python-2.7.6-0.77.15.1

x86_64
libxml2-doc-2.7.6-0.77.15.1
libxml2-2.7.6-0.77.15.1
libxml2-python-2.7.6-0.77.15.1
libxml2-32bit-2.7.6-0.77.15.1

163828 - Oracle Enterprise Linux ELSA-2019-4594 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10879

Description

The scan detected that the host is missing the following update:
ELSA-2019-4594

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008602.html
http://oss.oracle.com/pipermail/el-errata/2019-March/008603.html

OEL7
x86_64
kernel-uek-debug-devel-4.1.12-124.26.5.el7uek
kernel-uek-4.1.12-124.26.5.el7uek
kernel-uek-doc-4.1.12-124.26.5.el7uek
kernel-uek-debug-4.1.12-124.26.5.el7uek
kernel-uek-devel-4.1.12-124.26.5.el7uek
kernel-uek-firmware-4.1.12-124.26.5.el7uek

OEL6
x86_64
kernel-uek-doc-4.1.12-124.26.5.el6uek
kernel-uek-firmware-4.1.12-124.26.5.el6uek
kernel-uek-debug-devel-4.1.12-124.26.5.el6uek
kernel-uek-4.1.12-124.26.5.el6uek
kernel-uek-debug-4.1.12-124.26.5.el6uek
kernel-uek-devel-4.1.12-124.26.5.el6uek

171079 - Amazon Linux AMI ALAS-2019-1186 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-8904, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907

Description

The scan detected that the host is missing the following update:
ALAS-2019-1186

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1186.html

Amazon Linux AMI
i686
file-libs-5.34-3.37.amzn1
file-static-5.34-3.37.amzn1
file-debuginfo-5.34-3.37.amzn1
file-5.34-3.37.amzn1
file-devel-5.34-3.37.amzn1

noarch
python27-magic-5.34-3.37.amzn1
python26-magic-5.34-3.37.amzn1

x86_64
file-libs-5.34-3.37.amzn1
file-debuginfo-5.34-3.37.amzn1
file-devel-5.34-3.37.amzn1
file-5.34-3.37.amzn1
file-static-5.34-3.37.amzn1

186618 - Ubuntu Linux 16.04 USN-3912-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12447

Description

The scan detected that the host is missing the following update:
USN-3912-1

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-March/004807.html

Ubuntu 16.04

libgdk-pixbuf2.0-0_2.32.2-1ubuntu1.6

186619 - Ubuntu Linux 16.04 USN-3913-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2335, CVE-2017-17969

Description

The scan detected that the host is missing the following update:
USN-3913-1

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-March/004810.html

Ubuntu 16.04

p7zip-full_9.20.1~dfsg.1-4.2ubuntu0.1
p7zip_9.20.1~dfsg.1-4.2ubuntu0.1

194892 - Fedora Linux 28 FEDORA-2019-d333d01e08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20004, CVE-2018-20005, CVE-2018-20592, CVE-2018-20593

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d333d01e08

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/2019/3/?count=200&page=1

Fedora Core 28

mxml-3.0-1.fc28

194893 - Fedora Linux 28 FEDORA-2019-918aad6bd5 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-2019-918aad6bd5

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

Fedora Core 28

SDL-1.2.15-32.fc28

194895 - Fedora Linux 29 FEDORA-2019-561eae4626 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5754, CVE-2019-5755, CVE-2019-5756, CVE-2019-5757, CVE-2019-5758, CVE-2019-5759, CVE-2019-5760, CVE-2019-5761, CVE-2019-5762, CVE-2019-5763, CVE-2019-5764, CVE-2019-5765, CVE-2019-5766, CVE-2019-5767, CVE-2019-5768, CVE-2019-5769, CVE-2019-5770, CVE-2019-5771, CVE-2019-5772, CVE-2019-5773, CVE-2019-5774, CVE-2019-5775, CVE-2019-5776, CVE-2019-5777, CVE-2019-5778, CVE-2019-5779, CVE-2019-5780, CVE-2019-5781, CVE-2019-5782, CVE-2019-5784, CVE-2019-5786, CVE-2019-5787, CVE-2019-5788, CVE-2019-5789, CVE-2019-5790, CVE-2019-5791, CVE-2019-5792, CVE-2019-5793, CVE-2019-5794, CVE-2019-5795, CVE-2019-5796, CVE-2019-5797, CVE-2019-5798, CVE-2019-5799, CVE-2019-5800, CVE-2019-5801, CVE-2019-5802, CVE-2019-5803, CVE-2019-5804

Description

The scan detected that the host is missing the following update:
FEDORA-2019-561eae4626

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/2019/3/?count=200&page=1

Fedora Core 29

chromium-73.0.3683.75-2.fc29

194897 - Fedora Linux 29 FEDORA-2019-0233ec0ff3 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0233ec0ff3

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/2019/3/?count=200&page=1

Fedora Core 29

libarchive-3.3.3-6.fc29

194918 - Fedora Linux 29 FEDORA-2019-15d57af79a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6116

Description

The scan detected that the host is missing the following update:
FEDORA-2019-15d57af79a

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

Fedora Core 29

ghostscript-9.26-3.fc29

194922 - Fedora Linux 28 FEDORA-2019-7b9bb0e426 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10194, CVE-2018-16802, CVE-2019-6116

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7b9bb0e426

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

Fedora Core 28

ghostscript-9.26-3.fc28

194923 - Fedora Linux 28 FEDORA-2019-8606c6da35 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12895

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8606c6da35

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

Fedora Core 28

wordpress-5.1.1-1.fc28

24878 - IBM WebSphere Application Server Admin Console Cross-Site Scripting Vulnerability (ibm10873042)

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

Risk Level: Medium

CVE: CVE-2019-4030

Description

A vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

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

A vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in Admin Console. Successful exploitation could allow an attacker to execute arbitrary JavaScript code, leading to credentials disclosure within a trusted session.

24884 - IBM WebSphere Application Server Multiple Vulnerabilities (ibm10873042)

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

Risk Level: Medium

CVE: CVE-2018-12547, CVE-2018-1890, CVE-2019-2426

Description

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

Observation

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

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaws lie in IBM Java SDK. Successful exploitation could allow a remote attacker to obtain elevated privileges, execute remote code, retrieve sensitive information or cause a denial of service condition on the target system.

24889 - Cisco NX-OS Software Privilege Escalation Vulnerability (CVE-2019-1603)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-1603

Description

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

Observation

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

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to insufficient authorization enforcement. Successful exploitation could allow an authenticated attacker to gain elevated privileges.

24895 - IBM WebSphere Application Server Spoofing Vulnerability (ibm10795115)

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

Risk Level: Medium

CVE: CVE-2018-1902

Description

A vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

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

A vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in unknown component. Successful exploitation could allow a remote attacker to affect the integrity and disclose the sensitive information of target system.

24908 - Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1613)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-1613

Description

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

Observation

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

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

24910 - IBM WebSphere Service Registry And Repository Multiple Vulnerabilities (ibm10874918)

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

Risk Level: Medium

CVE: CVE-2018-12547, CVE-2019-2426

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Service Registry and Repository.

Observation

IBM WebSphere Service Registry and Repository is a product for enterprise's service oriented architecture applications.

Multiple vulnerabilities are present in some versions of IBM WebSphere Service Registry and Repository. The flaws lie in IBM Java SDK. Successful exploitation could allow an attacker to retrieve sensitive information, execute arbitrary code or cause a denial of service condition on the target system.

24911 - IBM WebSphere Service Registry And Repository Multiple Vulnerabilities (ibm10874918)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-12547, CVE-2019-2426

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Service Registry and Repository.

Observation

IBM WebSphere Service Registry and Repository is a product for enterprise's service oriented architecture applications.

Multiple vulnerabilities are present in some versions of IBM WebSphere Service Registry and Repository. The flaws lie in IBM Java

SDK. Successful exploitation could allow an attacker to retrieve sensitive information, execute arbitrary code or cause a denial of service condition on the target system.

131317 - Debian Linux 9.0 DSA-4416-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5716, CVE-2019-5717, CVE-2019-5718, CVE-2019-5719, CVE-2019-9208, CVE-2019-9209, CVE-2019-9214

Description

The scan detected that the host is missing the following update:
DSA-4416-1

Observation

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

http://www.debian.org/security/2019/dsa-4416

Debian 9.0
all
wireshark_2.6.7-1~deb9u1

147731 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0656-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0656-1

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-March/005211.html

SuSE SLED 12 SP3
x86_64
libwsman_clientpp1-2.4.11-21.8.1
openwsman-server-debuginfo-2.4.11-21.8.1
openwsman-debugsource-2.4.11-21.8.1
openwsman-server-2.4.11-21.8.1
libwsman1-debuginfo-2.4.11-21.8.1
libwsman1-2.4.11-21.8.1
libwsman_clientpp1-debuginfo-2.4.11-21.8.1

SuSE SLED 12 SP4
x86_64
libwsman_clientpp1-2.4.11-21.8.1
openwsman-server-debuginfo-2.4.11-21.8.1
openwsman-debugsource-2.4.11-21.8.1
openwsman-server-2.4.11-21.8.1
libwsman1-debuginfo-2.4.11-21.8.1

libwsman1-2.4.11-21.8.1
libwsman_clientpp1-debuginfo-2.4.11-21.8.1

SuSE SLES 12 SP4
x86_64
libwsman_clientpp1-2.4.11-21.8.1
openwsman-server-debuginfo-2.4.11-21.8.1
openwsman-debugsource-2.4.11-21.8.1
openwsman-server-2.4.11-21.8.1
libwsman1-debuginfo-2.4.11-21.8.1
libwsman1-2.4.11-21.8.1
libwsman_clientpp1-debuginfo-2.4.11-21.8.1

SuSE SLES 12 SP3
x86_64
libwsman_clientpp1-2.4.11-21.8.1
openwsman-server-debuginfo-2.4.11-21.8.1
openwsman-debugsource-2.4.11-21.8.1
openwsman-server-2.4.11-21.8.1
libwsman1-debuginfo-2.4.11-21.8.1
libwsman1-2.4.11-21.8.1
libwsman_clientpp1-debuginfo-2.4.11-21.8.1

147732 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0688-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9208, CVE-2019-9209, CVE-2019-9214

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0688-1

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-March/005216.html

SuSE SLED 12 SP3
x86_64
wireshark-debugsource-2.4.13-48.42.1
libwscodecs1-debuginfo-2.4.13-48.42.1
wireshark-2.4.13-48.42.1
libwsutil8-2.4.13-48.42.1
wireshark-gtk-debuginfo-2.4.13-48.42.1
libwsutil8-debuginfo-2.4.13-48.42.1
libwscodecs1-2.4.13-48.42.1
wireshark-gtk-2.4.13-48.42.1
libwiretap7-2.4.13-48.42.1
wireshark-debuginfo-2.4.13-48.42.1
libwireshark9-debuginfo-2.4.13-48.42.1
libwiretap7-debuginfo-2.4.13-48.42.1
libwireshark9-2.4.13-48.42.1

SuSE SLED 12 SP4
x86_64
wireshark-debugsource-2.4.13-48.42.1

libwscodecs1-debuginfo-2.4.13-48.42.1
wireshark-2.4.13-48.42.1
libwsutil8-2.4.13-48.42.1
wireshark-gtk-debuginfo-2.4.13-48.42.1
libwsutil8-debuginfo-2.4.13-48.42.1
libwscodecs1-2.4.13-48.42.1
wireshark-gtk-2.4.13-48.42.1
libwiretap7-2.4.13-48.42.1
wireshark-debuginfo-2.4.13-48.42.1
libwireshark9-debuginfo-2.4.13-48.42.1
libwiretap7-debuginfo-2.4.13-48.42.1
libwireshark9-2.4.13-48.42.1

SuSE SLES 12 SP4
x86_64
wireshark-debugsource-2.4.13-48.42.1
libwscodecs1-debuginfo-2.4.13-48.42.1
wireshark-2.4.13-48.42.1
libwsutil8-2.4.13-48.42.1
wireshark-gtk-debuginfo-2.4.13-48.42.1
libwsutil8-debuginfo-2.4.13-48.42.1
libwscodecs1-2.4.13-48.42.1
wireshark-gtk-2.4.13-48.42.1
libwiretap7-2.4.13-48.42.1
wireshark-debuginfo-2.4.13-48.42.1
libwireshark9-debuginfo-2.4.13-48.42.1
libwiretap7-debuginfo-2.4.13-48.42.1
libwireshark9-2.4.13-48.42.1

SuSE SLES 12 SP3
x86_64
wireshark-debugsource-2.4.13-48.42.1
libwscodecs1-debuginfo-2.4.13-48.42.1
wireshark-2.4.13-48.42.1
libwsutil8-2.4.13-48.42.1
wireshark-gtk-debuginfo-2.4.13-48.42.1
libwsutil8-debuginfo-2.4.13-48.42.1
libwscodecs1-2.4.13-48.42.1
wireshark-gtk-2.4.13-48.42.1
libwiretap7-2.4.13-48.42.1
wireshark-debuginfo-2.4.13-48.42.1
libwireshark9-debuginfo-2.4.13-48.42.1
libwiretap7-debuginfo-2.4.13-48.42.1
libwireshark9-2.4.13-48.42.1

163827 - Oracle Enterprise Linux ELSA-2019-0638 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3816

Description

The scan detected that the host is missing the following update:
ELSA-2019-0638

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008600.html

OEL7
x86_64
libwsman-devel-2.6.3-6.git4391e5c.el7_6
openwsman-python-2.6.3-6.git4391e5c.el7_6
openwsman-perl-2.6.3-6.git4391e5c.el7_6
openwsman-client-2.6.3-6.git4391e5c.el7_6
libwsman1-2.6.3-6.git4391e5c.el7_6
openwsman-ruby-2.6.3-6.git4391e5c.el7_6
openwsman-server-2.6.3-6.git4391e5c.el7_6

171078 - Amazon Linux AMI ALAS-2019-1181 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux 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:
ALAS-2019-1181

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1181.html

Amazon Linux AMI
x86_64
mysql57-libs-5.7.25-1.11.amzn1
mysql57-common-5.7.25-1.11.amzn1
mysql57-server-5.7.25-1.11.amzn1
mysql57-devel-5.7.25-1.11.amzn1
mysql57-debuginfo-5.7.25-1.11.amzn1
mysql57-5.7.25-1.11.amzn1
mysql57-test-5.7.25-1.11.amzn1
mysql57-errmsg-5.7.25-1.11.amzn1
mysql57-embedded-5.7.25-1.11.amzn1
mysql57-embedded-devel-5.7.25-1.11.amzn1

i686
mysql57-libs-5.7.25-1.11.amzn1
mysql57-common-5.7.25-1.11.amzn1
mysql57-server-5.7.25-1.11.amzn1
mysql57-devel-5.7.25-1.11.amzn1
mysql57-debuginfo-5.7.25-1.11.amzn1
mysql57-embedded-5.7.25-1.11.amzn1
mysql57-test-5.7.25-1.11.amzn1
mysql57-errmsg-5.7.25-1.11.amzn1
mysql57-5.7.25-1.11.amzn1
mysql57-embedded-devel-5.7.25-1.11.amzn1

171083 - Amazon Linux AMI ALAS-2019-1178 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2455, CVE-2019-2481, CVE-2019-2482, CVE-2019-2503, CVE-2019-2507, CVE-2019-2529, CVE-2019-2531, CVE-2019-2534, CVE-2019-2537

Description

The scan detected that the host is missing the following update:
ALAS-2019-1178

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1178.html

Amazon Linux AMI
x86_64
mysql56-common-5.6.43-1.32.amzn1
mysql56-devel-5.6.43-1.32.amzn1
mysql56-embedded-devel-5.6.43-1.32.amzn1
mysql56-test-5.6.43-1.32.amzn1
mysql56-errmsg-5.6.43-1.32.amzn1
mysql56-5.6.43-1.32.amzn1
mysql56-debuginfo-5.6.43-1.32.amzn1
mysql56-libs-5.6.43-1.32.amzn1
mysql56-bench-5.6.43-1.32.amzn1
mysql56-server-5.6.43-1.32.amzn1
mysql56-embedded-5.6.43-1.32.amzn1

i686
mysql56-common-5.6.43-1.32.amzn1
mysql56-devel-5.6.43-1.32.amzn1
mysql56-test-5.6.43-1.32.amzn1
mysql56-5.6.43-1.32.amzn1
mysql56-debuginfo-5.6.43-1.32.amzn1
mysql56-errmsg-5.6.43-1.32.amzn1
mysql56-embedded-5.6.43-1.32.amzn1
mysql56-server-5.6.43-1.32.amzn1
mysql56-bench-5.6.43-1.32.amzn1
mysql56-libs-5.6.43-1.32.amzn1
mysql56-embedded-devel-5.6.43-1.32.amzn1

171085 - Amazon Linux AMI ALAS-2019-1169 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5010

Description

The scan detected that the host is missing the following update:
ALAS-2019-1169

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1169.html

Amazon Linux AMI
x86_64
python27-2.7.16-1.125.amzn1
python27-test-2.7.16-1.125.amzn1
python34-3.4.9-1.41.amzn1
python36-3.6.8-1.11.amzn1
python35-libs-3.5.6-1.14.amzn1
python36-debuginfo-3.6.8-1.11.amzn1
python34-test-3.4.9-1.41.amzn1
python34-devel-3.4.9-1.41.amzn1
python36-libs-3.6.8-1.11.amzn1
python34-tools-3.4.9-1.41.amzn1
python27-devel-2.7.16-1.125.amzn1
python35-debuginfo-3.5.6-1.14.amzn1
python36-devel-3.6.8-1.11.amzn1
python35-3.5.6-1.14.amzn1
python27-libs-2.7.16-1.125.amzn1
python34-libs-3.4.9-1.41.amzn1
python36-test-3.6.8-1.11.amzn1
python34-debuginfo-3.4.9-1.41.amzn1
python35-tools-3.5.6-1.14.amzn1
python35-test-3.5.6-1.14.amzn1
python36-debug-3.6.8-1.11.amzn1
python35-devel-3.5.6-1.14.amzn1
python27-debuginfo-2.7.16-1.125.amzn1
python36-tools-3.6.8-1.11.amzn1
python27-tools-2.7.16-1.125.amzn1

i686
python27-2.7.16-1.125.amzn1
python27-test-2.7.16-1.125.amzn1
python34-3.4.9-1.41.amzn1
python36-test-3.6.8-1.11.amzn1
python35-libs-3.5.6-1.14.amzn1
python36-debuginfo-3.6.8-1.11.amzn1
python34-test-3.4.9-1.41.amzn1
python34-devel-3.4.9-1.41.amzn1
python34-tools-3.4.9-1.41.amzn1
python27-devel-2.7.16-1.125.amzn1
python36-tools-3.6.8-1.11.amzn1
python36-devel-3.6.8-1.11.amzn1
python35-3.5.6-1.14.amzn1
python35-tools-3.5.6-1.14.amzn1
python27-libs-2.7.16-1.125.amzn1
python34-libs-3.4.9-1.41.amzn1
python34-debuginfo-3.4.9-1.41.amzn1
python35-debuginfo-3.5.6-1.14.amzn1
python35-test-3.5.6-1.14.amzn1
python36-debug-3.6.8-1.11.amzn1
python35-devel-3.5.6-1.14.amzn1
python27-debuginfo-2.7.16-1.125.amzn1
python36-libs-3.6.8-1.11.amzn1
python36-3.6.8-1.11.amzn1
python27-tools-2.7.16-1.125.amzn1

178713 - Gentoo Linux GLSA-201903-16 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-16

Observation

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

https://security.gentoo.org/glsa/201903-16

Affected packages:
net-misc/openssh < 7.9_p1-r4

194894 - Fedora Linux 29 FEDORA-2019-f528d75a69 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3498, CVE-2019-6975

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f528d75a69

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

Fedora Core 29

python2-django1.11-1.11.20-1.fc29

194898 - Fedora Linux 29 FEDORA-2019-07e8e806e0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17075, CVE-2018-17142, CVE-2018-17143, CVE-2018-17846, CVE-2018-17847, CVE-2018-17848

Description

The scan detected that the host is missing the following update:
FEDORA-2019-07e8e806e0

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/2019/3/?count=200&page=1

Fedora Core 29

golang-googlecode-net-0-0.49.20190302git16b79f2.fc29

194909 - Fedora Linux 28 FEDORA-2019-5ad2149e99 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14574, CVE-2019-3498, CVE-2019-6975

Description

The scan detected that the host is missing the following update:
FEDORA-2019-5ad2149e99

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

Fedora Core 28

python2-django1.11-1.11.20-1.fc28

194916 - Fedora Linux 28 FEDORA-2019-07d447a1d3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17075, CVE-2018-17142, CVE-2018-17143, CVE-2018-17846, CVE-2018-17847, CVE-2018-17848

Description

The scan detected that the host is missing the following update:
FEDORA-2019-07d447a1d3

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/2019/3/?count=200&page=1

Fedora Core 28

golang-googlecode-net-0-0.48.20190302git16b79f2.fc28

194920 - Fedora Linux 29 FEDORA-2019-0300c36537 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11763, CVE-2018-17189

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0300c36537

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

Fedora Core 29

mod_http2-1.14.1-1.fc29

194921 - Fedora Linux 28 FEDORA-2019-133a8a7cb5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11763, CVE-2018-17189

Description

The scan detected that the host is missing the following update:
FEDORA-2019-133a8a7cb5

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/2019/3/?count=200&page=1

Fedora Core 28

mod_http2-1.14.1-1.fc28

194924 - Fedora Linux 29 FEDORA-2019-243442e600 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5010, CVE-2019-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2019-243442e600

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/2019/3/?count=200&page=1

Fedora Core 29

python3-3.7.2-5.fc29

196277 - Red Hat Enterprise Linux RHSA-2019-0638 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3816

Description

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

RHSA-2019-0638

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00036.html

RHEL7D
x86_64
libwsman-devel-2.6.3-6.git4391e5c.el7_6
openwsman-python-2.6.3-6.git4391e5c.el7_6
openwsman-perl-2.6.3-6.git4391e5c.el7_6
openwsman-client-2.6.3-6.git4391e5c.el7_6
libwsman1-2.6.3-6.git4391e5c.el7_6
openwsman-ruby-2.6.3-6.git4391e5c.el7_6
openwsman-server-2.6.3-6.git4391e5c.el7_6
openwsman-debuginfo-2.6.3-6.git4391e5c.el7_6

RHEL7S
x86_64
libwsman-devel-2.6.3-6.git4391e5c.el7_6
openwsman-python-2.6.3-6.git4391e5c.el7_6
openwsman-perl-2.6.3-6.git4391e5c.el7_6
openwsman-client-2.6.3-6.git4391e5c.el7_6
libwsman1-2.6.3-6.git4391e5c.el7_6
openwsman-ruby-2.6.3-6.git4391e5c.el7_6
openwsman-server-2.6.3-6.git4391e5c.el7_6
openwsman-debuginfo-2.6.3-6.git4391e5c.el7_6

RHEL7WS
x86_64
libwsman-devel-2.6.3-6.git4391e5c.el7_6
openwsman-python-2.6.3-6.git4391e5c.el7_6
openwsman-perl-2.6.3-6.git4391e5c.el7_6
openwsman-client-2.6.3-6.git4391e5c.el7_6
libwsman1-2.6.3-6.git4391e5c.el7_6
openwsman-ruby-2.6.3-6.git4391e5c.el7_6
openwsman-server-2.6.3-6.git4391e5c.el7_6
openwsman-debuginfo-2.6.3-6.git4391e5c.el7_6

24856 - Joomla Browserside mime-type Sniffing Cross-Site Scripting Vulnerability (20190202)

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

Risk Level: Medium

CVE: CVE-2019-7742

Description

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

Observation

Joomla! CMS is an open source content management system.

A vulnerability is present in some versions of Joomla! CMS. The flaw lies in web server configurations. Successful exploitation could allow an attacker to affect the integrity of the target system.

24892 - Joomla XSS In Media Form Field Vulnerability (20190303)

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

Risk Level: Medium

CVE: CVE-2019-9714

Description

A cross-site scripting vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A cross-site scripting vulnerability is present in some versions of Joomla! CMS. The flaw lies in media form field. Successful exploitation could allow an attacker to affect the integrity of the target system.

24894 - Joomla XSS com_config JSON Handler Vulnerability (20190301)

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

Risk Level: Medium

CVE: CVE-2019-9712

Description

A cross-site scripting vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A cross-site scripting vulnerability is present in some versions of Joomla! CMS. The flaw is due to a lack of input validation in com_config JSON handler. Successful exploitation could allow an attacker to affect the integrity of the target system.

24896 - Joomla XSS In item_title Layout Vulnerability (20190302)

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

Risk Level: Medium

CVE: CVE-2019-9711

Description

A cross-site scripting vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A cross-site scripting vulnerability is present in some versions of Joomla! CMS. The flaw lies in item_title layout . Successful exploitation could allow an attacker to execute arbitrary script code in the browser.

131314 - Debian Linux 9.0 DSA-4410-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
DSA-4410-1

Observation

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

http://www.debian.org/security/2019/dsa-4410

Debian 9.0
all
openjdk-8-source_8u212-b01-1~deb9u1
openjdk-8-jre-headless_8u212-b01-1~deb9u1
openjdk-8-jre-zero_8u212-b01-1~deb9u1
openjdk-8-doc_8u212-b01-1~deb9u1
openjdk-8-demo_8u212-b01-1~deb9u1
openjdk-8-jre_8u212-b01-1~deb9u1
openjdk-8-jdk_8u212-b01-1~deb9u1
openjdk-8-dbg_8u212-b01-1~deb9u1
openjdk-8-jdk-headless_8u212-b01-1~deb9u1

131318 - Debian Linux 9.0 DSA-4411-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796

Description

The scan detected that the host is missing the following update:
DSA-4411-1

Observation

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

http://www.debian.org/security/2019/dsa-4411

Debian 9.0
all
firefox-esr_60.6.0esr-1~deb9u1

147733 - SuSE SLES 11 SP4 SUSE-SU-2019:13984-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18384

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13984-1

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-March/005218.html

SuSE SLES 11 SP4
i586
unzip-6.00-11.18.8.1

x86_64
unzip-6.00-11.18.8.1

160536 - CentOS 7 CESA-2019-0622 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796

Description

The scan detected that the host is missing the following update:
CESA-2019-0622

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-March/023250.html

CentOS 7
x86_64
firefox-60.6.0-3.el7.centos

i686
firefox-60.6.0-3.el7.centos

160537 - CentOS 6 CESA-2019-0623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796

Description

The scan detected that the host is missing the following update:
CESA-2019-0623

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-March/023249.html

CentOS 6
x86_64
firefox-60.6.0-3.el6.centos

i686
firefox-60.6.0-3.el6.centos

163829 - Oracle Enterprise Linux ELSA-2019-0623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796

Description

The scan detected that the host is missing the following update:
ELSA-2019-0623

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008592.html

OEL6
x86_64
firefox-60.6.0-3.0.1.el6_10

163831 - Oracle Enterprise Linux ELSA-2019-0622 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796

Description

The scan detected that the host is missing the following update:
ELSA-2019-0622

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-March/008590.html

OEL7
x86_64
firefox-60.6.0-3.0.1.el7_6

171075 - Amazon Linux AMI ALAS-2019-1177 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
ALAS-2019-1177

Observation

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

For more information see:

https://alas.aws.amazon.com/ALAS-2019-1177.html

Amazon Linux AMI
i686
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.79.amzn1
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.79.amzn1
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.79.amzn1
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.79.amzn1
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.79.amzn1

noarch
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.79.amzn1

x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.79.amzn1
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.79.amzn1
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.79.amzn1
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.79.amzn1
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.79.amzn1

171080 - Amazon Linux AMI ALAS-2019-1176 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19132

Description

The scan detected that the host is missing the following update:
ALAS-2019-1176

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1176.html

Amazon Linux AMI
x86_64
squid-migration-script-3.5.20-12.38.amzn1
squid-3.5.20-12.38.amzn1
squid-debuginfo-3.5.20-12.38.amzn1

i686
squid-migration-script-3.5.20-12.38.amzn1
squid-3.5.20-12.38.amzn1
squid-debuginfo-3.5.20-12.38.amzn1

171082 - Amazon Linux AMI ALAS-2019-1153 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-0734

Description

The scan detected that the host is missing the following update:
ALAS-2019-1153

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1153.html

Amazon Linux AMI
x86_64
openssl-1.0.2k-16.148.amzn1
openssl-devel-1.0.2k-16.148.amzn1
openssl-perl-1.0.2k-16.148.amzn1
openssl-debuginfo-1.0.2k-16.148.amzn1
openssl-static-1.0.2k-16.148.amzn1

i686
openssl-devel-1.0.2k-16.148.amzn1
openssl-1.0.2k-16.148.amzn1
openssl-perl-1.0.2k-16.148.amzn1
openssl-debuginfo-1.0.2k-16.148.amzn1
openssl-static-1.0.2k-16.148.amzn1

186621 - Ubuntu Linux 18.10 USN-3916-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20532, CVE-2018-20533, CVE-2018-20534

Description

The scan detected that the host is missing the following update:
USN-3916-1

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-March/004813.html

Ubuntu 18.10

libsolv-tools_0.6.35-2ubuntu0.18.10.1
libsolv0_0.6.35-2ubuntu0.18.10.1
libsolvext0_0.6.35-2ubuntu0.18.10.1

194905 - Fedora Linux 29 FEDORA-2019-2c020ccbd5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18409

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2c020ccbd5

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

Fedora Core 29

tcpflow-1.5.0-4.fc29

194910 - Fedora Linux 28 FEDORA-2019-8cdd669aca Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18409

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8cdd669aca

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

Fedora Core 28

tcpflow-1.5.0-4.fc28

196275 - Red Hat Enterprise Linux RHSA-2019-0623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796

Description

The scan detected that the host is missing the following update:
RHSA-2019-0623

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00033.html

RHEL6D
x86_64
firefox-60.6.0-3.el6_10
firefox-debuginfo-60.6.0-3.el6_10

i386
firefox-60.6.0-3.el6_10
firefox-debuginfo-60.6.0-3.el6_10

RHEL6S
i386
firefox-60.6.0-3.el6_10
firefox-debuginfo-60.6.0-3.el6_10

x86_64
firefox-60.6.0-3.el6_10
firefox-debuginfo-60.6.0-3.el6_10

RHEL6WS
x86_64
firefox-60.6.0-3.el6_10
firefox-debuginfo-60.6.0-3.el6_10

i386
firefox-60.6.0-3.el6_10
firefox-debuginfo-60.6.0-3.el6_10

196276 - Red Hat Enterprise Linux RHSA-2019-0622 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796

Description

The scan detected that the host is missing the following update:
RHSA-2019-0622

Observation

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

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

RHEL7D
x86_64
firefox-debuginfo-60.6.0-3.el7_6
firefox-60.6.0-3.el7_6

RHEL7S
x86_64
firefox-debuginfo-60.6.0-3.el7_6
firefox-60.6.0-3.el7_6

RHEL7WS
x86_64
firefox-debuginfo-60.6.0-3.el7_6
firefox-60.6.0-3.el7_6

24909 - (K31424926) F5 BIG-IP APM XSS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2019-6595

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in BIG-IP APM Admin Web UI. Successful exploitation could allow an attacker to remotely inject arbitrary code on the target system.

89011 - Slackware Linux 14.2 SSA:2019-084-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2019-084-01

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.365256

Slackware 14.2
x86_64
mozilla-thunderbird-60.6.1-x86_64-1

i686
mozilla-thunderbird-60.6.1-i686-1

89012 - Slackware Linux 14.2 SSA:2019-081-01 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
SSA:2019-081-01

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.386904

Slackware 14.2
x86_64
mozilla-firefox-60.6.1esr-x86_64-1

i686
mozilla-firefox-60.6.1esr-i686-1

131315 - Debian Linux 9.0 DSA-4412-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6341

Description

The scan detected that the host is missing the following update:
DSA-4412-1

Observation

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

http://www.debian.org/security/2019/dsa-4412

Debian 9.0
all
drupal7_7.52-2+deb9u7

131316 - Debian Linux 9.0 DSA-4414-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
DSA-4414-1

Observation

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

http://www.debian.org/security/2019/dsa-4414

Debian 9.0
all
libapache2-mod-auth-mellon_0.12.0-2+deb9u1

131319 - Debian Linux 9.0 DSA-4413-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9755

Description

The scan detected that the host is missing the following update:
DSA-4413-1

Observation

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

http://www.debian.org/security/2019/dsa-4413

Debian 9.0
all
ntfs-3g_1:2016.2.22AR.1+dfsg-1+deb9u1

131321 - Debian Linux 9.0 DSA-4417-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
DSA-4417-1

Observation

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

http://www.debian.org/security/2019/dsa-4417

Debian 9.0
all
firefox-esr_60.6.1esr-1~deb9u1

182937 - FreeBSD Python NULL Pointer Dereference Vulnerability (d74371d2-4fee-11e9-a5cd-1df8a848de3d)

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

Risk Level: Low

CVE: CVE-2019-5010

Description

The scan detected that the host is missing the following update:
Python -- NULL pointer dereference vulnerability (d74371d2-4fee-11e9-a5cd-1df8a848de3d)

Observation

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

http://www.vuxml.org/freebsd/d74371d2-4fee-11e9-a5cd-1df8a848de3d.html

Affected packages:
python37 < 3.7.3

182939 - FreeBSD wordpress Multiple Issues (15ee0e93-4bbb-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:
wordpress -- multiple issues (15ee0e93-4bbb-11e9-9ba0-4c72b94353b5)

Observation

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

http://www.vuxml.org/freebsd/15ee0e93-4bbb-11e9-9ba0-4c72b94353b5.html

Affected packages:
wordpress < 5.1.1,1
fr-wordpress < 5.1.1,1
de-wordpress < 5.1.1
zh_CN-wordpress < 5.1.1
zh_TW-wordpress < 5.1.1
ja-wordpress < 5.1.1
ru-wordpress < 5.1.1

182940 - FreeBSD Gitlab Vulnerability (7ba5a3d0-4b18-11e9-adcb-001b217b3468)

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

Risk Level: Low

CVE: CVE-2019-9732

Description

The scan detected that the host is missing the following update:
Gitlab -- Vulnerability (7ba5a3d0-4b18-11e9-adcb-001b217b3468)

Observation

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

http://www.vuxml.org/freebsd/7ba5a3d0-4b18-11e9-adcb-001b217b3468.html

Affected packages:
gitlab-ce < 11.8.2

182941 - FreeBSD gitea XSS Vulnerability (a8ba7358-4b02-11e9-9ba0-4c72b94353b5)

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 -- XSS vulnerability (a8ba7358-4b02-11e9-9ba0-4c72b94353b5)

Observation

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

http://www.vuxml.org/freebsd/a8ba7358-4b02-11e9-9ba0-4c72b94353b5.html

Affected packages:
gitea < 1.7.4

182942 - FreeBSD Gitlab Vulnerability (e0382fde-4bb0-11e9-adcb-001b217b3468)

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

Risk Level: Low

CVE: CVE-2019-9866

Description

The scan detected that the host is missing the following update:
Gitlab -- Vulnerability (e0382fde-4bb0-11e9-adcb-001b217b3468)

Observation

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

http://www.vuxml.org/freebsd/e0382fde-4bb0-11e9-adcb-001b217b3468.html

Affected packages:
11.8.0 <= gitlab-ce < 11.8.3
gitlab-ce < 11.7.7

186614 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3917-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7303

Description

The scan detected that the host is missing the following update:
USN-3917-1

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-March/004812.html

Ubuntu 16.04

snapd_2.37.4ubuntu0.1

Ubuntu 18.10

snapd_2.37.4+18.10.1

Ubuntu 14.04

snapd_2.37.4~14.04.1

Ubuntu 18.04

snapd_2.37.4+18.04.1

186615 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3915-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
USN-3915-1

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-March/004809.html

Ubuntu 16.04

libgs9_9.26~dfsg+0-0ubuntu0.16.04.8
ghostscript_9.26~dfsg+0-0ubuntu0.16.04.8

Ubuntu 18.10

ghostscript_9.26~dfsg+0-0ubuntu0.18.10.8
libgs9_9.26~dfsg+0-0ubuntu0.18.10.8

Ubuntu 14.04

libgs9_9.26~dfsg+0-0ubuntu0.14.04.8
ghostscript_9.26~dfsg+0-0ubuntu0.14.04.8

Ubuntu 18.04

ghostscript_9.26~dfsg+0-0ubuntu0.18.04.8
libgs9_9.26~dfsg+0-0ubuntu0.18.04.8

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

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

Risk Level: Low

CVE: CVE-2019-9628

Description

The scan detected that the host is missing the following update:
USN-3921-1

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-March/004816.html

Ubuntu 16.04

libxmltooling6v5_1.5.6-2ubuntu0.3

Ubuntu 18.10

libxmltooling8_3.0.2-1ubuntu1.1

Ubuntu 14.04

libxmltooling6_1.5.3-2+deb8u3ubuntu0.1

Ubuntu 18.04

libxmltooling7_1.6.4-1ubuntu2.1

194891 - Fedora Linux 30 FEDORA-2019-2e62c6961a 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-2019-2e62c6961a

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/2019/3/?count=200&page=1

Fedora Core 30

firefox-66.0.1-1.fc30

194896 - Fedora Linux 29 FEDORA-2019-a9a37fed18 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-a9a37fed18

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/2019/3/?count=200&page=1

Fedora Core 29

php-twig2-2.7.2-1.fc29

194899 - Fedora Linux 28 FEDORA-2019-0b73bd3e5d 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-2019-0b73bd3e5d

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

Fedora Core 28

libzip-1.5.2-1.fc28

194900 - Fedora Linux 29 FEDORA-2019-bf68d77a2c 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-bf68d77a2c

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/2019/3/?count=200&page=1

Fedora Core 29

wordpress-5.1.1-1.fc29

194901 - Fedora Linux 29 FEDORA-2019-10812c1db6 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-2019-10812c1db6

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/2019/3/?count=200&page=1

Fedora Core 29

filezilla-3.41.2-1.fc29

194902 - Fedora Linux 29 FEDORA-2019-39213e0232 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-2019-39213e0232

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/2019/3/?count=200&page=1

Fedora Core 29

thunderbird-60.6.0-1.fc29

194907 - Fedora Linux 28 FEDORA-2019-e86155be6e 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-e86155be6e

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/2019/3/?count=200&page=1

Fedora Core 28

php-twig2-2.7.2-1.fc28

194912 - Fedora Linux 29 FEDORA-2019-615e060d4e 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-2019-615e060d4e

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

Fedora Core 29

libzip-1.5.2-1.fc29

194915 - Fedora Linux 29 FEDORA-2019-c8712a42dc 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-c8712a42dc

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/2019/3/?count=200&page=1

Fedora Core 29

php-twig-1.38.2-2.fc29

194917 - Fedora Linux 29 FEDORA-2019-e96019b473 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-e96019b473

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

Fedora Core 29

firefox-66.0-6.fc29

194919 - Fedora Linux 28 FEDORA-2019-64f6c399c9 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-2019-64f6c399c9

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/2019/3/?count=200&page=1

Fedora Core 28

php-twig-1.38.2-2.fc28

131320 - Debian Linux 9.0 DSA-4415-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16355

Description

The scan detected that the host is missing the following update:
DSA-4415-1

Observation

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

http://www.debian.org/security/2019/dsa-4415

Debian 9.0
all
passenger_5.0.30-1+deb9u1

171081 - Amazon Linux AMI ALAS-2019-1182 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6260

Description

The scan detected that the host is missing the following update:
ALAS-2019-1182

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1182.html

Amazon Linux AMI
x86_64
nvidia-dkms-410.104-2018.03.111.amzn1
nvidia-410.104-2018.03.111.amzn1

182938 - FreeBSD libXdmcp Insufficient Entropy Generating Session Keys (1b6a10e9-4b7b-11e9-9e89-54e1ad3d6335)

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

Risk Level: Low

CVE: CVE-2017-2625

Description

The scan detected that the host is missing the following update:
libXdmcp -- insufficient entropy generating session keys (1b6a10e9-4b7b-11e9-9e89-54e1ad3d6335)

Observation

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

http://www.vuxml.org/freebsd/1b6a10e9-4b7b-11e9-9e89-54e1ad3d6335.html

Affected packages:
libXdmcp < 1.1.3

194904 - Fedora Linux 29 FEDORA-2019-7104a00054 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9704, CVE-2019-9705

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7104a00054

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

Fedora Core 29

cronie-1.5.4-1.fc29

24902 - Microsoft Office 365 ProPlus and Office 2019 Mar 2019 Updates

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

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

Observation

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

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

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.

89010 - Slackware Linux 14.2 SSA:2019-077-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Update Details

Risk is updated

147723 - SuSE SLES 11 SP4 SUSE-SU-2019:13982-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Update Details

Risk is updated

194731 - Fedora Linux 29 FEDORA-2019-d8ec88b21e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3808, CVE-2019-3809, CVE-2019-3810

Update Details

Risk is updated

194733 - Fedora Linux 28 FEDORA-2019-077cd6f168 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3808, CVE-2019-3809, CVE-2019-3810

Update Details

Risk is updated

18988 - Moxa SoftCMS Buffer Overflow Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2015-6457, CVE-2015-6458

Update Details

Risk is updated

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

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-6116

Update Details
Risk is updated

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: Medium
CVE: CVE-2019-6116

Update Details
Risk is updated

147593 - SuSE Linux 42.3 openSUSE-SU-2019:0103-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-6116

Update Details
Risk is updated

147598 - SuSE Linux 15.0 openSUSE-SU-2019:0104-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-6116

Update Details
Risk is updated

182932 - FreeBSD PowerDNS Insufficient Validation In The HTTP Remote Backend (6001cfc6-9f0f-4fae-9b4f-9b8fae001425)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-3871

Update Details
Risk is updated

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: Medium
CVE: CVE-2019-6116

Update Details
Risk is updated

22305 - (K57211290) F5 BIG-IP IPv6 Fragmentation Vulnerability

Category: SSH Module -> NonIntrusive -> F5
Risk Level: Medium
CVE: CVE-2016-10142

Update Details
FASLScript is updated

24422 - IBM AIX FreeBSD Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-6922

Update Details
FASLScript is updated

147634 - SuSE Linux 15.0 openSUSE-SU-2019:0166-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-20615

Update Details
Risk is updated

182884 - FreeBSD py-matrix-synapse Undisclosed Vulnerability (383931ba-1818-11e9-92ea-448a5b29e8a9)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-5885

Update Details
Risk is updated

182886 - FreeBSD Gitlab Arbitrary Repo Read In Gitlab Project Import (ff50192c-19eb-11e9-8573-001b217b3468)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-6240

Update Details
Risk is updated

182901 - FreeBSD p5-Email-Address-List DDoS Related Vulnerability (22b90fe6-258e-11e9-9c8d-6805ca0b3d42)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18898

Update Details

Risk is updated

194706 - Fedora Linux 29 FEDORA-2019-4d914f9257 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5885

Update Details

Risk is updated

194770 - Fedora Linux 29 FEDORA-2019-73cbc02e14 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18898

Update Details

Risk is updated

194780 - Fedora Linux 28 FEDORA-2019-ef5551fcff Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18898

Update Details

Risk is updated

196242 - Red Hat Enterprise Linux RHSA-2019-0275 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20615

Update Details

Risk is updated

70029 - db2.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70048 - adobe.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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