2018-FEB-15
FSL version 7.6.4

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

146364 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0383-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0383-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003711.html

SuSE SLED 12 SP3
x86_64
kernel-default-4.4.114-94.11.3
kernel-default-devel-4.4.114-94.11.3
kernel-syms-4.4.114-94.11.2
kernel-default-debuginfo-4.4.114-94.11.3
kernel-default-extra-debuginfo-4.4.114-94.11.3
kernel-default-extra-4.4.114-94.11.3
kernel-default-debugsource-4.4.114-94.11.3

noarch
kernel-source-4.4.114-94.11.2
kernel-devel-4.4.114-94.11.2
kernel-macros-4.4.114-94.11.2

SuSE SLES 12 SP3
noarch
kernel-source-4.4.114-94.11.2
kernel-devel-4.4.114-94.11.2
kernel-macros-4.4.114-94.11.2

x86_64
kernel-default-4.4.114-94.11.3
kernel-default-devel-4.4.114-94.11.3
kernel-syms-4.4.114-94.11.2
kernel-default-base-4.4.114-94.11.3
kernel-default-base-debuginfo-4.4.114-94.11.3
kernel-default-debuginfo-4.4.114-94.11.3
kernel-default-debugsource-4.4.114-94.11.3

146377 - SuSE Linux 42.3 openSUSE-SU-2018:0408-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0408-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00035.html

SuSE Linux 42.3
x86_64
kernel-default-devel-4.4.114-42.1
kernel-debug-devel-4.4.114-42.1
kernel-debug-debuginfo-4.4.114-42.1
kernel-vanilla-devel-4.4.114-42.1
kernel-vanilla-debuginfo-4.4.114-42.1
kernel-vanilla-debugsource-4.4.114-42.1
kselftests-kmp-default-4.4.114-42.1
kselftests-kmp-vanilla-debuginfo-4.4.114-42.1
kernel-vanilla-4.4.114-42.1
kernel-debug-base-4.4.114-42.1
kselftests-kmp-debug-4.4.114-42.1
kernel-default-debugsource-4.4.114-42.1
kernel-vanilla-base-debuginfo-4.4.114-42.1
kernel-obs-qa-4.4.114-42.1
kernel-default-4.4.114-42.1
kernel-default-base-4.4.114-42.1
kernel-debug-debugsource-4.4.114-42.1
kernel-obs-build-4.4.114-42.1
kselftests-kmp-vanilla-4.4.114-42.1
kernel-debug-4.4.114-42.1
kernel-default-debuginfo-4.4.114-42.1
kernel-obs-build-debugsource-4.4.114-42.1
kernel-debug-base-debuginfo-4.4.114-42.1
kernel-vanilla-base-4.4.114-42.1
kselftests-kmp-debug-debuginfo-4.4.114-42.1
kernel-debug-devel-debuginfo-4.4.114-42.1
kernel-syms-4.4.114-42.1
kselftests-kmp-default-debuginfo-4.4.114-42.1
kernel-default-base-debuginfo-4.4.114-42.1

noarch
kernel-docs-html-4.4.114-42.1
kernel-docs-4.4.114-42.1
kernel-devel-4.4.114-42.1
kernel-macros-4.4.114-42.1
kernel-source-vanilla-4.4.114-42.1
kernel-source-4.4.114-42.1
kernel-docs-pdf-4.4.114-42.1

146379 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0416-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0416-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003721.html

SuSE SLED 12 SP2
x86_64
kernel-default-devel-4.4.114-92.64.1
kernel-default-extra-4.4.114-92.64.1
kernel-default-extra-debuginfo-4.4.114-92.64.1
kernel-syms-4.4.114-92.64.1
kernel-default-4.4.114-92.64.1
kernel-default-debuginfo-4.4.114-92.64.1
kernel-default-debugsource-4.4.114-92.64.1

noarch
kernel-devel-4.4.114-92.64.1
kernel-source-4.4.114-92.64.1
kernel-macros-4.4.114-92.64.1

SuSE SLES 12 SP2
noarch
kernel-devel-4.4.114-92.64.1
kernel-source-4.4.114-92.64.1
kernel-macros-4.4.114-92.64.1

x86_64
kernel-default-devel-4.4.114-92.64.1
kernel-default-debugsource-4.4.114-92.64.1
kernel-syms-4.4.114-92.64.1
kernel-default-4.4.114-92.64.1
kernel-default-base-4.4.114-92.64.1
kernel-default-debuginfo-4.4.114-92.64.1
kernel-default-base-debuginfo-4.4.114-92.64.1

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

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

Risk Level: High

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

Description

Multiple vulnerabilities are present in some versions of Apple macOS.

Observation

Apple macOS is the operating system developed by Apple.

Multiple vulnerabilities are present in some versions of Apple macOS. The flaws lie in several components. Successful exploitation could allow an attacker to retrieve sensitive data, escalate privileges, cause a denial of service condition or remotely execute arbitrary code on the target system.

23077 - Cisco ASA Software Remote Code Execution and Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-0101

Description

A vulnerability is present in some versions of Cisco Adaptive Security Appliance (ASA).

Observation

Cisco Adaptive Security Appliance is a firewall device.

A vulnerability is present in some versions of Cisco Adaptive Security Appliance (ASA). The flaw lies in the XML parser. Successful exploitation could allow an attacker to cause a denial of service condition or execute arbitrary code.

23135 - Microsoft Office 2016 Click-To-Run February 2018 Updates

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

Risk Level: High

CVE: CVE-2018-0841, CVE-2018-0850, CVE-2018-0851, CVE-2018-0852, CVE-2018-0853

Description

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run.

Observation

Microsoft Office 2016 Click-to-Run is an alternative to the Windows Installer-based (MSI) installation method of the popular office suite.

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run. 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.

141869 - Red Hat Enterprise Linux RHSA-2018-0285 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-4877, CVE-2018-4878

Description

The scan detected that the host is missing the following update:
RHSA-2018-0285

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-February/msg00009.html

RHEL6D
x86_64
flash-plugin-28.0.0.161-1.el6_9

i386
flash-plugin-28.0.0.161-1.el6_9

RHEL6S
x86_64
flash-plugin-28.0.0.161-1.el6_9

i386
flash-plugin-28.0.0.161-1.el6_9

RHEL6WS
x86_64
flash-plugin-28.0.0.161-1.el6_9

i386
flash-plugin-28.0.0.161-1.el6_9

23057 - (K24465120) F5 BIG-IP iControl REST Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6167

Description

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

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in iControl REST component. Successful exploitation could allow an attacker to gain elevated privileges on the target system.
.

23050 - Oracle Secure Global Desktop (SGD) Critical Patch Update January 2018

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-3736, CVE-2017-5645

Description

Multiple vulnerabilities are present in some versions of Oracle Secure Global Desktop.

Observation

Oracle Secure Global Desktop is a secure remote access solution.

Multiple vulnerabilities are present in some versions of Oracle Secure Global Desktop. The flaws lie in the core component. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability.

23052 - (K25033460) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6133

Description

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

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

A denial-of-service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in TMM URI parser library. Successful exploitation could allow a remote attacker to cause a denial of service condition.

23123 - Apache Tomcat Vulnerability Prior To 7.0.84

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

Risk Level: High

CVE: CVE-2017-15706

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

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

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

23125 - Joomla XSS Vulnerability (20180101)

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

Risk Level: High

CVE: CVE-2018-6380

Description

An XSS vulnerability is present in some versions of Joomla!.

Observation

Joomla! is an open source content management system.

An XSS vulnerability is present in some versions of Joomla!. The flaw is due to a lack of module chrome's escaping. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

132436 - Oracle VM OVMSA-2018-0017 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0861, CVE-2017-12193, CVE-2017-14140, CVE-2017-15115, CVE-2017-17712, CVE-2017-5754, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0017

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-February/000828.html

OVM3.4
x86_64
kernel-uek-4.1.12-112.14.14.el6uek
kernel-uek-firmware-4.1.12-112.14.14.el6uek

146352 - SuSE SLES 11 SP4 SUSE-SU-2018:0423-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10396

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0423-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003723.html

SuSE SLES 11 SP4
i586
ipsec-tools-0.7.3-1.38.3.1

x86_64
ipsec-tools-0.7.3-1.38.3.1

146354 - SuSE Linux 42.3 openSUSE-SU-2018:0389-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9780, CVE-2018-6560

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0389-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00019.html

SuSE Linux 42.3

x86_64
flatpak-debuginfo-0.8.9-3.1
typelib-1_0-Flatpak-1_0-0.8.9-3.1
flatpak-devel-0.8.9-3.1
flatpak-debugsource-0.8.9-3.1
libflatpak0-0.8.9-3.1
flatpak-builder-debuginfo-0.8.9-3.1
flatpak-0.8.9-3.1
libflatpak0-debuginfo-0.8.9-3.1
flatpak-builder-0.8.9-3.1

146355 - SuSE Linux 42.3 openSUSE-SU-2018:0429-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3836

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0429-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00040.html

SuSE Linux 42.3
x86_64
leptonica-tools-1.72-6.1
liblept4-1.72-6.1
liblept4-debuginfo-1.72-6.1
liblept4-32bit-1.72-6.1
leptonica-debugsource-1.72-6.1
leptonica-devel-1.72-6.1
leptonica-tools-debuginfo-1.72-6.1
liblept4-debuginfo-32bit-1.72-6.1

i586
leptonica-tools-1.72-6.1
liblept4-1.72-6.1
liblept4-debuginfo-1.72-6.1
leptonica-debugsource-1.72-6.1
leptonica-devel-1.72-6.1
leptonica-tools-debuginfo-1.72-6.1

146356 - SuSE SLES 11 SP4 SUSE-SU-2018:0409-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0409-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003718.html

SuSE SLES 11 SP4
i586
libdb-4_5-4.5.20-97.5
db-doc-4.5.20-97.5
db-utils-4.5.20-97.5
db-utils-doc-4.5.20-97.5

x86_64
libdb-4_5-4.5.20-97.5
db-doc-4.5.20-97.5
db-utils-4.5.20-97.5
libdb-4_5-32bit-4.5.20-97.5
db-utils-doc-4.5.20-97.5

146362 - SuSE Linux 42.3 openSUSE-SU-2018:0434-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10396

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0434-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00041.html

SuSE Linux 42.3
x86_64
ipsec-tools-0.8.0-14.3.1
ipsec-tools-debugsource-0.8.0-14.3.1
ipsec-tools-debuginfo-0.8.0-14.3.1

i586
ipsec-tools-0.8.0-14.3.1
ipsec-tools-debugsource-0.8.0-14.3.1
ipsec-tools-debuginfo-0.8.0-14.3.1

146366 - SuSE Linux 42.3 openSUSE-SU-2018:0419-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6612

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0419-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00037.html

SuSE Linux 42.3
x86_64
jhead-debugsource-3.00-8.1
jhead-debuginfo-3.00-8.1
jhead-3.00-8.1

i586
jhead-debugsource-3.00-8.1
jhead-debuginfo-3.00-8.1
jhead-3.00-8.1

146367 - SuSE SLED 12 SP2 SUSE-SU-2018:0428-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6871

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0428-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003725.html

SuSE SLED 12 SP2
x86_64
libreofficekit-5.4.5.1-40.24.1
libreoffice-5.4.5.1-40.24.1
libreoffice-officebean-debuginfo-5.4.5.1-40.24.1
libreoffice-base-debuginfo-5.4.5.1-40.24.1
libreoffice-draw-5.4.5.1-40.24.1
libreoffice-filters-optional-5.4.5.1-40.24.1
libreoffice-writer-debuginfo-5.4.5.1-40.24.1
libreoffice-pyuno-debuginfo-5.4.5.1-40.24.1
libreoffice-draw-debuginfo-5.4.5.1-40.24.1
libreoffice-base-drivers-mysql-5.4.5.1-40.24.1
libreoffice-impress-debuginfo-5.4.5.1-40.24.1
libreoffice-debugsource-5.4.5.1-40.24.1
libreoffice-gnome-debuginfo-5.4.5.1-40.24.1
libreoffice-base-drivers-mysql-debuginfo-5.4.5.1-40.24.1
libreoffice-base-5.4.5.1-40.24.1
libreoffice-impress-5.4.5.1-40.24.1
libreoffice-debuginfo-5.4.5.1-40.24.1
libreoffice-officebean-5.4.5.1-40.24.1
libreoffice-base-drivers-postgresql-debuginfo-5.4.5.1-40.24.1
libreoffice-gnome-5.4.5.1-40.24.1
libreoffice-calc-debuginfo-5.4.5.1-40.24.1
libreoffice-calc-extensions-5.4.5.1-40.24.1

libreoffice-math-5.4.5.1-40.24.1
libreoffice-mailmerge-5.4.5.1-40.24.1
libreoffice-writer-5.4.5.1-40.24.1
libreoffice-calc-5.4.5.1-40.24.1
libreoffice-writer-extensions-5.4.5.1-40.24.1
libreoffice-pyuno-5.4.5.1-40.24.1
libreoffice-math-debuginfo-5.4.5.1-40.24.1
libreoffice-base-drivers-postgresql-5.4.5.1-40.24.1

noarch
libreoffice-l10n-zu-5.4.5.1-40.24.1
libreoffice-l10n-cs-5.4.5.1-40.24.1
libreoffice-l10n-nl-5.4.5.1-40.24.1
libreoffice-l10n-pt_BR-5.4.5.1-40.24.1
libreoffice-l10n-zh_TW-5.4.5.1-40.24.1
libreoffice-l10n-hu-5.4.5.1-40.24.1
libreoffice-l10n-bg-5.4.5.1-40.24.1
libreoffice-l10n-zh_CN-5.4.5.1-40.24.1
libreoffice-l10n-pt_PT-5.4.5.1-40.24.1
libreoffice-l10n-fr-5.4.5.1-40.24.1
libreoffice-l10n-hr-5.4.5.1-40.24.1
libreoffice-l10n-af-5.4.5.1-40.24.1
libreoffice-l10n-es-5.4.5.1-40.24.1
libreoffice-l10n-gu-5.4.5.1-40.24.1
libreoffice-icon-theme-tango-5.4.5.1-40.24.1
libreoffice-l10n-uk-5.4.5.1-40.24.1
libreoffice-icon-theme-galaxy-5.4.5.1-40.24.1
libreoffice-l10n-sk-5.4.5.1-40.24.1
libreoffice-l10n-xh-5.4.5.1-40.24.1
libreoffice-l10n-en-5.4.5.1-40.24.1
libreoffice-l10n-pl-5.4.5.1-40.24.1
libreoffice-l10n-nb-5.4.5.1-40.24.1
libreoffice-l10n-lt-5.4.5.1-40.24.1
libreoffice-l10n-sv-5.4.5.1-40.24.1
libreoffice-l10n-ar-5.4.5.1-40.24.1
libreoffice-l10n-ro-5.4.5.1-40.24.1
libreoffice-l10n-de-5.4.5.1-40.24.1
libreoffice-l10n-ca-5.4.5.1-40.24.1
libreoffice-l10n-fi-5.4.5.1-40.24.1
libreoffice-l10n-hi-5.4.5.1-40.24.1
libreoffice-l10n-nn-5.4.5.1-40.24.1
libreoffice-l10n-ko-5.4.5.1-40.24.1
libreoffice-l10n-da-5.4.5.1-40.24.1
libreoffice-l10n-ja-5.4.5.1-40.24.1
libreoffice-l10n-it-5.4.5.1-40.24.1
libreoffice-l10n-ru-5.4.5.1-40.24.1

146368 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0414-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10244, CVE-2017-7864, CVE-2017-8105, CVE-2017-8287

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0414-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003720.html

SuSE SLES 12 SP2
x86_64
libfreetype6-debuginfo-2.6.3-7.15.1
libfreetype6-32bit-2.6.3-7.15.1
ft2demos-2.6.3-7.15.1
libfreetype6-debuginfo-32bit-2.6.3-7.15.1
freetype2-debugsource-2.6.3-7.15.1
libfreetype6-2.6.3-7.15.1

SuSE SLED 12 SP3
x86_64
libfreetype6-debuginfo-2.6.3-7.15.1
libfreetype6-32bit-2.6.3-7.15.1
ft2demos-2.6.3-7.15.1
libfreetype6-debuginfo-32bit-2.6.3-7.15.1
freetype2-debugsource-2.6.3-7.15.1
libfreetype6-2.6.3-7.15.1

SuSE SLED 12 SP2
x86_64
libfreetype6-debuginfo-2.6.3-7.15.1
libfreetype6-32bit-2.6.3-7.15.1
ft2demos-2.6.3-7.15.1
libfreetype6-debuginfo-32bit-2.6.3-7.15.1
freetype2-debugsource-2.6.3-7.15.1
libfreetype6-2.6.3-7.15.1

SuSE SLES 12 SP3
x86_64
libfreetype6-debuginfo-2.6.3-7.15.1
libfreetype6-32bit-2.6.3-7.15.1
ft2demos-2.6.3-7.15.1
libfreetype6-debuginfo-32bit-2.6.3-7.15.1
freetype2-debugsource-2.6.3-7.15.1
libfreetype6-2.6.3-7.15.1

146371 - SuSE Linux 42.3 openSUSE-SU-2018:0396-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10995, CVE-2017-11505, CVE-2017-11525, CVE-2017-11526, CVE-2017-11539, CVE-2017-11639, CVE-2017-11750, CVE-2017-12565, CVE-2017-12640, CVE-2017-12641, CVE-2017-12643, CVE-2017-12671, CVE-2017-12673, CVE-2017-12676, CVE-2017-12935, CVE-2017-13059, CVE-2017-13141, CVE-2017-13142, CVE-2017-13147, CVE-2017-14103, CVE-2017-14649, CVE-2017-15218, CVE-2017-17504, CVE-2017-17681, CVE-2017-17879, CVE-2017-17884, CVE-2017-17914, CVE-2017-18008, CVE-2017-18027, CVE-2017-18029, CVE-2017-9261, CVE-2017-9262, CVE-2018-5246, CVE-2018-5685

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0396-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00025.html

SuSE Linux 42.3
i586
libMagickWand-6_Q16-1-6.8.8.1-52.1
libMagick++-6_Q16-3-6.8.8.1-52.1
ImageMagick-debuginfo-6.8.8.1-52.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-52.1
ImageMagick-extra-6.8.8.1-52.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-52.1
perl-PerlMagick-6.8.8.1-52.1
ImageMagick-6.8.8.1-52.1
perl-PerlMagick-debuginfo-6.8.8.1-52.1
ImageMagick-debugsource-6.8.8.1-52.1
libMagick++-devel-6.8.8.1-52.1
libMagickCore-6_Q16-1-6.8.8.1-52.1
ImageMagick-devel-6.8.8.1-52.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-52.1
ImageMagick-extra-debuginfo-6.8.8.1-52.1

noarch
ImageMagick-doc-6.8.8.1-52.1

x86_64
libMagickWand-6_Q16-1-6.8.8.1-52.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-52.1
libMagick++-6_Q16-3-6.8.8.1-52.1
libMagick++-6_Q16-3-32bit-6.8.8.1-52.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-52.1
ImageMagick-debuginfo-6.8.8.1-52.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-52.1
libMagick++-devel-32bit-6.8.8.1-52.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-52.1
ImageMagick-extra-6.8.8.1-52.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-52.1
perl-PerlMagick-6.8.8.1-52.1
ImageMagick-6.8.8.1-52.1
perl-PerlMagick-debuginfo-6.8.8.1-52.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-52.1
ImageMagick-devel-32bit-6.8.8.1-52.1
ImageMagick-debugsource-6.8.8.1-52.1
libMagick++-devel-6.8.8.1-52.1
libMagickCore-6_Q16-1-6.8.8.1-52.1
ImageMagick-devel-6.8.8.1-52.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-52.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-52.1
ImageMagick-extra-debuginfo-6.8.8.1-52.1

146375 - SuSE Linux 42.3 openSUSE-SU-2018:0420-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10244, CVE-2017-7864, CVE-2017-8105, CVE-2017-8287

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0420-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00038.html

SuSE Linux 42.3
x86_64
freetype2-devel-2.6.3-5.3.1
libfreetype6-debuginfo-2.6.3-5.3.1
libfreetype6-debuginfo-32bit-2.6.3-5.3.1
libfreetype6-32bit-2.6.3-5.3.1
freetype2-devel-32bit-2.6.3-5.3.1
freetype2-debugsource-2.6.3-5.3.1
ft2demos-2.6.3-5.3.1
libfreetype6-2.6.3-5.3.1

i586
freetype2-debugsource-2.6.3-5.3.1
libfreetype6-debuginfo-2.6.3-5.3.1
libfreetype6-2.6.3-5.3.1
ft2demos-2.6.3-5.3.1
freetype2-devel-2.6.3-5.3.1

146376 - SuSE Linux 42.3 openSUSE-SU-2018:0394-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10711

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0394-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00024.html

SuSE Linux 42.3
x86_64
pound-doc-2.7-8.1
pound-debugsource-2.7-8.1
pound-debuginfo-2.7-8.1
pound-2.7-8.1

i586
pound-doc-2.7-8.1
pound-debugsource-2.7-8.1
pound-debuginfo-2.7-8.1
pound-2.7-8.1

146378 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2018:0424-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10396

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0424-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003724.html

SuSE SLES 12 SP3
x86_64
ipsec-tools-0.8.0-19.3.1
ipsec-tools-debuginfo-0.8.0-19.3.1
ipsec-tools-debugsource-0.8.0-19.3.1

SuSE SLES 12 SP2
x86_64
ipsec-tools-0.8.0-19.3.1
ipsec-tools-debuginfo-0.8.0-19.3.1
ipsec-tools-debugsource-0.8.0-19.3.1

146380 - SuSE Linux 42.3 openSUSE-SU-2018:0397-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0397-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00026.html

SuSE Linux 42.3
x86_64
plasma5-workspace-devel-5.8.7-11.1
plasma5-workspace-libs-5.8.7-11.1
plasma5-workspace-debugsource-5.8.7-11.1
plasma5-workspace-libs-debuginfo-5.8.7-11.1
drkonqi5-5.8.7-11.1
plasma5-workspace-5.8.7-11.1
drkonqi5-debuginfo-5.8.7-11.1
plasma5-workspace-debuginfo-5.8.7-11.1

noarch
plasma5-workspace-lang-5.8.7-11.1

146381 - SuSE SLES 11 SP4 SUSE-SU-2018:0422-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2562, CVE-2018-2622, CVE-2018-2640, CVE-2018-2665, CVE-2018-2668

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0422-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003722.html

SuSE SLES 11 SP4
i586
mysql-client-5.5.59-0.39.9.8
mysql-5.5.59-0.39.9.8
mysql-tools-5.5.59-0.39.9.8
libmysql55client_r18-5.5.59-0.39.9.8
libmysql55client18-5.5.59-0.39.9.8

x86_64
libmysql55client_r18-32bit-5.5.59-0.39.9.8
mysql-5.5.59-0.39.9.8
libmysql55client_r18-5.5.59-0.39.9.8
libmysql55client18-5.5.59-0.39.9.8
mysql-client-5.5.59-0.39.9.8
libmysql55client18-32bit-5.5.59-0.39.9.8
mysql-tools-5.5.59-0.39.9.8

163545 - Oracle Enterprise Linux ELSA-2018-4025 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0861, CVE-2017-12193, CVE-2017-14140, CVE-2017-15115, CVE-2017-17712, CVE-2017-5754, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
ELSA-2018-4025

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-February/007525.html
http://oss.oracle.com/pipermail/el-errata/2018-February/007524.html

OEL7
x86_64
kernel-uek-debug-devel-4.1.12-112.14.14.el7uek
kernel-uek-firmware-4.1.12-112.14.14.el7uek
kernel-uek-doc-4.1.12-112.14.14.el7uek
kernel-uek-devel-4.1.12-112.14.14.el7uek
kernel-uek-4.1.12-112.14.14.el7uek
kernel-uek-debug-4.1.12-112.14.14.el7uek

OEL6
x86_64
kernel-uek-firmware-4.1.12-112.14.14.el6uek
kernel-uek-4.1.12-112.14.14.el6uek
kernel-uek-doc-4.1.12-112.14.14.el6uek
kernel-uek-debug-4.1.12-112.14.14.el6uek
kernel-uek-debug-devel-4.1.12-112.14.14.el6uek
kernel-uek-devel-4.1.12-112.14.14.el6uek

170924 - Amazon Linux AMI ALAS-2018-945 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
ALAS-2018-945

Observation

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

https://alas.aws.amazon.com/ALAS-2018-945.html

Amazon Linux AMI
x86_64
python27-devel-2.7.13-2.122.amzn1
python27-2.7.13-2.122.amzn1
python27-libs-2.7.13-2.122.amzn1
python27-tools-2.7.13-2.122.amzn1
python27-test-2.7.13-2.122.amzn1
python27-debuginfo-2.7.13-2.122.amzn1

i686
python27-devel-2.7.13-2.122.amzn1
python27-2.7.13-2.122.amzn1
python27-libs-2.7.13-2.122.amzn1
python27-tools-2.7.13-2.122.amzn1
python27-test-2.7.13-2.122.amzn1
python27-debuginfo-2.7.13-2.122.amzn1

178583 - Gentoo Linux GLSA-201802-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201802-01

Observation

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

https://security.gentoo.org/glsa/201802-01

Affected packages:
app-emulation/virtualbox < 5.1.32
app-emulation/virtualbox-bin < 5.1.32.120294
app-emulation/virtualbox-guest-additions < 5.1.32

182604 - FreeBSD python Possible Integer Overflow Vulnerability (0fe70bcd-2ce3-46c9-a64b-4a7da097db07)

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

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
python -- possible integer overflow vulnerability (0fe70bcd-2ce3-46c9-a64b-4a7da097db07)

Observation

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

http://www.vuxml.org/freebsd/0fe70bcd-2ce3-46c9-a64b-4a7da097db07.html

Affected packages:
python34 < 3.4.8
python35 < 3.5.5

186098 - Ubuntu Linux 14.04 USN-3566-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12933, CVE-2017-16642, CVE-2018-5712

Description

The scan detected that the host is missing the following update:
USN-3566-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004274.html

Ubuntu 14.04

php5-cgi_5.5.9+dfsg-1ubuntu4.23
php5-fpm_5.5.9+dfsg-1ubuntu4.23
php5-cli_5.5.9+dfsg-1ubuntu4.23
libapache2-mod-php5_5.5.9+dfsg-1ubuntu4.23

193268 - Fedora Linux 26 FEDORA-2018-bbf8c38b51 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15095, CVE-2017-17485, CVE-2017-7525, CVE-2018-5968

Description

The scan detected that the host is missing the following update:
FEDORA-2018-bbf8c38b51

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/2/?count=200&page=1

Fedora Core 26

jackson-databind-2.7.6-8.fc26

193269 - Fedora Linux 27 FEDORA-2018-e4b025841e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15095, CVE-2017-17485, CVE-2017-7525, CVE-2018-5968

Description

The scan detected that the host is missing the following update:
FEDORA-2018-e4b025841e

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/2/?count=200&page=1

Fedora Core 27

jackson-databind-2.7.6-8.fc27

23045 - (HT208474) Apple iTunes Vulnerabilities Prior To 12.7.3

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

Risk Level: Medium

CVE: CVE-2018-4088, CVE-2018-4096

Description

Multiple vulnerabilities are present in some versions of Apple iTunes.

Observation

Apple iTunes is a media management software.

Multiple vulnerabilities are present in some versions of Apple iTunes. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code.

23058 - Joomla XSS Vulnerability (20180102)

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

Risk Level: Medium

CVE: CVE-2018-6377

Description

A vulnerability is present in some versions of Joomla!.

Observation

Joomla! is an open source content management system.

A vulnerability is present in some versions of Joomla!. The flaw is due to insufficient input filtering in com_fields. Successful exploitation could allow an attacker to remotely execute arbitrary code.

23059 - Joomla SQLi Vulnerability (20180104)

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

Risk Level: Medium

CVE: CVE-2018-6376

Description

A vulnerability is present in some versions of Joomla!.

Observation

Joomla! is an open source content management system.

A vulnerability is present in some versions of Joomla!. The flaw is due to a lack of type casting of a variable used in an SQL statement. Successful exploitation could allow an attacker to inject arbitrary SQL code.

146359 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0407-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10219, CVE-2016-10317, CVE-2017-11714, CVE-2017-9216, CVE-2017-9612, CVE-2017-9726, CVE-2017-9727, CVE-2017-9739, CVE-2017-9835

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0407-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003717.html

SuSE SLES 12 SP2
x86_64
ghostscript-debuginfo-9.15-23.7.1
ghostscript-debugsource-9.15-23.7.1
ghostscript-x11-debuginfo-9.15-23.7.1
ghostscript-9.15-23.7.1
ghostscript-x11-9.15-23.7.1

SuSE SLED 12 SP3
x86_64

ghostscript-debuginfo-9.15-23.7.1
ghostscript-debugsource-9.15-23.7.1
ghostscript-x11-debuginfo-9.15-23.7.1
ghostscript-9.15-23.7.1
ghostscript-x11-9.15-23.7.1

SuSE SLED 12 SP2
x86_64
ghostscript-debuginfo-9.15-23.7.1
ghostscript-debugsource-9.15-23.7.1
ghostscript-x11-debuginfo-9.15-23.7.1
ghostscript-9.15-23.7.1
ghostscript-x11-9.15-23.7.1

SuSE SLES 12 SP3
x86_64
ghostscript-debuginfo-9.15-23.7.1
ghostscript-debugsource-9.15-23.7.1
ghostscript-x11-debuginfo-9.15-23.7.1
ghostscript-9.15-23.7.1
ghostscript-x11-9.15-23.7.1

146365 - SuSE SLES 11 SP4 SUSE-SU-2018:0395-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5131, CVE-2017-15412, CVE-2017-16932, CVE-2017-5130

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0395-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003715.html

SuSE SLES 11 SP4
i586
libxml2-python-2.7.6-0.77.10.1
libxml2-2.7.6-0.77.10.1
libxml2-doc-2.7.6-0.77.10.1

x86_64
libxml2-python-2.7.6-0.77.10.1
libxml2-2.7.6-0.77.10.1
libxml2-doc-2.7.6-0.77.10.1
libxml2-32bit-2.7.6-0.77.10.1

146369 - SuSE Linux 42.3 openSUSE-SU-2018:0421-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10219, CVE-2016-10317, CVE-2017-11714, CVE-2017-9216, CVE-2017-9612, CVE-2017-9726, CVE-2017-9727, CVE-2017-9739, CVE-2017-9835

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0421-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00039.html

SuSE Linux 42.3
x86_64
ghostscript-x11-debuginfo-9.15-14.3.1
ghostscript-mini-devel-9.15-14.3.1
ghostscript-9.15-14.3.1
ghostscript-mini-debugsource-9.15-14.3.1
ghostscript-devel-9.15-14.3.1
ghostscript-debugsource-9.15-14.3.1
ghostscript-mini-9.15-14.3.1
ghostscript-x11-9.15-14.3.1
ghostscript-mini-debuginfo-9.15-14.3.1
ghostscript-debuginfo-9.15-14.3.1

i586
ghostscript-x11-debuginfo-9.15-14.3.1
ghostscript-mini-devel-9.15-14.3.1
ghostscript-9.15-14.3.1
ghostscript-mini-debugsource-9.15-14.3.1
ghostscript-devel-9.15-14.3.1
ghostscript-debugsource-9.15-14.3.1
ghostscript-mini-9.15-14.3.1
ghostscript-x11-9.15-14.3.1
ghostscript-mini-debuginfo-9.15-14.3.1
ghostscript-debuginfo-9.15-14.3.1

146372 - SuSE Linux 42.3 openSUSE-SU-2018:0388-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14245, CVE-2017-14246, CVE-2017-14634, CVE-2017-16942, CVE-2017-6892

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0388-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00018.html

SuSE Linux 42.3
x86_64
libsndfile-progs-debugsource-1.0.25-31.1
libsndfile1-debuginfo-1.0.25-31.1
libsndfile-devel-1.0.25-31.1
libsndfile1-32bit-1.0.25-31.1

libsndfile-progs-1.0.25-31.1
libsndfile1-1.0.25-31.1
libsndfile-progs-debuginfo-1.0.25-31.1
libsndfile-debugsource-1.0.25-31.1
libsndfile1-debuginfo-32bit-1.0.25-31.1

i586
libsndfile-progs-debugsource-1.0.25-31.1
libsndfile1-debuginfo-1.0.25-31.1
libsndfile-devel-1.0.25-31.1
libsndfile-progs-1.0.25-31.1
libsndfile1-1.0.25-31.1
libsndfile-progs-debuginfo-1.0.25-31.1
libsndfile-debugsource-1.0.25-31.1

146373 - SuSE Linux 42.3 openSUSE-SU-2018:0418-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5131, CVE-2017-15412, CVE-2017-5130

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0418-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00036.html

SuSE Linux 42.3
i586
libxml2-2-debuginfo-2.9.4-15.1
libxml2-tools-2.9.4-15.1
python-libxml2-debuginfo-2.9.4-15.1
python-libxml2-2.9.4-15.1
libxml2-devel-2.9.4-15.1
libxml2-2-2.9.4-15.1
libxml2-tools-debuginfo-2.9.4-15.1
libxml2-debugsource-2.9.4-15.1
python-libxml2-debugsource-2.9.4-15.1

noarch
libxml2-doc-2.9.4-15.1

x86_64
libxml2-2-debuginfo-2.9.4-15.1
libxml2-tools-2.9.4-15.1
python-libxml2-debuginfo-2.9.4-15.1
python-libxml2-2.9.4-15.1
libxml2-devel-2.9.4-15.1
libxml2-devel-32bit-2.9.4-15.1
libxml2-2-2.9.4-15.1
libxml2-tools-debuginfo-2.9.4-15.1
libxml2-debugsource-2.9.4-15.1
libxml2-2-32bit-2.9.4-15.1
python-libxml2-debugsource-2.9.4-15.1

libxml2-2-debuginfo-32bit-2.9.4-15.1

146374 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0401-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5131, CVE-2017-15412, CVE-2017-5130

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0401-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003716.html

SuSE SLES 12 SP2
noarch
libxml2-doc-2.9.4-46.12.1

x86_64
python-libxml2-debuginfo-2.9.4-46.12.1
libxml2-2-32bit-2.9.4-46.12.1
libxml2-2-debuginfo-32bit-2.9.4-46.12.1
libxml2-tools-2.9.4-46.12.1
libxml2-2-2.9.4-46.12.1
libxml2-tools-debuginfo-2.9.4-46.12.1
libxml2-2-debuginfo-2.9.4-46.12.1
python-libxml2-debugsource-2.9.4-46.12.1
libxml2-debugsource-2.9.4-46.12.1
python-libxml2-2.9.4-46.12.1

SuSE SLED 12 SP3
x86_64
python-libxml2-debuginfo-2.9.4-46.12.1
libxml2-2-32bit-2.9.4-46.12.1
libxml2-2-debuginfo-32bit-2.9.4-46.12.1
libxml2-debugsource-2.9.4-46.12.1
libxml2-2-2.9.4-46.12.1
libxml2-tools-debuginfo-2.9.4-46.12.1
libxml2-2-debuginfo-2.9.4-46.12.1
libxml2-tools-2.9.4-46.12.1
python-libxml2-debugsource-2.9.4-46.12.1
python-libxml2-2.9.4-46.12.1

SuSE SLED 12 SP2
x86_64
python-libxml2-debuginfo-2.9.4-46.12.1
libxml2-2-32bit-2.9.4-46.12.1
libxml2-2-debuginfo-32bit-2.9.4-46.12.1
libxml2-debugsource-2.9.4-46.12.1
libxml2-2-2.9.4-46.12.1
libxml2-tools-debuginfo-2.9.4-46.12.1
libxml2-2-debuginfo-2.9.4-46.12.1
libxml2-tools-2.9.4-46.12.1
python-libxml2-debugsource-2.9.4-46.12.1

python-libxml2-2.9.4-46.12.1

SuSE SLES 12 SP3
noarch
libxml2-doc-2.9.4-46.12.1

x86_64
python-libxml2-debuginfo-2.9.4-46.12.1
libxml2-2-32bit-2.9.4-46.12.1
libxml2-2-debuginfo-32bit-2.9.4-46.12.1
libxml2-tools-2.9.4-46.12.1
libxml2-2-2.9.4-46.12.1
libxml2-tools-debuginfo-2.9.4-46.12.1
libxml2-2-debuginfo-2.9.4-46.12.1
python-libxml2-debugsource-2.9.4-46.12.1
libxml2-debugsource-2.9.4-46.12.1
python-libxml2-2.9.4-46.12.1

170927 - Amazon Linux AMI ALAS-2018-950 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5702

Description

The scan detected that the host is missing the following update:
ALAS-2018-950

Observation

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

https://alas.aws.amazon.com/ALAS-2018-950.html

Amazon Linux AMI
x86_64
transmission-common-2.92-11.12.amzn1
transmission-debuginfo-2.92-11.12.amzn1
transmission-cli-2.92-11.12.amzn1
transmission-daemon-2.92-11.12.amzn1
transmission-2.92-11.12.amzn1

i686
transmission-common-2.92-11.12.amzn1
transmission-cli-2.92-11.12.amzn1
transmission-debuginfo-2.92-11.12.amzn1
transmission-daemon-2.92-11.12.amzn1
transmission-2.92-11.12.amzn1

182601 - FreeBSD tiff Multiple Vulnerabilities (b38e8150-0535-11e8-96ab-0800271d4b9c)

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

Risk Level: Medium

CVE: CVE-2017-18013, CVE-2017-9935

Description

The scan detected that the host is missing the following update:
tiff -- multiple vulnerabilities (b38e8150-0535-11e8-96ab-0800271d4b9c)

Observation

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

http://www.vuxml.org/freebsd/b38e8150-0535-11e8-96ab-0800271d4b9c.html

Affected packages:
tiff <= 4.0.9

131013 - Debian Linux 9.0 DSA-4106-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10790, CVE-2018-6003

Description

The scan detected that the host is missing the following update:
DSA-4106-1

Observation

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

http://www.debian.org/security/2018/dsa-4106

Debian 9.0
all
libtasn1-6_4.10-1.1+deb9u1

131019 - Debian Linux 8.0, 9.0 DSA-4109-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18076

Description

The scan detected that the host is missing the following update:
DSA-4109-1

Observation

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

http://www.debian.org/security/2018/dsa-4109

Debian 8.0
all
ruby-omniauth_1.2.1-1+deb8u1

Debian 9.0
all
ruby-omniauth_1.3.1-1+deb9u1

146370 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0385-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5748

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0385-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003713.html

SuSE SLED 12 SP2
x86_64
libvirt-client-debuginfo-32bit-2.0.0-27.29.1
libvirt-daemon-driver-interface-2.0.0-27.29.1
libvirt-daemon-driver-secret-2.0.0-27.29.1
libvirt-2.0.0-27.29.1
libvirt-daemon-driver-nodedev-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-libxl-2.0.0-27.29.1
libvirt-daemon-qemu-2.0.0-27.29.1
libvirt-daemon-driver-storage-debuginfo-2.0.0-27.29.1
libvirt-daemon-config-network-2.0.0-27.29.1
libvirt-daemon-driver-lxc-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-nodedev-2.0.0-27.29.1
libvirt-daemon-debuginfo-2.0.0-27.29.1
libvirt-daemon-config-nwfilter-2.0.0-27.29.1
libvirt-daemon-driver-network-2.0.0-27.29.1
libvirt-daemon-driver-qemu-2.0.0-27.29.1
libvirt-client-2.0.0-27.29.1
libvirt-daemon-lxc-2.0.0-27.29.1
libvirt-client-debuginfo-2.0.0-27.29.1
libvirt-client-32bit-2.0.0-27.29.1
libvirt-daemon-driver-lxc-2.0.0-27.29.1
libvirt-daemon-driver-storage-2.0.0-27.29.1
libvirt-daemon-driver-network-debuginfo-2.0.0-27.29.1
libvirt-debugsource-2.0.0-27.29.1
libvirt-daemon-driver-nwfilter-2.0.0-27.29.1
libvirt-daemon-driver-libxl-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-secret-debuginfo-2.0.0-27.29.1
libvirt-daemon-xen-2.0.0-27.29.1
libvirt-daemon-driver-qemu-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-nwfilter-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-interface-debuginfo-2.0.0-27.29.1
libvirt-daemon-2.0.0-27.29.1
libvirt-doc-2.0.0-27.29.1

SuSE SLES 12 SP2
x86_64
libvirt-daemon-driver-interface-2.0.0-27.29.1
libvirt-daemon-driver-secret-2.0.0-27.29.1
libvirt-2.0.0-27.29.1
libvirt-daemon-driver-qemu-2.0.0-27.29.1
libvirt-daemon-driver-libxl-2.0.0-27.29.1

libvirt-lock-sanlock-2.0.0-27.29.1
libvirt-daemon-qemu-2.0.0-27.29.1
libvirt-nss-2.0.0-27.29.1
libvirt-daemon-driver-network-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-storage-debuginfo-2.0.0-27.29.1
libvirt-daemon-config-network-2.0.0-27.29.1
libvirt-daemon-driver-lxc-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-nodedev-2.0.0-27.29.1
libvirt-daemon-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-nodedev-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-network-2.0.0-27.29.1
libvirt-lock-sanlock-debuginfo-2.0.0-27.29.1
libvirt-client-2.0.0-27.29.1
libvirt-daemon-lxc-2.0.0-27.29.1
libvirt-daemon-driver-interface-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-lxc-2.0.0-27.29.1
libvirt-daemon-driver-storage-2.0.0-27.29.1
libvirt-daemon-config-nwfilter-2.0.0-27.29.1
libvirt-debugsource-2.0.0-27.29.1
libvirt-daemon-driver-nwfilter-2.0.0-27.29.1
libvirt-daemon-driver-libxl-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-secret-debuginfo-2.0.0-27.29.1
libvirt-nss-debuginfo-2.0.0-27.29.1
libvirt-daemon-xen-2.0.0-27.29.1
libvirt-daemon-driver-qemu-debuginfo-2.0.0-27.29.1
libvirt-daemon-driver-nwfilter-debuginfo-2.0.0-27.29.1
libvirt-client-debuginfo-2.0.0-27.29.1
libvirt-daemon-2.0.0-27.29.1
libvirt-doc-2.0.0-27.29.1

170926 - Amazon Linux AMI ALAS-2018-949 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

The scan detected that the host is missing the following update:
ALAS-2018-949

Observation

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

https://alas.aws.amazon.com/ALAS-2018-949.html

Amazon Linux AMI
i686
java-1.8.0-openjdk-debuginfo-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-src-1.8.0.161-0.b14.36.amzn1

noarch
java-1.8.0-openjdk-javadoc-1.8.0.161-0.b14.36.amzn1

java-1.8.0-openjdk-javadoc-zip-1.8.0.161-0.b14.36.amzn1

x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.36.amzn1
java-1.8.0-openjdk-src-1.8.0.161-0.b14.36.amzn1

193266 - Fedora Linux 27 FEDORA-2018-0ad6e73ac0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6196, CVE-2018-6197, CVE-2018-6198

Description

The scan detected that the host is missing the following update:
FEDORA-2018-0ad6e73ac0

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/2/?count=200&page=1

Fedora Core 27

w3m-0.5.3-36.git20180125.fc27

23041 - IBM AIX OpenSSL Security Bypass Vulnerability (openssl_advisory25)

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

Risk Level: Medium

CVE: CVE-2017-3737

Description

A vulnerability is present in some versions of IBM AIX.

Observation

AIX is a Unix-like operating system developed by IBM.

A vulnerability is present in some versions of IBM AIX. The flaw lies in OpenSSL. Successful exploitation could allow an attacker to bypass certain security restrictions.

23056 - Joomla XSS Vulnerability (20180103)

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

Risk Level: Medium

CVE: CVE-2018-6379

Description

A vulnerability is present in some versions of Joomla!.

Observation

Joomla! is an open source content management system.

A vulnerability is present in some versions of Joomla!. The flaw is due to insufficient input filtering in the Uri class. Successful exploitation could allow an attacker to remotely execute arbitrary code.

88916 - Slackware Linux 14.2 SSA:2018-037-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SSA:2018-037-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2018&m=slackware-security.701978

Slackware 14.2
i586
kernel-huge-4.4.115-i586-1
kernel-modules-4.4.115-i586-1
kernel-generic-4.4.115-i586-1

i686
kernel-modules-smp-4.4.115_smp-i686-1
kernel-huge-smp-4.4.115_smp-i686-1
kernel-generic-smp-4.4.115_smp-i686-1

noarch
kernel-source-4.4.115-noarch-1
kernel-firmware-20180201_2aa2ac2-noarch-1
kernel-source-4.4.115_smp-noarch-1

x86_64
kernel-huge-4.4.115-x86_64-1
kernel-generic-4.4.115-x86_64-1
kernel-modules-4.4.115-x86_64-1

131016 - Debian Linux 8.0, 9.0 DSA-4108-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5950

Description

The scan detected that the host is missing the following update:
DSA-4108-1

Observation

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

For more information see:

http://www.debian.org/security/2018/dsa-4108

Debian 8.0
all
mailman_2.1.18-2+deb8u2

Debian 9.0
all
mailman_2.1.23-1+deb9u2

141868 - Red Hat Enterprise Linux RHSA-2018-0292 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0292

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-February/msg00011.html

RHEL5
i386
kernel-devel-2.6.18-426.el5
kernel-xen-devel-2.6.18-426.el5
kernel-xen-2.6.18-426.el5
kernel-headers-2.6.18-426.el5
kernel-debuginfo-2.6.18-426.el5
kernel-PAE-2.6.18-426.el5
kernel-debug-devel-2.6.18-426.el5
kernel-xen-debuginfo-2.6.18-426.el5
kernel-2.6.18-426.el5
kernel-PAE-debuginfo-2.6.18-426.el5
kernel-debug-2.6.18-426.el5
kernel-PAE-devel-2.6.18-426.el5
kernel-debuginfo-common-2.6.18-426.el5
kernel-debug-debuginfo-2.6.18-426.el5

noarch
kernel-doc-2.6.18-426.el5

x86_64
kernel-devel-2.6.18-426.el5
kernel-debug-debuginfo-2.6.18-426.el5
kernel-2.6.18-426.el5
kernel-xen-2.6.18-426.el5
kernel-debug-devel-2.6.18-426.el5
kernel-xen-devel-2.6.18-426.el5
kernel-debug-2.6.18-426.el5
kernel-headers-2.6.18-426.el5
kernel-xen-debuginfo-2.6.18-426.el5

kernel-debuginfo-2.6.18-426.el5
kernel-debuginfo-common-2.6.18-426.el5

146351 - SuSE Linux 42.3 openSUSE-SU-2018:0399-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15108

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0399-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00028.html

SuSE Linux 42.3
x86_64
spice-vdagent-0.16.0-8.1
spice-vdagent-debuginfo-0.16.0-8.1
spice-vdagent-debugsource-0.16.0-8.1

146353 - SuSE Linux 42.3 openSUSE-SU-2018:0406-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14992, CVE-2017-16539

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0406-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00034.html

SuSE Linux 42.3
i586
docker-libnetwork-0.7.0.1+gitr2066_7b2b1feb1de4-5.1
golang-github-docker-libnetwork-0.7.0.1+gitr2066_7b2b1feb1de4-5.1
docker-runc-debuginfo-1.0.0rc4+gitr3338_3f2f8b84a77f-2.1
containerd-ctr-debuginfo-0.2.9+gitr706_06b9cb351610-16.1
docker-libnetwork-debuginfo-0.7.0.1+gitr2066_7b2b1feb1de4-5.1
docker-runc-1.0.0rc4+gitr3338_3f2f8b84a77f-2.1
containerd-debugsource-0.2.9+gitr706_06b9cb351610-16.1
golang-github-docker-libnetwork-debugsource-0.7.0.1+gitr2066_7b2b1feb1de4-5.1
docker-runc-debugsource-1.0.0rc4+gitr3338_3f2f8b84a77f-2.1
containerd-0.2.9+gitr706_06b9cb351610-16.1
containerd-debuginfo-0.2.9+gitr706_06b9cb351610-16.1
containerd-ctr-0.2.9+gitr706_06b9cb351610-16.1

noarch
docker-runc-test-1.0.0rc4+gitr3338_3f2f8b84a77f-2.1
docker-zsh-completion-17.09.1_ce-36.1
containerd-test-0.2.9+gitr706_06b9cb351610-16.1
docker-bash-completion-17.09.1_ce-36.1

x86_64
docker-test-debuginfo-17.09.1_ce-36.1
containerd-ctr-0.2.9+gitr706_06b9cb351610-16.1
docker-debugsource-17.09.1_ce-36.1
docker-libnetwork-0.7.0.1+gitr2066_7b2b1feb1de4-5.1
containerd-0.2.9+gitr706_06b9cb351610-16.1
docker-libnetwork-debuginfo-0.7.0.1+gitr2066_7b2b1feb1de4-5.1
containerd-ctr-debuginfo-0.2.9+gitr706_06b9cb351610-16.1
docker-test-17.09.1_ce-36.1
docker-17.09.1_ce-36.1
docker-runc-debugsource-1.0.0rc4+gitr3338_3f2f8b84a77f-2.1
docker-runc-1.0.0rc4+gitr3338_3f2f8b84a77f-2.1
docker-debuginfo-17.09.1_ce-36.1
golang-github-docker-libnetwork-0.7.0.1+gitr2066_7b2b1feb1de4-5.1
golang-github-docker-libnetwork-debugsource-0.7.0.1+gitr2066_7b2b1feb1de4-5.1
docker-runc-debuginfo-1.0.0rc4+gitr3338_3f2f8b84a77f-2.1
containerd-debugsource-0.2.9+gitr706_06b9cb351610-16.1
containerd-debuginfo-0.2.9+gitr706_06b9cb351610-16.1

146357 - SuSE Linux 42.3 openSUSE-SU-2018:0400-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10268, CVE-2017-10378

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0400-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00029.html

SuSE Linux 42.3
x86_64
mariadb-bench-debuginfo-10.0.33-29.1
mariadb-debugsource-10.0.33-29.1
mariadb-debuginfo-10.0.33-29.1
mariadb-tools-debuginfo-10.0.33-29.1
libmysqlclient_r18-32bit-10.0.33-29.1
libmysqld-devel-10.0.33-29.1
libmysqlclient18-32bit-10.0.33-29.1
libmysqlclient-devel-10.0.33-29.1
mariadb-client-debuginfo-10.0.33-29.1
libmysqlclient18-debuginfo-10.0.33-29.1
mariadb-test-10.0.33-29.1
libmysqld18-10.0.33-29.1
mariadb-10.0.33-29.1
mariadb-tools-10.0.33-29.1
libmysqlclient18-10.0.33-29.1

mariadb-errormessages-10.0.33-29.1
libmysqlclient_r18-10.0.33-29.1
mariadb-bench-10.0.33-29.1
mariadb-client-10.0.33-29.1
mariadb-test-debuginfo-10.0.33-29.1
libmysqld18-debuginfo-10.0.33-29.1
libmysqlclient18-debuginfo-32bit-10.0.33-29.1

i586
mariadb-bench-debuginfo-10.0.33-29.1
mariadb-debugsource-10.0.33-29.1
mariadb-debuginfo-10.0.33-29.1
mariadb-tools-debuginfo-10.0.33-29.1
libmysqld-devel-10.0.33-29.1
libmysqlclient-devel-10.0.33-29.1
mariadb-client-debuginfo-10.0.33-29.1
libmysqlclient18-debuginfo-10.0.33-29.1
mariadb-test-10.0.33-29.1
libmysqld18-10.0.33-29.1
mariadb-10.0.33-29.1
mariadb-tools-10.0.33-29.1
libmysqlclient18-10.0.33-29.1
mariadb-errormessages-10.0.33-29.1
libmysqlclient_r18-10.0.33-29.1
mariadb-bench-10.0.33-29.1
mariadb-client-10.0.33-29.1
mariadb-test-debuginfo-10.0.33-29.1
libmysqld18-debuginfo-10.0.33-29.1

146358 - SuSE Linux 42.3 openSUSE-SU-2018:0393-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15232

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0393-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00023.html

SuSE Linux 42.3
x86_64
libjpeg8-debuginfo-32bit-8.1.2-42.1
libturbojpeg0-8.1.2-42.1
libturbojpeg0-debuginfo-8.1.2-42.1
libturbojpeg0-debuginfo-32bit-8.1.2-42.1
libjpeg8-devel-32bit-8.1.2-42.1
libjpeg62-turbo-1.5.3-42.1
libjpeg62-debuginfo-62.2.0-42.1
libjpeg62-turbo-debugsource-1.5.3-42.1
libjpeg8-32bit-8.1.2-42.1
libjpeg62-devel-62.2.0-42.1
libjpeg-turbo-debugsource-1.5.3-42.1

libjpeg-turbo-1.5.3-42.1
libjpeg62-62.2.0-42.1
libjpeg62-devel-32bit-62.2.0-42.1
libjpeg62-debuginfo-32bit-62.2.0-42.1
libturbojpeg0-32bit-8.1.2-42.1
libjpeg-turbo-debuginfo-1.5.3-42.1
libjpeg62-32bit-62.2.0-42.1
libjpeg8-debuginfo-8.1.2-42.1
libjpeg8-8.1.2-42.1
libjpeg8-devel-8.1.2-42.1

i586
libturbojpeg0-8.1.2-42.1
libturbojpeg0-debuginfo-8.1.2-42.1
libjpeg62-turbo-1.5.3-42.1
libjpeg62-debuginfo-62.2.0-42.1
libjpeg62-turbo-debugsource-1.5.3-42.1
libjpeg62-devel-62.2.0-42.1
libjpeg-turbo-debugsource-1.5.3-42.1
libjpeg-turbo-1.5.3-42.1
libjpeg62-62.2.0-42.1
libjpeg-turbo-debuginfo-1.5.3-42.1
libjpeg8-debuginfo-8.1.2-42.1
libjpeg8-8.1.2-42.1
libjpeg8-devel-8.1.2-42.1

146360 - SuSE Linux 42.3 openSUSE-SU-2018:0402-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15612, CVE-2017-16876

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0402-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00030.html

SuSE Linux 42.3
noarch
python-mistune-0.8.3-11.1
python3-mistune-0.8.3-9.1

146361 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0384-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10268, CVE-2017-10378

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0384-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003712.html

SuSE SLED 12 SP2
x86_64
mariadb-debuginfo-10.0.33-29.13.1
mariadb-client-debuginfo-10.0.33-29.13.1
libmysqlclient18-32bit-10.0.33-29.13.1
libmysqlclient18-debuginfo-10.0.33-29.13.1
libmysqlclient18-10.0.33-29.13.1
mariadb-10.0.33-29.13.1
libmysqlclient_r18-32bit-10.0.33-29.13.1
mariadb-errormessages-10.0.33-29.13.1
libmysqlclient18-debuginfo-32bit-10.0.33-29.13.1
libmysqlclient_r18-10.0.33-29.13.1
mariadb-client-10.0.33-29.13.1
mariadb-debugsource-10.0.33-29.13.1

SuSE SLES 12 SP3
x86_64
libmysqlclient18-debuginfo-32bit-10.0.33-29.13.1
mariadb-debuginfo-10.0.33-29.13.1
mariadb-client-debuginfo-10.0.33-29.13.1
libmysqlclient18-32bit-10.0.33-29.13.1
mariadb-client-10.0.33-29.13.1
libmysqlclient18-10.0.33-29.13.1
mariadb-tools-10.0.33-29.13.1
libmysqlclient18-debuginfo-10.0.33-29.13.1
mariadb-tools-debuginfo-10.0.33-29.13.1
mariadb-10.0.33-29.13.1
mariadb-errormessages-10.0.33-29.13.1
mariadb-debugsource-10.0.33-29.13.1

SuSE SLES 12 SP2
x86_64
libmysqlclient18-debuginfo-32bit-10.0.33-29.13.1
mariadb-debuginfo-10.0.33-29.13.1
mariadb-client-debuginfo-10.0.33-29.13.1
libmysqlclient18-32bit-10.0.33-29.13.1
mariadb-client-10.0.33-29.13.1
libmysqlclient18-10.0.33-29.13.1
mariadb-tools-10.0.33-29.13.1
libmysqlclient18-debuginfo-10.0.33-29.13.1
mariadb-tools-debuginfo-10.0.33-29.13.1
mariadb-10.0.33-29.13.1
mariadb-errormessages-10.0.33-29.13.1
mariadb-debugsource-10.0.33-29.13.1

SuSE SLED 12 SP3
x86_64
mariadb-debuginfo-10.0.33-29.13.1
mariadb-client-debuginfo-10.0.33-29.13.1
libmysqlclient18-32bit-10.0.33-29.13.1
libmysqlclient18-debuginfo-10.0.33-29.13.1
libmysqlclient18-10.0.33-29.13.1
mariadb-10.0.33-29.13.1
libmysqlclient_r18-32bit-10.0.33-29.13.1

mariadb-errormessages-10.0.33-29.13.1
libmysqlclient18-debuginfo-32bit-10.0.33-29.13.1
libmysqlclient_r18-10.0.33-29.13.1
mariadb-client-10.0.33-29.13.1
mariadb-debugsource-10.0.33-29.13.1

146363 - SuSE Linux 42.3 openSUSE-SU-2018:0405-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6187, CVE-2018-6192, CVE-2018-6544

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0405-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00033.html

SuSE Linux 42.3
x86_64
mupdf-devel-static-1.12.0-28.1
mupdf-1.12.0-28.1

i586
mupdf-devel-static-1.12.0-28.1
mupdf-1.12.0-28.1

170922 - Amazon Linux AMI ALAS-2018-946 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5711, CVE-2018-5712

Description

The scan detected that the host is missing the following update:
ALAS-2018-946

Observation

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

https://alas.aws.amazon.com/ALAS-2018-946.html

Amazon Linux AMI
x86_64
php70-pdo-7.0.27-1.27.amzn1
php71-common-7.1.13-1.30.amzn1
php71-imap-7.1.13-1.30.amzn1
php71-7.1.13-1.30.amzn1
php56-odbc-5.6.33-1.136.amzn1
php56-mysqlnd-5.6.33-1.136.amzn1
php71-gd-7.1.13-1.30.amzn1

php70-common-7.0.27-1.27.amzn1
php70-pspell-7.0.27-1.27.amzn1
php56-pspell-5.6.33-1.136.amzn1
php56-opcache-5.6.33-1.136.amzn1
php56-mssql-5.6.33-1.136.amzn1
php56-tidy-5.6.33-1.136.amzn1
php71-bcmath-7.1.13-1.30.amzn1
php71-xmlrpc-7.1.13-1.30.amzn1
php56-intl-5.6.33-1.136.amzn1
php70-pdo-dblib-7.0.27-1.27.amzn1
php71-soap-7.1.13-1.30.amzn1
php70-recode-7.0.27-1.27.amzn1
php70-tidy-7.0.27-1.27.amzn1
php71-xml-7.1.13-1.30.amzn1
php56-dba-5.6.33-1.136.amzn1
php56-common-5.6.33-1.136.amzn1
php56-fpm-5.6.33-1.136.amzn1
php71-cli-7.1.13-1.30.amzn1
php70-cli-7.0.27-1.27.amzn1
php70-zip-7.0.27-1.27.amzn1
php70-dba-7.0.27-1.27.amzn1
php56-process-5.6.33-1.136.amzn1
php56-cli-5.6.33-1.136.amzn1
php56-xmlrpc-5.6.33-1.136.amzn1
php70-enchant-7.0.27-1.27.amzn1
php71-mcrypt-7.1.13-1.30.amzn1
php71-mbstring-7.1.13-1.30.amzn1
php70-7.0.27-1.27.amzn1
php70-xmlrpc-7.0.27-1.27.amzn1
php70-fpm-7.0.27-1.27.amzn1
php71-odbc-7.1.13-1.30.amzn1
php70-debuginfo-7.0.27-1.27.amzn1
php71-gmp-7.1.13-1.30.amzn1
php71-mysqlnd-7.1.13-1.30.amzn1
php70-json-7.0.27-1.27.amzn1
php56-gd-5.6.33-1.136.amzn1
php71-dba-7.1.13-1.30.amzn1
php70-odbc-7.0.27-1.27.amzn1
php56-recode-5.6.33-1.136.amzn1
php71-pdo-dblib-7.1.13-1.30.amzn1
php56-enchant-5.6.33-1.136.amzn1
php70-mbstring-7.0.27-1.27.amzn1
php70-opcache-7.0.27-1.27.amzn1
php70-gmp-7.0.27-1.27.amzn1
php70-intl-7.0.27-1.27.amzn1
php70-dbg-7.0.27-1.27.amzn1
php71-devel-7.1.13-1.30.amzn1
php71-pdo-7.1.13-1.30.amzn1
php70-process-7.0.27-1.27.amzn1
php70-xml-7.0.27-1.27.amzn1
php71-tidy-7.1.13-1.30.amzn1
php70-bcmath-7.0.27-1.27.amzn1
php71-pspell-7.1.13-1.30.amzn1
php70-snmp-7.0.27-1.27.amzn1
php56-pdo-5.6.33-1.136.amzn1
php56-5.6.33-1.136.amzn1
php71-opcache-7.1.13-1.30.amzn1
php56-bcmath-5.6.33-1.136.amzn1
php56-gmp-5.6.33-1.136.amzn1
php70-pgsql-7.0.27-1.27.amzn1

php71-debuginfo-7.1.13-1.30.amzn1
php71-enchant-7.1.13-1.30.amzn1
php71-pgsql-7.1.13-1.30.amzn1
php71-snmp-7.1.13-1.30.amzn1
php71-ldap-7.1.13-1.30.amzn1
php70-imap-7.0.27-1.27.amzn1
php70-embedded-7.0.27-1.27.amzn1
php70-gd-7.0.27-1.27.amzn1
php56-debuginfo-5.6.33-1.136.amzn1
php71-json-7.1.13-1.30.amzn1
php70-devel-7.0.27-1.27.amzn1
php56-embedded-5.6.33-1.136.amzn1
php56-snmp-5.6.33-1.136.amzn1
php56-soap-5.6.33-1.136.amzn1
php70-mysqlnd-7.0.27-1.27.amzn1
php70-ldap-7.0.27-1.27.amzn1
php70-soap-7.0.27-1.27.amzn1
php71-fpm-7.1.13-1.30.amzn1
php71-process-7.1.13-1.30.amzn1
php70-mcrypt-7.0.27-1.27.amzn1
php56-dbg-5.6.33-1.136.amzn1
php56-devel-5.6.33-1.136.amzn1
php56-xml-5.6.33-1.136.amzn1
php56-mbstring-5.6.33-1.136.amzn1
php71-recode-7.1.13-1.30.amzn1
php56-mcrypt-5.6.33-1.136.amzn1
php71-embedded-7.1.13-1.30.amzn1
php71-dbg-7.1.13-1.30.amzn1
php71-intl-7.1.13-1.30.amzn1
php56-imap-5.6.33-1.136.amzn1
php56-pgsql-5.6.33-1.136.amzn1
php56-ldap-5.6.33-1.136.amzn1

i686
php70-pdo-7.0.27-1.27.amzn1
php71-common-7.1.13-1.30.amzn1
php71-imap-7.1.13-1.30.amzn1
php71-7.1.13-1.30.amzn1
php56-odbc-5.6.33-1.136.amzn1
php56-mysqlnd-5.6.33-1.136.amzn1
php71-gd-7.1.13-1.30.amzn1
php70-common-7.0.27-1.27.amzn1
php70-pspell-7.0.27-1.27.amzn1
php56-pspell-5.6.33-1.136.amzn1
php56-opcache-5.6.33-1.136.amzn1
php56-mssql-5.6.33-1.136.amzn1
php56-tidy-5.6.33-1.136.amzn1
php71-bcmath-7.1.13-1.30.amzn1
php71-xmlrpc-7.1.13-1.30.amzn1
php56-5.6.33-1.136.amzn1
php70-pdo-dblib-7.0.27-1.27.amzn1
php71-soap-7.1.13-1.30.amzn1
php70-recode-7.0.27-1.27.amzn1
php70-tidy-7.0.27-1.27.amzn1
php71-xml-7.1.13-1.30.amzn1
php56-dba-5.6.33-1.136.amzn1
php56-common-5.6.33-1.136.amzn1
php56-fpm-5.6.33-1.136.amzn1
php71-cli-7.1.13-1.30.amzn1
php70-cli-7.0.27-1.27.amzn1

php70-zip-7.0.27-1.27.amzn1
php70-dba-7.0.27-1.27.amzn1
php56-mcrypt-5.6.33-1.136.amzn1
php56-process-5.6.33-1.136.amzn1
php56-cli-5.6.33-1.136.amzn1
php56-xmlrpc-5.6.33-1.136.amzn1
php70-enchant-7.0.27-1.27.amzn1
php71-mcrypt-7.1.13-1.30.amzn1
php71-mbstring-7.1.13-1.30.amzn1
php70-7.0.27-1.27.amzn1
php70-xmlrpc-7.0.27-1.27.amzn1
php70-fpm-7.0.27-1.27.amzn1
php56-intl-5.6.33-1.136.amzn1
php71-odbc-7.1.13-1.30.amzn1
php70-gmp-7.0.27-1.27.amzn1
php71-gmp-7.1.13-1.30.amzn1
php71-mysqlnd-7.1.13-1.30.amzn1
php70-json-7.0.27-1.27.amzn1
php56-gd-5.6.33-1.136.amzn1
php71-dba-7.1.13-1.30.amzn1
php70-odbc-7.0.27-1.27.amzn1
php56-recode-5.6.33-1.136.amzn1
php70-ldap-7.0.27-1.27.amzn1
php56-enchant-5.6.33-1.136.amzn1
php70-opcache-7.0.27-1.27.amzn1
php70-intl-7.0.27-1.27.amzn1
php70-dbg-7.0.27-1.27.amzn1
php71-devel-7.1.13-1.30.amzn1
php71-pdo-7.1.13-1.30.amzn1
php70-process-7.0.27-1.27.amzn1
php70-xml-7.0.27-1.27.amzn1
php71-tidy-7.1.13-1.30.amzn1
php70-bcmath-7.0.27-1.27.amzn1
php71-pspell-7.1.13-1.30.amzn1
php70-snmp-7.0.27-1.27.amzn1
php56-pdo-5.6.33-1.136.amzn1
php70-mbstring-7.0.27-1.27.amzn1
php56-bcmath-5.6.33-1.136.amzn1
php56-gmp-5.6.33-1.136.amzn1
php70-pgsql-7.0.27-1.27.amzn1
php71-debuginfo-7.1.13-1.30.amzn1
php71-enchant-7.1.13-1.30.amzn1
php71-pgsql-7.1.13-1.30.amzn1
php71-snmp-7.1.13-1.30.amzn1
php71-ldap-7.1.13-1.30.amzn1
php70-imap-7.0.27-1.27.amzn1
php70-embedded-7.0.27-1.27.amzn1
php70-gd-7.0.27-1.27.amzn1
php71-pdo-dblib-7.1.13-1.30.amzn1
php56-debuginfo-5.6.33-1.136.amzn1
php71-json-7.1.13-1.30.amzn1
php70-devel-7.0.27-1.27.amzn1
php56-snmp-5.6.33-1.136.amzn1
php56-soap-5.6.33-1.136.amzn1
php70-mysqlnd-7.0.27-1.27.amzn1
php70-soap-7.0.27-1.27.amzn1
php71-fpm-7.1.13-1.30.amzn1
php71-process-7.1.13-1.30.amzn1
php70-mcrypt-7.0.27-1.27.amzn1
php71-opcache-7.1.13-1.30.amzn1

php56-dbg-5.6.33-1.136.amzn1
php56-devel-5.6.33-1.136.amzn1
php56-xml-5.6.33-1.136.amzn1
php56-mbstring-5.6.33-1.136.amzn1
php71-recode-7.1.13-1.30.amzn1
php56-embedded-5.6.33-1.136.amzn1
php71-embedded-7.1.13-1.30.amzn1
php70-debuginfo-7.0.27-1.27.amzn1
php71-dbg-7.1.13-1.30.amzn1
php71-intl-7.1.13-1.30.amzn1
php56-imap-5.6.33-1.136.amzn1
php56-pgsql-5.6.33-1.136.amzn1
php56-ldap-5.6.33-1.136.amzn1

170925 - Amazon Linux AMI ALAS-2018-948 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15298

Description

The scan detected that the host is missing the following update:
ALAS-2018-948

Observation

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

https://alas.aws.amazon.com/ALAS-2018-948.html

Amazon Linux AMI
i686
git-2.13.6-2.56.amzn1
git-svn-2.13.6-2.56.amzn1
git-debuginfo-2.13.6-2.56.amzn1
git-daemon-2.13.6-2.56.amzn1

noarch
perl-Git-2.13.6-2.56.amzn1
git-cvs-2.13.6-2.56.amzn1
git-bzr-2.13.6-2.56.amzn1
gitweb-2.13.6-2.56.amzn1
git-email-2.13.6-2.56.amzn1
emacs-git-el-2.13.6-2.56.amzn1
git-all-2.13.6-2.56.amzn1
git-p4-2.13.6-2.56.amzn1
emacs-git-2.13.6-2.56.amzn1
git-hg-2.13.6-2.56.amzn1
perl-Git-SVN-2.13.6-2.56.amzn1

x86_64
git-2.13.6-2.56.amzn1
git-svn-2.13.6-2.56.amzn1
git-debuginfo-2.13.6-2.56.amzn1
git-daemon-2.13.6-2.56.amzn1

182594 - FreeBSD bchunk Heap-based Buffer Overflow (with invalid free) and crash (8ba2819c-0e9d-11e8-83e7-

485b3931c969)

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

Risk Level: Medium

CVE: CVE-2017-15954

Description

The scan detected that the host is missing the following update:
bchunk -- heap-based buffer overflow (with invalid free) and crash (8ba2819c-0e9d-11e8-83e7-485b3931c969)

Observation

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

http://www.vuxml.org/freebsd/8ba2819c-0e9d-11e8-83e7-485b3931c969.html

Affected packages:
1.2.0 <= bchunk <= 1.2.1

182597 - FreeBSD bchunk Heap-based Buffer Overflow And Crash (1ec1c59b-0e98-11e8-83e7-485b3931c969)

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

Risk Level: Medium

CVE: CVE-2017-15953

Description

The scan detected that the host is missing the following update:
bchunk -- heap-based buffer overflow and crash (1ec1c59b-0e98-11e8-83e7-485b3931c969)

Observation

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

http://www.vuxml.org/freebsd/1ec1c59b-0e98-11e8-83e7-485b3931c969.html

Affected packages:
1.2.0 <= bchunk <= 1.2.1

182599 - FreeBSD bchunk Access Violation Near NULL On Destination Operand And Crash (279f682c-0e9e-11e8-83e7-485b3931c969)

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

Risk Level: Medium

CVE: CVE-2017-15955

Description

The scan detected that the host is missing the following update:
bchunk -- access violation near NULL on destination operand and crash (279f682c-0e9e-11e8-83e7-485b3931c969)

Observation

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

http://www.vuxml.org/freebsd/279f682c-0e9e-11e8-83e7-485b3931c969.html

Affected packages:
1.2.0 <= bchunk <= 1.2.1

182605 - FreeBSD Mailman Cross-site Scripting (XSS) vulnerability in the web UI (3d0eeef8-0cf9-11e8-99b0-d017c2987f9a)

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

Risk Level: Medium

CVE: CVE-2018-5950

Description

The scan detected that the host is missing the following update:
Mailman -- Cross-site scripting (XSS) vulnerability in the web UI (3d0eeef8-0cf9-11e8-99b0-d017c2987f9a)

Observation

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

http://www.vuxml.org/freebsd/3d0eeef8-0cf9-11e8-99b0-d017c2987f9a.html

Affected packages:
mailman < 2.1.26
mailman-with-htdig < 2.1.26
ja-mailman <= 2.1.14.j7_2,1

186091 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3562-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000494

Description

The scan detected that the host is missing the following update:
USN-3562-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004270.html

Ubuntu 16.04

libminiupnpc10_1.9.20140610-2ubuntu2.16.04.2

Ubuntu 14.04

libminiupnpc8_1.6-3ubuntu2.14.04.4

Ubuntu 17.10

libminiupnpc10_1.9.20140610-4ubuntu1.1

186093 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3560-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
USN-3560-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004268.html

Ubuntu 16.04

qemu-system_2.5+dfsg-5ubuntu10.20
qemu-system-s390x_2.5+dfsg-5ubuntu10.20
qemu-system-x86_2.5+dfsg-5ubuntu10.20

Ubuntu 14.04

qemu-system_2.0.0+dfsg-2ubuntu1.38
qemu-system-x86_2.0.0+dfsg-2ubuntu1.38

Ubuntu 17.10

qemu-system-s390x_2.10+dfsg-0ubuntu3.4
qemu-system_2.10+dfsg-0ubuntu3.4
qemu-system-x86_2.10+dfsg-0ubuntu3.4

186096 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3561-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
USN-3561-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004269.html

Ubuntu 16.04

libvirt0_1.3.1-1ubuntu10.17
libvirt-bin_1.3.1-1ubuntu10.17

Ubuntu 14.04

libvirt0_1.2.2-0ubuntu13.1.25
libvirt-bin_1.2.2-0ubuntu13.1.25

Ubuntu 17.10

libvirt0_3.6.0-1ubuntu6.2
libvirt-bin_3.6.0-1ubuntu6.2

23078 - IBM WebSphere Application Server Liberty Information Disclosure Vulnerability (swg22010419)

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

Risk Level: Low

CVE: CVE-2017-1681

Description

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

Observation

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

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

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

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

Risk Level: Low

CVE: CVE-2018-6360

Description

The scan detected that the host is missing the following update:
DSA-4105-1

Observation

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

http://www.debian.org/security/2018/dsa-4105

Debian 9.0
all
mpv_0.23.0-2+deb9u1

131015 - Debian Linux 9.0 DSA-4107-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6596

Description

The scan detected that the host is missing the following update:
DSA-4107-1

Observation

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

http://www.debian.org/security/2018/dsa-4107

Debian 9.0
all
python3-django-anymail_0.8-2+deb9u1
python-django-anymail_0.8-2+deb9u1

131017 - Debian Linux 8.0, 9.0 DSA-4110-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6789

Description

The scan detected that the host is missing the following update:
DSA-4110-1

Observation

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

http://www.debian.org/security/2018/dsa-4110

Debian 8.0
all
exim4_4.84.2-2+deb8u5

Debian 9.0
all
exim4_4.89-2+deb9u3

131018 - Debian Linux 9.0 DSA-4111-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6871

Description

The scan detected that the host is missing the following update:
DSA-4111-1

Observation

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

http://www.debian.org/security/2018/dsa-4111

Debian 9.0
all
libreoffice_1:5.2.7-1+deb9u2

141870 - Red Hat Enterprise Linux RHSA-2018-0316 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12613

Description

The scan detected that the host is missing the following update:
RHSA-2018-0316

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-February/msg00018.html

RHEL6_7S
x86_64
httpd24-apr-debuginfo-1.5.1-1.el6.1
httpd24-apr-1.5.1-1.el6.1
httpd24-apr-devel-1.5.1-1.el6.1

RHEL6S
x86_64
httpd24-apr-debuginfo-1.5.1-1.el6.1
httpd24-apr-1.5.1-1.el6.1
httpd24-apr-devel-1.5.1-1.el6.1

RHEL6WS
x86_64
httpd24-apr-debuginfo-1.5.1-1.el6.1
httpd24-apr-1.5.1-1.el6.1
httpd24-apr-devel-1.5.1-1.el6.1

170923 - Amazon Linux AMI ALAS-2018-947 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15706

Description

The scan detected that the host is missing the following update:
ALAS-2018-947

Observation

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

https://alas.aws.amazon.com/ALAS-2018-947.html

Amazon Linux AMI
noarch
tomcat7-el-2.2-api-7.0.84-1.31.amzn1
tomcat7-servlet-3.0-api-7.0.84-1.31.amzn1
tomcat7-docs-webapp-7.0.84-1.31.amzn1
tomcat7-lib-7.0.84-1.31.amzn1
tomcat7-log4j-7.0.84-1.31.amzn1
tomcat7-jsp-2.2-api-7.0.84-1.31.amzn1
tomcat7-javadoc-7.0.84-1.31.amzn1
tomcat7-webapps-7.0.84-1.31.amzn1
tomcat7-admin-webapps-7.0.84-1.31.amzn1

tomcat7-7.0.84-1.31.amzn1

182595 - FreeBSD libtorrent Remote DoS (e4dd787e-0ea9-11e8-95f2-005056925db4)

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:
libtorrent -- remote DoS (e4dd787e-0ea9-11e8-95f2-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/e4dd787e-0ea9-11e8-95f2-005056925db4.html

Affected packages:
libtorrent < 0.13.6_5

182596 - FreeBSD exim A Buffer Overflow Vulnerability, Remote Code Execution (316b3c3e-0e98-11e8-8d41-97657151f8c2)

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:
exim -- a buffer overflow vulnerability, remote code execution (316b3c3e-0e98-11e8-8d41-97657151f8c2)

Observation

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

http://www.vuxml.org/freebsd/316b3c3e-0e98-11e8-8d41-97657151f8c2.html

Affected packages:
exim < 4.90.1

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

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

Risk Level: Low

CVE: CVE-2018-6360

Description

The scan detected that the host is missing the following update:
mpv -- arbitrary code execution via crafted website (3ee6e521-0d32-11e8-99b0-d017c2987f9a)

Observation

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

http://www.vuxml.org/freebsd/3ee6e521-0d32-11e8-99b0-d017c2987f9a.html

Affected packages:
mpv < 0.27.1

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

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

Risk Level: Low

CVE: CVE-2018-5996

Description

The scan detected that the host is missing the following update:
p7zip-codec-rar -- insufficient error handling (7a2e0063-0e4e-11e8-94c0-5453ed2e2b49)

Observation

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

http://www.vuxml.org/freebsd/7a2e0063-0e4e-11e8-94c0-5453ed2e2b49.html

Affected packages:
p7zip-codec-rar < 16.02_1

182602 - FreeBSD PostgreSQL Vulnerabilities (c602c791-0cf4-11e8-a2ec-6cc21735f730)

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

Risk Level: Low

CVE: CVE-2018-1052, CVE-2018-1053

Description

The scan detected that the host is missing the following update:
PostgreSQL vulnerabilities (c602c791-0cf4-11e8-a2ec-6cc21735f730)

Observation

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

http://www.vuxml.org/freebsd/c602c791-0cf4-11e8-a2ec-6cc21735f730.html

Affected packages:
9.3.0 <= postgresql93-server < 9.3.21
9.4.0 <= postgresql94-server < 9.4.16
9.5.0 <= postgresql95-server < 9.5.11
9.6.0 <= postgresql96-server < 9.6.7
10.0 <= postgresql10-server < 10.2

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

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

Risk Level: Low

CVE: CVE-2017-17969

Description

The scan detected that the host is missing the following update:
p7zip -- heap-based buffer overflow (6d337396-0e4a-11e8-94c0-5453ed2e2b49)

Observation

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

http://www.vuxml.org/freebsd/6d337396-0e4a-11e8-94c0-5453ed2e2b49.html

Affected packages:
p7zip < 16.02_1

182606 - FreeBSD uwsgi A Stack-based Buffer Overflow (a8f25565-109e-11e8-8d41-97657151f8c2)

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

Risk Level: Low

CVE: CVE-2018-6758

Description

The scan detected that the host is missing the following update:
uwsgi -- a stack-based buffer overflow (a8f25565-109e-11e8-8d41-97657151f8c2)

Observation

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

http://www.vuxml.org/freebsd/a8f25565-109e-11e8-8d41-97657151f8c2.html

Affected packages:
uwsgi < 2.0.16

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

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

Risk Level: Low

CVE: CVE-2018-6353

Description

The scan detected that the host is missing the following update:
electrum -- JSONRPC vulnerability (aa743ee4-0f16-11e8-8fd2-10bf48e1088e)

Observation

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

http://www.vuxml.org/freebsd/aa743ee4-0f16-11e8-8fd2-10bf48e1088e.html

Affected packages:
2.6 <= electrum-py36 < 3.0.5
2.6 <= electrum2 < 3.0.5

186089 - Ubuntu Linux 14.04 USN-3567-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-10689

Description

The scan detected that the host is missing the following update:
USN-3567-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004275.html

Ubuntu 14.04

puppet-common_3.4.3-1ubuntu1.3

186092 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3565-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6789

Description

The scan detected that the host is missing the following update:
USN-3565-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004273.html

Ubuntu 16.04

exim4-daemon-light_4.86.2-2ubuntu2.3
exim4-daemon-heavy_4.86.2-2ubuntu2.3

Ubuntu 14.04

exim4-daemon-heavy_4.82-3ubuntu2.4
exim4-daemon-light_4.82-3ubuntu2.4

Ubuntu 17.10

exim4-daemon-light_4.89-5ubuntu1.3
exim4-daemon-heavy_4.89-5ubuntu1.3

186097 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3544-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5089, CVE-2018-5090, CVE-2018-5091, CVE-2018-5092, CVE-2018-5093, CVE-2018-5094, CVE-2018-5095, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5100, CVE-2018-5101, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5105, CVE-2018-5106, CVE-2018-5107, CVE-2018-5108, CVE-2018-5109, CVE-2018-5111, CVE-2018-5112, CVE-2018-

5113, CVE-2018-5114, CVE-2018-5115, CVE-2018-5116, CVE-2018-5117, CVE-2018-5118, CVE-2018-5119, CVE-2018-5122

Description

The scan detected that the host is missing the following update:
USN-3544-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004277.html

Ubuntu 16.04

firefox_58.0.2+build1-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_58.0.2+build1-0ubuntu0.14.04.1

Ubuntu 17.10

firefox_58.0.2+build1-0ubuntu0.17.10.1

193267 - Fedora Linux 26 FEDORA-2018-318b5d74bd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15698

Description

The scan detected that the host is missing the following update:
FEDORA-2018-318b5d74bd

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/2/?count=200&page=1

Fedora Core 26

tomcat-native-1.2.16-1.fc26

193270 - Fedora Linux 27 FEDORA-2018-7b1517bc6e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15698

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7b1517bc6e

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/2/?count=200&page=1

Fedora Core 27

tomcat-native-1.2.16-1.fc27

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.