2018-JAN-17
FSL version 7.5.996

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

22901 - IBM WebSphere Application Server Liberty Profile Apache Commons Vulnerability (swg21970575)

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

Risk Level: High

CVE: CVE-2015-7450

Description

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

Observation

IBM WebSphere Application Server is a Java application server.

A vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile. The flaw lies in the Apache Commons Collections component. Successful exploitation could allow an attacker to execute arbitrary code.

22982 - (HPESBHF03776) HPE Intelligent Management Center Remote Arbitrary File Download Vulnerability

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

Risk Level: High

CVE: CVE-2017-12555

Description

A vulnerability is present in some versions of HPE Intelligent Management Center Service Operation Management.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A vulnerability is present in some versions of HPE Intelligent Management Center Service Operation Management.The flaw lies in some components. Successful exploitation could allow an attacker to remotely download files on the target system and cause an information of disclosure.

146224 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0089-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000408, CVE-2017-1000409, CVE-2017-15670, CVE-2017-15671, CVE-2017-15804, CVE-2017-16997, CVE-2018-1000001

Description

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

openSUSE-SU-2018:0089-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00033.html

SuSE Linux 42.2
i586
glibc-devel-2.22-4.12.1
nscd-2.22-4.12.1
glibc-obsolete-2.22-4.12.1
glibc-utils-2.22-4.12.1
glibc-utils-debugsource-2.22-4.12.1
glibc-devel-static-2.22-4.12.1
glibc-locale-2.22-4.12.1
glibc-2.22-4.12.1
glibc-utils-debuginfo-2.22-4.12.1
glibc-locale-debuginfo-2.22-4.12.1
glibc-devel-debuginfo-2.22-4.12.1
glibc-extra-2.22-4.12.1
glibc-debugsource-2.22-4.12.1
nscd-debuginfo-2.22-4.12.1
glibc-debuginfo-2.22-4.12.1
glibc-profile-2.22-4.12.1
glibc-extra-debuginfo-2.22-4.12.1
glibc-obsolete-debuginfo-2.22-4.12.1

noarch
glibc-info-2.22-4.12.1
glibc-html-2.22-4.12.1
glibc-i18ndata-2.22-4.12.1

x86_64
glibc-devel-2.22-4.12.1
nscd-2.22-4.12.1
glibc-utils-2.22-4.12.1
glibc-utils-debugsource-2.22-4.12.1
glibc-devel-static-2.22-4.12.1
glibc-locale-2.22-4.12.1
glibc-utils-32bit-2.22-4.12.1
glibc-utils-debuginfo-32bit-2.22-4.12.1
glibc-2.22-4.12.1
glibc-utils-debuginfo-2.22-4.12.1
glibc-locale-debuginfo-2.22-4.12.1
glibc-devel-debuginfo-2.22-4.12.1
glibc-extra-2.22-4.12.1
glibc-debugsource-2.22-4.12.1
nscd-debuginfo-2.22-4.12.1
glibc-debuginfo-2.22-4.12.1
glibc-profile-2.22-4.12.1
glibc-extra-debuginfo-2.22-4.12.1

SuSE Linux 42.3
i586
glibc-devel-static-2.22-10.1
glibc-obsolete-2.22-10.1
nscd-2.22-10.1
glibc-debugsource-2.22-10.1

glibc-devel-2.22-10.1
glibc-utils-2.22-10.1
glibc-locale-2.22-10.1
glibc-obsolete-debuginfo-2.22-10.1
glibc-extra-debuginfo-2.22-10.1
glibc-utils-debuginfo-2.22-10.1
glibc-utils-debugsource-2.22-10.1
glibc-2.22-10.1
glibc-locale-debuginfo-2.22-10.1
glibc-devel-debuginfo-2.22-10.1
glibc-debuginfo-2.22-10.1
nscd-debuginfo-2.22-10.1
glibc-profile-2.22-10.1
glibc-extra-2.22-10.1

i686
glibc-locale-2.22-10.1
glibc-debugsource-2.22-10.1
glibc-debuginfo-2.22-10.1
glibc-profile-2.22-10.1
glibc-locale-debuginfo-2.22-10.1
glibc-devel-2.22-10.1
glibc-2.22-10.1
glibc-devel-debuginfo-2.22-10.1
glibc-devel-static-2.22-10.1

noarch
glibc-i18ndata-2.22-10.1
glibc-info-2.22-10.1
glibc-html-2.22-10.1

x86_64
glibc-devel-static-2.22-10.1
glibc-devel-32bit-2.22-10.1
nscd-2.22-10.1
glibc-debugsource-2.22-10.1
glibc-utils-32bit-2.22-10.1
glibc-devel-static-32bit-2.22-10.1
glibc-32bit-2.22-10.1
glibc-devel-2.22-10.1
glibc-locale-32bit-2.22-10.1
glibc-profile-32bit-2.22-10.1
glibc-utils-2.22-10.1
glibc-locale-2.22-10.1
glibc-devel-debuginfo-32bit-2.22-10.1
glibc-utils-debuginfo-32bit-2.22-10.1
glibc-locale-debuginfo-32bit-2.22-10.1
glibc-extra-debuginfo-2.22-10.1
glibc-utils-debuginfo-2.22-10.1
glibc-utils-debugsource-2.22-10.1
glibc-2.22-10.1
glibc-locale-debuginfo-2.22-10.1
glibc-debuginfo-32bit-2.22-10.1
glibc-devel-debuginfo-2.22-10.1
glibc-debuginfo-2.22-10.1
nscd-debuginfo-2.22-10.1
glibc-profile-2.22-10.1
glibc-extra-2.22-10.1

146246 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0074-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000408, CVE-2017-1000409, CVE-2017-15670, CVE-2017-15671, CVE-2017-15804, CVE-2017-16997, CVE-2018-1000001

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0074-1

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-January/003592.html

SuSE SLES 12 SP2
noarch
glibc-info-2.22-62.3.4
glibc-html-2.22-62.3.4
glibc-i18ndata-2.22-62.3.4

x86_64
glibc-locale-32bit-2.22-62.3.4
glibc-debuginfo-32bit-2.22-62.3.4
glibc-devel-debuginfo-2.22-62.3.4
glibc-devel-32bit-2.22-62.3.4
glibc-locale-debuginfo-2.22-62.3.4
glibc-debugsource-2.22-62.3.4
glibc-locale-debuginfo-32bit-2.22-62.3.4
glibc-32bit-2.22-62.3.4
glibc-2.22-62.3.4
glibc-debuginfo-2.22-62.3.4
nscd-2.22-62.3.4
glibc-locale-2.22-62.3.4
nscd-debuginfo-2.22-62.3.4
glibc-devel-2.22-62.3.4
glibc-profile-2.22-62.3.4
glibc-profile-32bit-2.22-62.3.4
glibc-devel-debuginfo-32bit-2.22-62.3.4

SuSE SLED 12 SP3
x86_64
glibc-debuginfo-32bit-2.22-62.3.4
glibc-devel-debuginfo-2.22-62.3.4
glibc-devel-32bit-2.22-62.3.4
nscd-2.22-62.3.4
glibc-locale-debuginfo-2.22-62.3.4
glibc-debugsource-2.22-62.3.4
nscd-debuginfo-2.22-62.3.4
glibc-32bit-2.22-62.3.4
glibc-2.22-62.3.4
glibc-debuginfo-2.22-62.3.4
glibc-locale-debuginfo-32bit-2.22-62.3.4
glibc-locale-2.22-62.3.4
glibc-locale-32bit-2.22-62.3.4
glibc-devel-2.22-62.3.4
glibc-devel-debuginfo-32bit-2.22-62.3.4

noarch
glibc-i18ndata-2.22-62.3.4

SuSE SLED 12 SP2
x86_64
glibc-debuginfo-32bit-2.22-62.3.4
glibc-devel-debuginfo-2.22-62.3.4
glibc-devel-32bit-2.22-62.3.4
nscd-2.22-62.3.4
glibc-locale-debuginfo-2.22-62.3.4
glibc-debugsource-2.22-62.3.4
nscd-debuginfo-2.22-62.3.4
glibc-32bit-2.22-62.3.4
glibc-2.22-62.3.4
glibc-debuginfo-2.22-62.3.4
glibc-locale-debuginfo-32bit-2.22-62.3.4
glibc-locale-2.22-62.3.4
glibc-locale-32bit-2.22-62.3.4
glibc-devel-2.22-62.3.4
glibc-devel-debuginfo-32bit-2.22-62.3.4

noarch
glibc-i18ndata-2.22-62.3.4

SuSE SLES 12 SP3
noarch
glibc-info-2.22-62.3.4
glibc-html-2.22-62.3.4
glibc-i18ndata-2.22-62.3.4

x86_64
glibc-locale-32bit-2.22-62.3.4
glibc-debuginfo-32bit-2.22-62.3.4
glibc-devel-debuginfo-2.22-62.3.4
glibc-devel-32bit-2.22-62.3.4
glibc-locale-debuginfo-2.22-62.3.4
glibc-debugsource-2.22-62.3.4
glibc-locale-debuginfo-32bit-2.22-62.3.4
glibc-32bit-2.22-62.3.4
glibc-2.22-62.3.4
glibc-debuginfo-2.22-62.3.4
nscd-2.22-62.3.4
glibc-locale-2.22-62.3.4
nscd-debuginfo-2.22-62.3.4
glibc-devel-2.22-62.3.4
glibc-profile-2.22-62.3.4
glibc-profile-32bit-2.22-62.3.4
glibc-devel-debuginfo-32bit-2.22-62.3.4

193165 - Fedora Linux 27 FEDORA-2017-01ad8b3946 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15103, CVE-2017-15104

Description

The scan detected that the host is missing the following update:
FEDORA-2017-01ad8b3946

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/2018/1/?count=200&page=3

Fedora Core 27

heketi-5.0.1-1.fc27

193174 - Fedora Linux 26 FEDORA-2017-f7cbe22fd8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15103, CVE-2017-15104

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f7cbe22fd8

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/2018/1/?count=200&page=3

Fedora Core 26

heketi-5.0.1-1.fc26

22942 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52.5.2

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

Risk Level: High

CVE: CVE-2017-7829, CVE-2017-7845, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

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 a malicious user to conduct spoofing attacks and bypass security restrictions, disclose sensitive information, cause a denial of service condition or remotely execute arbitrary code on the target system.

22943 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52.5.2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-7829, CVE-2017-7845, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

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 a malicious user to conduct spoofing attacks and bypass security restrictions, disclose sensitive information, cause a denial of service condition or remotely execute arbitrary code on the target system.

22993 - Oracle Java SE Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2581, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2627, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2638, CVE-2018-2639, CVE-2018-2641, CVE-2018-2657, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

Multiple vulnerabilities are present in some versions of Oracle Java SE.

Observation

Oracle Java SE is used to run Java applications.

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

22868 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.5.2 (CVE-2017-7845)

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

Risk Level: High

CVE: CVE-2017-7845

Description

A vulnerability is present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox ESR. The flaw lies in the graphics processing component. Successful exploitation could allow an attacker to cause a denial of service condition.

22977 - (VMSA-2017-0021) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4933, CVE-2017-4941

Description

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

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of WMware Workstation Player. The flaws are related with VNC packet handling. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

22978 - (VMSA-2017-0021) VMware Workstation Player Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4933, CVE-2017-4941

Description

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

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of WMware Workstation Player. The flaws are related with VNC packet handling. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

146225 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0096-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0096-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00040.html

SuSE Linux 42.2
x86_64
gifsicle-1.91-2.3.1
gifsicle-debuginfo-1.91-2.3.1
gifsicle-debugsource-1.91-2.3.1

i586
gifsicle-1.91-2.3.1
gifsicle-debuginfo-1.91-2.3.1
gifsicle-debugsource-1.91-2.3.1

SuSE Linux 42.3
x86_64
gifsicle-1.91-5.1
gifsicle-debuginfo-1.91-5.1
gifsicle-debugsource-1.91-5.1

i586

gifsicle-1.91-5.1
gifsicle-debuginfo-1.91-5.1
gifsicle-debugsource-1.91-5.1

146227 - SuSE Linux 42.2 openSUSE-SU-2018:0063-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0063-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00023.html

SuSE Linux 42.2
noarch
clamav-database-201801080006-54.127.1

146228 - SuSE SLES 11 SP4 SUSE-SU-2018:0075-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000001

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0075-1

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-January/003593.html

SuSE SLES 11 SP4
i686
glibc-2.11.3-17.110.3.1
glibc-devel-2.11.3-17.110.3.1

i586
glibc-i18ndata-2.11.3-17.110.3.1
glibc-2.11.3-17.110.3.1
nscd-2.11.3-17.110.3.1
glibc-devel-2.11.3-17.110.3.1
glibc-info-2.11.3-17.110.3.1
glibc-locale-2.11.3-17.110.3.1
glibc-profile-2.11.3-17.110.3.1
glibc-html-2.11.3-17.110.3.1

x86_64

glibc-i18ndata-2.11.3-17.110.3.1
glibc-devel-32bit-2.11.3-17.110.3.1
glibc-2.11.3-17.110.3.1
nscd-2.11.3-17.110.3.1
glibc-devel-2.11.3-17.110.3.1
glibc-32bit-2.11.3-17.110.3.1
glibc-info-2.11.3-17.110.3.1
glibc-locale-32bit-2.11.3-17.110.3.1
glibc-locale-2.11.3-17.110.3.1
glibc-profile-2.11.3-17.110.3.1
glibc-html-2.11.3-17.110.3.1
glibc-profile-32bit-2.11.3-17.110.3.1

146229 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0095-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15098

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0095-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00039.html

SuSE Linux 42.2
i586
postgresql94-server-9.4.15-9.12.1
postgresql94-test-9.4.15-9.12.1
postgresql94-plperl-debuginfo-9.4.15-9.12.1
postgresql94-libs-debugsource-9.4.15-9.12.1
postgresql94-contrib-debuginfo-9.4.15-9.12.1
postgresql94-plperl-9.4.15-9.12.1
postgresql94-debugsource-9.4.15-9.12.1
postgresql94-server-debuginfo-9.4.15-9.12.1
postgresql94-devel-9.4.15-9.12.1
postgresql94-pltcl-debuginfo-9.4.15-9.12.1
postgresql94-debuginfo-9.4.15-9.12.1
postgresql94-devel-debuginfo-9.4.15-9.12.1
postgresql94-pltcl-9.4.15-9.12.1
postgresql94-plpython-9.4.15-9.12.1
postgresql94-contrib-9.4.15-9.12.1
postgresql94-plpython-debuginfo-9.4.15-9.12.1
postgresql94-9.4.15-9.12.1

noarch
postgresql94-docs-9.4.15-9.12.1

x86_64
postgresql94-server-9.4.15-9.12.1
postgresql94-test-9.4.15-9.12.1
postgresql94-plperl-debuginfo-9.4.15-9.12.1
postgresql94-libs-debugsource-9.4.15-9.12.1
postgresql94-contrib-debuginfo-9.4.15-9.12.1

postgresql94-plperl-9.4.15-9.12.1
postgresql94-debugsource-9.4.15-9.12.1
postgresql94-server-debuginfo-9.4.15-9.12.1
postgresql94-devel-9.4.15-9.12.1
postgresql94-pltcl-debuginfo-9.4.15-9.12.1
postgresql94-debuginfo-9.4.15-9.12.1
postgresql94-devel-debuginfo-9.4.15-9.12.1
postgresql94-pltcl-9.4.15-9.12.1
postgresql94-plpython-9.4.15-9.12.1
postgresql94-contrib-9.4.15-9.12.1
postgresql94-plpython-debuginfo-9.4.15-9.12.1
postgresql94-9.4.15-9.12.1

SuSE Linux 42.3
i586
postgresql94-server-9.4.15-15.1
postgresql94-debugsource-9.4.15-15.1
postgresql94-server-debuginfo-9.4.15-15.1
postgresql94-devel-9.4.15-15.1
postgresql94-pltcl-9.4.15-15.1
postgresql94-pltcl-debuginfo-9.4.15-15.1
postgresql94-libs-debugsource-9.4.15-15.1
postgresql94-plpython-9.4.15-15.1
postgresql94-plperl-debuginfo-9.4.15-15.1
postgresql94-9.4.15-15.1
postgresql94-contrib-debuginfo-9.4.15-15.1
postgresql94-test-9.4.15-15.1
postgresql94-plpython-debuginfo-9.4.15-15.1
postgresql94-debuginfo-9.4.15-15.1
postgresql94-plperl-9.4.15-15.1
postgresql94-devel-debuginfo-9.4.15-15.1
postgresql94-contrib-9.4.15-15.1

noarch
postgresql94-docs-9.4.15-15.1

x86_64
postgresql94-server-9.4.15-15.1
postgresql94-debugsource-9.4.15-15.1
postgresql94-server-debuginfo-9.4.15-15.1
postgresql94-devel-9.4.15-15.1
postgresql94-pltcl-9.4.15-15.1
postgresql94-pltcl-debuginfo-9.4.15-15.1
postgresql94-libs-debugsource-9.4.15-15.1
postgresql94-plpython-9.4.15-15.1
postgresql94-plperl-debuginfo-9.4.15-15.1
postgresql94-9.4.15-15.1
postgresql94-contrib-debuginfo-9.4.15-15.1
postgresql94-test-9.4.15-15.1
postgresql94-plpython-debuginfo-9.4.15-15.1
postgresql94-debuginfo-9.4.15-15.1
postgresql94-plperl-9.4.15-15.1
postgresql94-devel-debuginfo-9.4.15-15.1
postgresql94-contrib-9.4.15-15.1

146230 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0101-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9512, CVE-2017-16548, CVE-2017-17433, CVE-2017-17434

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0101-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00044.html

SuSE Linux 42.2
x86_64
rsync-3.1.0-7.3.1
rsync-debuginfo-3.1.0-7.3.1
rsync-debugsource-3.1.0-7.3.1

i586
rsync-3.1.0-7.3.1
rsync-debuginfo-3.1.0-7.3.1
rsync-debugsource-3.1.0-7.3.1

SuSE Linux 42.3
x86_64
rsync-3.1.0-10.1
rsync-debuginfo-3.1.0-10.1
rsync-debugsource-3.1.0-10.1

i586
rsync-3.1.0-10.1
rsync-debuginfo-3.1.0-10.1
rsync-debugsource-3.1.0-10.1

146232 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0081-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15098

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0081-1

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-January/003597.html

SuSE SLED 12 SP2
x86_64
postgresql94-debugsource-9.4.15-21.13.1
postgresql94-debuginfo-9.4.15-21.13.1
postgresql94-9.4.15-21.13.1

SuSE SLES 12 SP2

noarch
postgresql94-docs-9.4.15-21.13.1

x86_64
postgresql94-server-debuginfo-9.4.15-21.13.1
postgresql94-9.4.15-21.13.1
postgresql94-contrib-9.4.15-21.13.1
postgresql94-debuginfo-9.4.15-21.13.1
postgresql94-debugsource-9.4.15-21.13.1
postgresql94-contrib-debuginfo-9.4.15-21.13.1
postgresql94-server-9.4.15-21.13.1

146233 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0094-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7542

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0094-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00038.html

SuSE Linux 42.2
i586
gwenhywfar-debugsource-4.9.0beta-8.3.1
libgwenhywfar60-plugins-4.9.0beta-8.3.1
libgwenhywfar60-plugins-debuginfo-4.9.0beta-8.3.1
libgwenhywfar60-4.9.0beta-8.3.1
libgwenhywfar60-debuginfo-4.9.0beta-8.3.1
libgwengui-gtk2-0-4.9.0beta-8.3.1
gwenhywfar-tools-debuginfo-4.9.0beta-8.3.1
gwenhywfar-tools-4.9.0beta-8.3.1
gwenhywfar-devel-4.9.0beta-8.3.1
libgwengui-qt4-0-4.9.0beta-8.3.1
libgwengui-qt4-0-debuginfo-4.9.0beta-8.3.1
libgwengui-gtk2-0-debuginfo-4.9.0beta-8.3.1

noarch
gwenhywfar-lang-4.9.0beta-8.3.1

x86_64
gwenhywfar-debugsource-4.9.0beta-8.3.1
libgwenhywfar60-plugins-4.9.0beta-8.3.1
libgwenhywfar60-plugins-debuginfo-4.9.0beta-8.3.1
libgwenhywfar60-4.9.0beta-8.3.1
libgwenhywfar60-debuginfo-4.9.0beta-8.3.1
libgwengui-gtk2-0-4.9.0beta-8.3.1
gwenhywfar-tools-debuginfo-4.9.0beta-8.3.1
gwenhywfar-tools-4.9.0beta-8.3.1
gwenhywfar-devel-4.9.0beta-8.3.1
libgwengui-qt4-0-4.9.0beta-8.3.1
libgwengui-qt4-0-debuginfo-4.9.0beta-8.3.1

libgwengui-gtk2-0-debuginfo-4.9.0beta-8.3.1

SuSE Linux 42.3
i586
libgwenhywfar60-plugins-debuginfo-4.9.0beta-11.1
gwenhywfar-debugsource-4.9.0beta-11.1
libgwengui-qt4-0-debuginfo-4.9.0beta-11.1
libgwengui-gtk2-0-debuginfo-4.9.0beta-11.1
gwenhywfar-devel-4.9.0beta-11.1
libgwengui-gtk2-0-4.9.0beta-11.1
libgwengui-qt4-0-4.9.0beta-11.1
libgwenhywfar60-4.9.0beta-11.1
libgwenhywfar60-debuginfo-4.9.0beta-11.1
gwenhywfar-tools-4.9.0beta-11.1
gwenhywfar-tools-debuginfo-4.9.0beta-11.1
libgwenhywfar60-plugins-4.9.0beta-11.1

noarch
gwenhywfar-lang-4.9.0beta-11.1

x86_64
libgwenhywfar60-plugins-debuginfo-4.9.0beta-11.1
gwenhywfar-debugsource-4.9.0beta-11.1
libgwengui-qt4-0-debuginfo-4.9.0beta-11.1
libgwengui-gtk2-0-debuginfo-4.9.0beta-11.1
gwenhywfar-devel-4.9.0beta-11.1
libgwengui-gtk2-0-4.9.0beta-11.1
libgwengui-qt4-0-4.9.0beta-11.1
libgwenhywfar60-4.9.0beta-11.1
libgwenhywfar60-debuginfo-4.9.0beta-11.1
gwenhywfar-tools-4.9.0beta-11.1
gwenhywfar-tools-debuginfo-4.9.0beta-11.1
libgwenhywfar60-plugins-4.9.0beta-11.1

146234 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0100-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4912, CVE-2016-7567

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0100-1

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-January/003598.html

SuSE SLED 12 SP2
x86_64
openslp-2.0.0-18.2.1
openslp-debugsource-2.0.0-18.2.1
openslp-debuginfo-32bit-2.0.0-18.2.1
openslp-32bit-2.0.0-18.2.1
openslp-debuginfo-2.0.0-18.2.1

SuSE SLES 12 SP2
x86_64
openslp-debugsource-2.0.0-18.2.1
openslp-server-debuginfo-2.0.0-18.2.1
openslp-server-2.0.0-18.2.1
openslp-debuginfo-32bit-2.0.0-18.2.1
openslp-32bit-2.0.0-18.2.1
openslp-2.0.0-18.2.1
openslp-debuginfo-2.0.0-18.2.1

146236 - SuSE SLES 11 SP4 SUSE-SU-2018:0077-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15098

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0077-1

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-January/003595.html

SuSE SLES 11 SP4
i586
postgresql94-server-9.4.15-0.23.10.1
libecpg6-9.4.15-0.23.10.1
postgresql94-docs-9.4.15-0.23.10.1
libpq5-9.4.15-0.23.10.1
postgresql94-9.4.15-0.23.10.1
postgresql94-contrib-9.4.15-0.23.10.1

x86_64
postgresql94-server-9.4.15-0.23.10.1
libpq5-32bit-9.4.15-0.23.10.1
libecpg6-9.4.15-0.23.10.1
postgresql94-docs-9.4.15-0.23.10.1
libpq5-9.4.15-0.23.10.1
postgresql94-9.4.15-0.23.10.1
postgresql94-contrib-9.4.15-0.23.10.1

146238 - SuSE Linux 42.3 openSUSE-SU-2018:0060-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0359

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0060-1

Observation

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

For more information see:

http://lists.opensuse.org/opensuse-updates/2018-01/msg00021.html

SuSE Linux 42.3
noarch
diffoscope-85-3.1

146239 - SuSE SLED 12 SP2, 12 SP3 SUSE-SU-2018:0072-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7542

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0072-1

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-January/003590.html

SuSE SLED 12 SP3
x86_64
gwenhywfar-tools-4.9.0beta-3.3.1
libgwenhywfar60-debuginfo-4.9.0beta-3.3.1
libgwengui-gtk2-0-4.9.0beta-3.3.1
libgwenhywfar60-4.9.0beta-3.3.1
libgwengui-gtk2-0-debuginfo-4.9.0beta-3.3.1
gwenhywfar-debugsource-4.9.0beta-3.3.1
libgwenhywfar60-plugins-4.9.0beta-3.3.1
libgwenhywfar60-plugins-debuginfo-4.9.0beta-3.3.1
gwenhywfar-tools-debuginfo-4.9.0beta-3.3.1

noarch
gwenhywfar-lang-4.9.0beta-3.3.1

SuSE SLED 12 SP2
x86_64
gwenhywfar-tools-4.9.0beta-3.3.1
libgwenhywfar60-debuginfo-4.9.0beta-3.3.1
libgwengui-gtk2-0-4.9.0beta-3.3.1
libgwenhywfar60-4.9.0beta-3.3.1
libgwengui-gtk2-0-debuginfo-4.9.0beta-3.3.1
gwenhywfar-debugsource-4.9.0beta-3.3.1
libgwenhywfar60-plugins-4.9.0beta-3.3.1
libgwenhywfar60-plugins-debuginfo-4.9.0beta-3.3.1
gwenhywfar-tools-debuginfo-4.9.0beta-3.3.1

noarch
gwenhywfar-lang-4.9.0beta-3.3.1

146240 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0092-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000445, CVE-2017-1000476, CVE-2017-11449, CVE-2017-11751, CVE-2017-12430, CVE-2017-12642, CVE-2017-14249, CVE-2017-17680, CVE-2017-17882, CVE-2017-9409

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0092-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00036.html

SuSE Linux 42.2
i586
ImageMagick-extra-6.8.8.1-30.18.1
perl-PerlMagick-debuginfo-6.8.8.1-30.18.1
perl-PerlMagick-6.8.8.1-30.18.1
libMagickCore-6_Q16-1-6.8.8.1-30.18.1
libMagick++-devel-6.8.8.1-30.18.1
ImageMagick-debuginfo-6.8.8.1-30.18.1
ImageMagick-extra-debuginfo-6.8.8.1-30.18.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.18.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.18.1
ImageMagick-devel-6.8.8.1-30.18.1
libMagickWand-6_Q16-1-6.8.8.1-30.18.1
ImageMagick-6.8.8.1-30.18.1
ImageMagick-debugsource-6.8.8.1-30.18.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.18.1
libMagick++-6_Q16-3-6.8.8.1-30.18.1

noarch
ImageMagick-doc-6.8.8.1-30.18.1

x86_64
libMagickWand-6_Q16-1-32bit-6.8.8.1-30.18.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-30.18.1
ImageMagick-extra-6.8.8.1-30.18.1
perl-PerlMagick-debuginfo-6.8.8.1-30.18.1
ImageMagick-devel-32bit-6.8.8.1-30.18.1
perl-PerlMagick-6.8.8.1-30.18.1
libMagick++-6_Q16-3-32bit-6.8.8.1-30.18.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-30.18.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-30.18.1
libMagickCore-6_Q16-1-6.8.8.1-30.18.1
libMagick++-devel-6.8.8.1-30.18.1
ImageMagick-debuginfo-6.8.8.1-30.18.1
ImageMagick-extra-debuginfo-6.8.8.1-30.18.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.18.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.18.1
ImageMagick-devel-6.8.8.1-30.18.1
libMagickWand-6_Q16-1-6.8.8.1-30.18.1
ImageMagick-6.8.8.1-30.18.1
ImageMagick-debugsource-6.8.8.1-30.18.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.18.1
libMagick++-6_Q16-3-6.8.8.1-30.18.1
libMagick++-devel-32bit-6.8.8.1-30.18.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-30.18.1

SuSE Linux 42.3
i586
libMagickCore-6_Q16-1-6.8.8.1-46.1
ImageMagick-debugsource-6.8.8.1-46.1
libMagick++-6_Q16-3-6.8.8.1-46.1
libMagick++-devel-6.8.8.1-46.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-46.1
libMagickWand-6_Q16-1-6.8.8.1-46.1
ImageMagick-extra-debuginfo-6.8.8.1-46.1
ImageMagick-6.8.8.1-46.1
perl-PerlMagick-debuginfo-6.8.8.1-46.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-46.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-46.1
perl-PerlMagick-6.8.8.1-46.1
ImageMagick-devel-6.8.8.1-46.1
ImageMagick-extra-6.8.8.1-46.1
ImageMagick-debuginfo-6.8.8.1-46.1

noarch
ImageMagick-doc-6.8.8.1-46.1

x86_64
ImageMagick-devel-32bit-6.8.8.1-46.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-46.1
libMagickCore-6_Q16-1-6.8.8.1-46.1
ImageMagick-debugsource-6.8.8.1-46.1
libMagick++-6_Q16-3-6.8.8.1-46.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-46.1
libMagick++-6_Q16-3-32bit-6.8.8.1-46.1
libMagick++-devel-6.8.8.1-46.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-46.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-46.1
libMagickWand-6_Q16-1-6.8.8.1-46.1
ImageMagick-extra-debuginfo-6.8.8.1-46.1
ImageMagick-6.8.8.1-46.1
perl-PerlMagick-debuginfo-6.8.8.1-46.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-46.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-46.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-46.1
perl-PerlMagick-6.8.8.1-46.1
libMagick++-devel-32bit-6.8.8.1-46.1
ImageMagick-devel-6.8.8.1-46.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-46.1
ImageMagick-extra-6.8.8.1-46.1
ImageMagick-debuginfo-6.8.8.1-46.1

146248 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0098-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7700

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0098-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00042.html

SuSE Linux 42.2
x86_64
pngcrush-debugsource-1.7.85-5.3.1
pngcrush-debuginfo-1.7.85-5.3.1
pngcrush-1.7.85-5.3.1

i586
pngcrush-debugsource-1.7.85-5.3.1
pngcrush-debuginfo-1.7.85-5.3.1
pngcrush-1.7.85-5.3.1

SuSE Linux 42.3
x86_64
pngcrush-debugsource-1.7.85-8.1
pngcrush-debuginfo-1.7.85-8.1
pngcrush-1.7.85-8.1

i586
pngcrush-debugsource-1.7.85-8.1
pngcrush-debuginfo-1.7.85-8.1
pngcrush-1.7.85-8.1

146252 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0073-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8128, CVE-2015-7554, CVE-2016-10095, CVE-2016-5318, CVE-2017-16232

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0073-1

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-January/003591.html

SuSE SLES 12 SP2
x86_64
libtiff5-32bit-4.0.9-44.7.1
tiff-4.0.9-44.7.1
tiff-debugsource-4.0.9-44.7.1
libtiff5-debuginfo-32bit-4.0.9-44.7.1
libtiff5-4.0.9-44.7.1
libtiff5-debuginfo-4.0.9-44.7.1
tiff-debuginfo-4.0.9-44.7.1

SuSE SLED 12 SP3
x86_64
libtiff5-32bit-4.0.9-44.7.1
tiff-debugsource-4.0.9-44.7.1
libtiff5-debuginfo-32bit-4.0.9-44.7.1

libtiff5-4.0.9-44.7.1
libtiff5-debuginfo-4.0.9-44.7.1
tiff-debuginfo-4.0.9-44.7.1

SuSE SLED 12 SP2
x86_64
libtiff5-32bit-4.0.9-44.7.1
tiff-debugsource-4.0.9-44.7.1
libtiff5-debuginfo-32bit-4.0.9-44.7.1
libtiff5-4.0.9-44.7.1
libtiff5-debuginfo-4.0.9-44.7.1
tiff-debuginfo-4.0.9-44.7.1

SuSE SLES 12 SP3
x86_64
libtiff5-32bit-4.0.9-44.7.1
tiff-4.0.9-44.7.1
tiff-debugsource-4.0.9-44.7.1
libtiff5-debuginfo-32bit-4.0.9-44.7.1
libtiff5-4.0.9-44.7.1
libtiff5-debuginfo-4.0.9-44.7.1
tiff-debuginfo-4.0.9-44.7.1

146253 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0097-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8128, CVE-2015-7554, CVE-2016-10095, CVE-2016-5318, CVE-2017-16232

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0097-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00041.html

SuSE Linux 42.2
x86_64
libtiff-devel-32bit-4.0.9-17.9.1
libtiff5-debuginfo-4.0.9-17.9.1
tiff-4.0.9-17.9.1
libtiff-devel-4.0.9-17.9.1
libtiff5-debuginfo-32bit-4.0.9-17.9.1
libtiff5-32bit-4.0.9-17.9.1
libtiff5-4.0.9-17.9.1
tiff-debuginfo-4.0.9-17.9.1
tiff-debugsource-4.0.9-17.9.1

i586
libtiff5-debuginfo-4.0.9-17.9.1
tiff-4.0.9-17.9.1
libtiff-devel-4.0.9-17.9.1
libtiff5-4.0.9-17.9.1
tiff-debuginfo-4.0.9-17.9.1
tiff-debugsource-4.0.9-17.9.1

SuSE Linux 42.3
x86_64
tiff-4.0.9-24.1
libtiff5-32bit-4.0.9-24.1
tiff-debuginfo-4.0.9-24.1
libtiff5-debuginfo-4.0.9-24.1
libtiff-devel-4.0.9-24.1
tiff-debugsource-4.0.9-24.1
libtiff-devel-32bit-4.0.9-24.1
libtiff5-4.0.9-24.1
libtiff5-debuginfo-32bit-4.0.9-24.1

i586
tiff-4.0.9-24.1
tiff-debuginfo-4.0.9-24.1
libtiff5-debuginfo-4.0.9-24.1
libtiff-devel-4.0.9-24.1
tiff-debugsource-4.0.9-24.1
libtiff5-4.0.9-24.1

178574 - Gentoo Linux GLSA-201801-14 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-201801-14

Observation

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

https://security.gentoo.org/glsa/201801-14

Affected packages:
app-emulation/xen < 4.9.1-r1
app-emulation/xen-tools < 4.9.1-r1

186040 - Ubuntu Linux 17.10 USN-3523-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16995, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864

Description

The scan detected that the host is missing the following update:
USN-3523-3

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004220.html

Ubuntu 17.10

linux-image-raspi2_4.13.0.1011.9
linux-image-4.13.0-1011-raspi2_4.13.0-1011.11

186044 - Ubuntu Linux 16.04 USN-3523-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16995, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3523-2

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-January/004219.html

Ubuntu 16.04

linux-image-4.13.0-1015-oem_4.13.0-1015.16
linux-image-4.13.0-1006-gcp_4.13.0-1006.9
linux-image-generic-lpae-hwe-16.04_4.13.0.26.46
linux-image-4.13.0-26-lowlatency_4.13.0-26.29~16.04.2
linux-image-generic-hwe-16.04_4.13.0.26.46
linux-image-oem_4.13.0.1015.18
linux-image-4.13.0-26-generic-lpae_4.13.0-26.29~16.04.2
linux-image-lowlatency-hwe-16.04_4.13.0.26.46
linux-image-4.13.0-1005-azure_4.13.0-1005.7
linux-image-4.13.0-26-generic_4.13.0-26.29~16.04.2
linux-image-gcp_4.13.0.1006.8
linux-image-azure_4.13.0.1005.6
linux-image-gke_4.13.0.1006.8

193173 - Fedora Linux 27 FEDORA-2018-7edfa0cfbf Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000501

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7edfa0cfbf

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/2018/1/?count=200&page=3

Fedora Core 27

awstats-7.6-8.fc27

193179 - Fedora Linux 26 FEDORA-2018-17ba1a2393 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000501

Description

The scan detected that the host is missing the following update:
FEDORA-2018-17ba1a2393

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/2018/1/?count=200&page=2

Fedora Core 26

awstats-7.6-4.fc26

22975 - (VMSA-2018-0003) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4945, CVE-2017-4948

Description

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

Observation

VMware Workstation is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Pro. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose sensitive information or may cause a Denial of Service.

146231 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0087-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10800, CVE-2017-11449, CVE-2017-11532, CVE-2017-12564, CVE-2017-12670, CVE-2017-12672, CVE-2017-12675, CVE-2017-13060, CVE-2017-13648, CVE-2017-14326, CVE-2017-16547, CVE-2017-17881, CVE-2017-18022

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0087-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00031.html

SuSE Linux 42.2
x86_64
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.60.1
GraphicsMagick-debugsource-1.3.25-11.60.1
GraphicsMagick-1.3.25-11.60.1
perl-GraphicsMagick-debuginfo-1.3.25-11.60.1
libGraphicsMagick3-config-1.3.25-11.60.1
GraphicsMagick-devel-1.3.25-11.60.1
GraphicsMagick-debuginfo-1.3.25-11.60.1
libGraphicsMagick++-Q16-12-1.3.25-11.60.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.60.1
libGraphicsMagick++-devel-1.3.25-11.60.1
libGraphicsMagickWand-Q16-2-1.3.25-11.60.1
perl-GraphicsMagick-1.3.25-11.60.1
libGraphicsMagick-Q16-3-1.3.25-11.60.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.60.1

i586
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.60.1
GraphicsMagick-debugsource-1.3.25-11.60.1
GraphicsMagick-1.3.25-11.60.1
perl-GraphicsMagick-debuginfo-1.3.25-11.60.1
libGraphicsMagick3-config-1.3.25-11.60.1
GraphicsMagick-devel-1.3.25-11.60.1
GraphicsMagick-debuginfo-1.3.25-11.60.1
libGraphicsMagick++-Q16-12-1.3.25-11.60.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.60.1
libGraphicsMagick++-devel-1.3.25-11.60.1
libGraphicsMagickWand-Q16-2-1.3.25-11.60.1
perl-GraphicsMagick-1.3.25-11.60.1
libGraphicsMagick-Q16-3-1.3.25-11.60.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.60.1

SuSE Linux 42.3
x86_64
GraphicsMagick-debuginfo-1.3.25-57.1
libGraphicsMagickWand-Q16-2-1.3.25-57.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-57.1
libGraphicsMagick-Q16-3-1.3.25-57.1
GraphicsMagick-devel-1.3.25-57.1
libGraphicsMagick++-Q16-12-1.3.25-57.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-57.1
libGraphicsMagick++-devel-1.3.25-57.1
perl-GraphicsMagick-debuginfo-1.3.25-57.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-57.1
GraphicsMagick-1.3.25-57.1
libGraphicsMagick3-config-1.3.25-57.1
GraphicsMagick-debugsource-1.3.25-57.1
perl-GraphicsMagick-1.3.25-57.1

i586
GraphicsMagick-debuginfo-1.3.25-57.1
libGraphicsMagickWand-Q16-2-1.3.25-57.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-57.1
libGraphicsMagick-Q16-3-1.3.25-57.1
GraphicsMagick-devel-1.3.25-57.1
libGraphicsMagick++-Q16-12-1.3.25-57.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-57.1

libGraphicsMagick++-devel-1.3.25-57.1
perl-GraphicsMagick-debuginfo-1.3.25-57.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-57.1
GraphicsMagick-1.3.25-57.1
libGraphicsMagick3-config-1.3.25-57.1
GraphicsMagick-debugsource-1.3.25-57.1
perl-GraphicsMagick-1.3.25-57.1

146243 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0109-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000420

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0109-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00046.html

SuSE Linux 42.2
x86_64
syncthing-0.14.42-7.3.1

i586
syncthing-0.14.42-7.3.1

SuSE Linux 42.3
x86_64
syncthing-0.14.42-3.1

i586
syncthing-0.14.42-3.1

22869 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.5.2 (CVE-2017-7843)

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

Risk Level: Medium

CVE: CVE-2017-7843

Description

A vulnerability is present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox ESR. The flaw occurs when When Private Browsing mode is used. Successful exploitation could allow an attacker to bypass security restrictions and perform unauthorized actions.

22870 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.5.2 (CVE-2017-7843)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-7843

Description

A vulnerability is present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox ESR. The flaw occurs when When Private Browsing mode is used. Successful exploitation could allow an attacker to bypass security restrictions and perform unauthorized actions.

22981 - (VMSA-2018-0002) VMware Fusion Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of VMware Fusion.

Observation

VMware Fusion is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware Fusion. The flaws lie in the CPU feature known as Speculative Execution. Successful exploitation could allow an attacker to obtain sensitive information.

22984 - (HT208401) Apple iOS Multiple Vulnerabilities Prior To 11.2.2

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

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

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information.

22986 - (VMSA-2018-0003) VMware Horizon View Client Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-4948

Description

A vulnerability is present in some versions of VMWare Horizon View Client.

Observation

VMware Horizon View Client is VMWare desktop-virtualization product.

A vulnerability is present in some versions of VMWare Horizon View Client. The flaw lies in TPView.dll. Successful exploitation could allow an attacker to disclose private information or cause a denial of service condition on the Windows OS running VMware Horizon View Client.

22992 - Wireshark Multiple Vulnerabilities Prior To 2.2.12

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

Risk Level: Medium

CVE: CVE-2017-17997, CVE-2018-5334, CVE-2018-5335, CVE-2018-5336

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

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

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

141838 - Red Hat Enterprise Linux RHSA-2018-0081 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11305, CVE-2018-4871

Description

The scan detected that the host is missing the following update:
RHSA-2018-0081

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00054.html

RHEL6D
x86_64
flash-plugin-28.0.0.137-1.el6_9

i386
flash-plugin-28.0.0.137-1.el6_9

RHEL6S
x86_64
flash-plugin-28.0.0.137-1.el6_9

i386
flash-plugin-28.0.0.137-1.el6_9

RHEL6WS
x86_64

flash-plugin-28.0.0.137-1.el6_9

i386
flash-plugin-28.0.0.137-1.el6_9

146241 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0108-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5992

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0108-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00045.html

SuSE Linux 42.2
noarch
python-openpyxl-2.2.2-4.5.1

SuSE Linux 42.3
noarch
python-openpyxl-2.2.2-7.1

146247 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0099-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8825

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0099-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00043.html

SuSE Linux 42.2
x86_64
libetpan17-debuginfo-1.6-5.3.1
libetpan-devel-1.6-5.3.1
libetpan17-1.6-5.3.1
libetpan-debugsource-1.6-5.3.1

i586
libetpan17-debuginfo-1.6-5.3.1
libetpan-devel-1.6-5.3.1
libetpan17-1.6-5.3.1

libetpan-debugsource-1.6-5.3.1

SuSE Linux 42.3
x86_64
libetpan-debugsource-1.6-8.1
libetpan17-1.6-8.1
libetpan-devel-1.6-8.1
libetpan17-debuginfo-1.6-8.1

i586
libetpan-debugsource-1.6-8.1
libetpan17-1.6-8.1
libetpan-devel-1.6-8.1
libetpan17-debuginfo-1.6-8.1

146249 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0090-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17997, CVE-2018-5334, CVE-2018-5335, CVE-2018-5336

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0090-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00034.html

SuSE Linux 42.2
x86_64
wireshark-ui-gtk-2.2.12-14.24.1
wireshark-ui-qt-debuginfo-2.2.12-14.24.1
wireshark-2.2.12-14.24.1
wireshark-ui-gtk-debuginfo-2.2.12-14.24.1
wireshark-devel-2.2.12-14.24.1
wireshark-ui-qt-2.2.12-14.24.1
wireshark-debuginfo-2.2.12-14.24.1
wireshark-debugsource-2.2.12-14.24.1

SuSE Linux 42.3
x86_64
wireshark-2.2.12-32.1
wireshark-devel-2.2.12-32.1
wireshark-debugsource-2.2.12-32.1
wireshark-debuginfo-2.2.12-32.1
wireshark-ui-gtk-debuginfo-2.2.12-32.1
wireshark-ui-gtk-2.2.12-32.1
wireshark-ui-qt-debuginfo-2.2.12-32.1
wireshark-ui-qt-2.2.12-32.1

178575 - Gentoo Linux GLSA-201801-13 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201801-13

Observation

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

https://security.gentoo.org/glsa/201801-13

Affected packages:
net-misc/tigervnc < 1.8.0

178576 - Gentoo Linux GLSA-201801-12 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201801-12

Observation

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

https://security.gentoo.org/glsa/201801-12

Affected packages:
media-gfx/icoutils < 0.32.0

178577 - Gentoo Linux GLSA-201801-15 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201801-15

Observation

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

https://security.gentoo.org/glsa/201801-15

Affected packages:
net-libs/polarssl < 1.3.9-r1

178578 - Gentoo Linux GLSA-201801-16 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-201801-16

Observation

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

https://security.gentoo.org/glsa/201801-16

Affected packages:
net-misc/rsync < 3.1.2-r2

193178 - Fedora Linux 26 FEDORA-2018-48569250d1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17810, CVE-2017-17811, CVE-2017-17812, CVE-2017-17813, CVE-2017-17814, CVE-2017-17815, CVE-2017-17816, CVE-2017-17817, CVE-2017-17818, CVE-2017-17819, CVE-2017-17820

Description

The scan detected that the host is missing the following update:
FEDORA-2018-48569250d1

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/2018/1/?count=200&page=2

Fedora Core 26

nasm-2.13.02-1.fc26

193186 - Fedora Linux 27 FEDORA-2018-b1f3217ae6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17810, CVE-2017-17811, CVE-2017-17812, CVE-2017-17813, CVE-2017-17814, CVE-2017-17815, CVE-2017-17816, CVE-2017-17817, CVE-2017-17818, CVE-2017-17819, CVE-2017-17820

Description

The scan detected that the host is missing the following update:
FEDORA-2018-b1f3217ae6

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/2018/1/?count=200&page=2

Fedora Core 27

nasm-2.13.02-1.fc27

22895 - Pivotal RabbitMQ Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4965, CVE-2017-4966, CVE-2017-4967

Description

Multiple vulnerabilities are present in some versions of Pivotal RabbitMQ.

Observation

Pivotal RabbitMQ is a messaging broker server application.

Multiple vulnerabilities are present in some versions of Pivotal RabbitMQ. The flaws lie in the web-based management user interface. Exploitation could allow an attacker to perform XSS attacks.

22985 - (HPSBHF03564) HP Synaptics Touchpad Driver Potential Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-17556

Description

An information disclosure vulnerability is present within Synaptics Touchpad Driver in HP devices.

Observation

Synaptics Touchpad Driver is the controller software for Synaptics' Touchpad devices.

An information disclosure vulnerability is present within Synaptics Touchpad Driver in HP devices. The flaw lies in Synaptics' Touchpad Driver. Successful exploitation could allow a malicious local user to obtain sensitive information. Exploitation requires administrative privileges.

88908 - Slackware Linux 14.0, 14.2 SSA:2018-016-01 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
SSA:2018-016-01

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.1191628

Slackware 14.0
i586
kernel-huge-3.2.98-i586-1
kernel-generic-3.2.98-i586-1
kernel-modules-3.2.98-i586-1

i686
kernel-modules-smp-3.2.98_smp-i686-1
kernel-huge-smp-3.2.98_smp-i686-1
kernel-generic-smp-3.2.98_smp-i686-1

noarch
kernel-source-3.2.98-noarch-1
kernel-firmware-20180104_65b1c68-noarch-1
kernel-source-3.2.98_smp-noarch-1

x86_64
kernel-generic-3.2.98-x86_64-1
kernel-huge-3.2.98-x86_64-1
kernel-modules-3.2.98-x86_64-1

Slackware 14.2
i586
kernel-modules-4.4.111-i586-1
kernel-generic-4.4.111-i586-1
kernel-huge-4.4.111-i586-1

i686
kernel-huge-smp-4.4.111_smp-i686-1
kernel-generic-smp-4.4.111_smp-i686-1
kernel-modules-smp-4.4.111_smp-i686-1

noarch
kernel-firmware-20180104_65b1c68-noarch-1
kernel-source-4.4.111_smp-noarch-1
kernel-source-4.4.111-noarch-1

x86_64
kernel-modules-4.4.111-x86_64-1
kernel-huge-4.4.111-x86_64-1
kernel-generic-4.4.111-x86_64-1

132427 - Oracle VM OVMSA-2018-0008 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0008

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000819.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-112.14.10.el6uek
kernel-uek-4.1.12-112.14.10.el6uek

132428 - Oracle VM OVMSA-2018-0007 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0007

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000818.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-112.14.5.el6uek
kernel-uek-4.1.12-112.14.5.el6uek

141836 - Red Hat Enterprise Linux RHSA-2018-0093 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0093

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00060.html

RHEL6_2S
x86_64
microcode_ctl-1.17-9.2.el6_2
microcode_ctl-debuginfo-1.17-9.2.el6_2

RHEL7S
x86_64
microcode_ctl-debuginfo-2.1-22.5.el7_4
microcode_ctl-2.1-22.5.el7_4

RHEL6S
x86_64

microcode_ctl-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-25.4.el6_9

i386
microcode_ctl-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-25.4.el6_9

RHEL6WS
x86_64
microcode_ctl-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-25.4.el6_9

i386
microcode_ctl-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-25.4.el6_9

RHEL6_4S
x86_64
microcode_ctl-debuginfo-1.17-16.2.el6_4
microcode_ctl-1.17-16.2.el6_4

RHEL7_3S
x86_64
microcode_ctl-debuginfo-2.1-16.5.el7_3
microcode_ctl-2.1-16.5.el7_3

RHEL6_7S
x86_64
microcode_ctl-debuginfo-1.17-20.2.el6_7
microcode_ctl-1.17-20.2.el6_7

i386
microcode_ctl-debuginfo-1.17-20.2.el6_7
microcode_ctl-1.17-20.2.el6_7

RHEL6_6S
x86_64
microcode_ctl-debuginfo-1.17-19.2.el6_6
microcode_ctl-1.17-19.2.el6_6

RHEL6_5S
x86_64
microcode_ctl-1.17-17.el6_5.3
microcode_ctl-debuginfo-1.17-17.el6_5.3

RHEL7D
x86_64
microcode_ctl-debuginfo-2.1-22.5.el7_4
microcode_ctl-2.1-22.5.el7_4

RHEL6D
x86_64
microcode_ctl-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-25.4.el6_9

i386
microcode_ctl-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-25.4.el6_9

RHEL7WS

x86_64
microcode_ctl-debuginfo-2.1-22.5.el7_4
microcode_ctl-2.1-22.5.el7_4

141837 - Red Hat Enterprise Linux RHSA-2018-0094 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0094

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00059.html

RHEL7D
noarch
iwl3160-firmware-22.0.7.0-58.el7_4
iwl1000-firmware-39.31.5.1-58.el7_4
iwl2000-firmware-18.168.6.1-58.el7_4
iwl4965-firmware-228.61.2.24-58.el7_4
linux-firmware-20170606-58.gitc990aae.el7_4
iwl7265-firmware-22.0.7.0-58.el7_4
iwl7260-firmware-22.0.7.0-58.el7_4
iwl105-firmware-18.168.6.1-58.el7_4
iwl6000g2b-firmware-17.168.5.2-58.el7_4
iwl3945-firmware-15.32.2.9-58.el7_4
iwl135-firmware-18.168.6.1-58.el7_4
iwl6050-firmware-41.28.5.1-58.el7_4
iwl100-firmware-39.31.5.1-58.el7_4
iwl2030-firmware-18.168.6.1-58.el7_4
iwl6000g2a-firmware-17.168.5.3-58.el7_4
iwl6000-firmware-9.221.4.1-58.el7_4
iwl5150-firmware-8.24.2.2-58.el7_4
iwl5000-firmware-8.83.5.1_1-58.el7_4

RHEL7S
noarch
iwl3160-firmware-22.0.7.0-58.el7_4
iwl1000-firmware-39.31.5.1-58.el7_4
iwl2000-firmware-18.168.6.1-58.el7_4
iwl4965-firmware-228.61.2.24-58.el7_4
linux-firmware-20170606-58.gitc990aae.el7_4
iwl7265-firmware-22.0.7.0-58.el7_4
iwl7260-firmware-22.0.7.0-58.el7_4
iwl105-firmware-18.168.6.1-58.el7_4
iwl6000g2b-firmware-17.168.5.2-58.el7_4
iwl3945-firmware-15.32.2.9-58.el7_4
iwl135-firmware-18.168.6.1-58.el7_4
iwl6050-firmware-41.28.5.1-58.el7_4
iwl100-firmware-39.31.5.1-58.el7_4
iwl2030-firmware-18.168.6.1-58.el7_4
iwl6000g2a-firmware-17.168.5.3-58.el7_4

iwl6000-firmware-9.221.4.1-58.el7_4
iwl5150-firmware-8.24.2.2-58.el7_4
iwl5000-firmware-8.83.5.1_1-58.el7_4

RHEL7WS
noarch
iwl3160-firmware-22.0.7.0-58.el7_4
iwl1000-firmware-39.31.5.1-58.el7_4
iwl2000-firmware-18.168.6.1-58.el7_4
iwl4965-firmware-228.61.2.24-58.el7_4
linux-firmware-20170606-58.gitc990aae.el7_4
iwl7265-firmware-22.0.7.0-58.el7_4
iwl7260-firmware-22.0.7.0-58.el7_4
iwl105-firmware-18.168.6.1-58.el7_4
iwl6000g2b-firmware-17.168.5.2-58.el7_4
iwl3945-firmware-15.32.2.9-58.el7_4
iwl135-firmware-18.168.6.1-58.el7_4
iwl6050-firmware-41.28.5.1-58.el7_4
iwl100-firmware-39.31.5.1-58.el7_4
iwl2030-firmware-18.168.6.1-58.el7_4
iwl6000g2a-firmware-17.168.5.3-58.el7_4
iwl6000-firmware-9.221.4.1-58.el7_4
iwl5150-firmware-8.24.2.2-58.el7_4
iwl5000-firmware-8.83.5.1_1-58.el7_4

RHEL7_3S
noarch
iwl5000-firmware-8.83.5.1_1-51.el7_3
iwl3160-firmware-22.0.7.0-51.el7_3
iwl6000-firmware-9.221.4.1-51.el7_3
iwl1000-firmware-39.31.5.1-51.el7_3
iwl2030-firmware-18.168.6.1-51.el7_3
iwl135-firmware-18.168.6.1-51.el7_3
linux-firmware-20160830-51.git7534e19.el7_3
iwl4965-firmware-228.61.2.24-51.el7_3
iwl100-firmware-39.31.5.1-51.el7_3
iwl105-firmware-18.168.6.1-51.el7_3
iwl7260-firmware-22.0.7.0-51.el7_3
iwl6050-firmware-41.28.5.1-51.el7_3
iwl2000-firmware-18.168.6.1-51.el7_3
iwl6000g2a-firmware-17.168.5.3-51.el7_3
iwl6000g2b-firmware-17.168.5.2-51.el7_3
iwl7265-firmware-22.0.7.0-51.el7_3
iwl3945-firmware-15.32.2.9-51.el7_3
iwl5150-firmware-8.24.2.2-51.el7_3

146226 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0088-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3636, CVE-2017-3641, CVE-2017-3653

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0088-1

Observation

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

For more information see:

http://lists.opensuse.org/opensuse-updates/2018-01/msg00032.html

SuSE Linux 42.2
x86_64
mariadb-debuginfo-10.0.32-20.10.1
mariadb-tools-10.0.32-20.10.1
mariadb-debugsource-10.0.32-20.10.1
mariadb-tools-debuginfo-10.0.32-20.10.1
mariadb-test-10.0.32-20.10.1
libmysqld18-10.0.32-20.10.1
libmysqld18-debuginfo-10.0.32-20.10.1
libmysqlclient18-debuginfo-10.0.32-20.10.1
libmysqlclient_r18-32bit-10.0.32-20.10.1
libmysqld-devel-10.0.32-20.10.1
mariadb-errormessages-10.0.32-20.10.1
libmysqlclient-devel-10.0.32-20.10.1
mariadb-10.0.32-20.10.1
mariadb-test-debuginfo-10.0.32-20.10.1
mariadb-bench-10.0.32-20.10.1
libmysqlclient18-32bit-10.0.32-20.10.1
mariadb-client-10.0.32-20.10.1
mariadb-bench-debuginfo-10.0.32-20.10.1
mariadb-client-debuginfo-10.0.32-20.10.1
libmysqlclient_r18-10.0.32-20.10.1
libmysqlclient18-10.0.32-20.10.1
libmysqlclient18-debuginfo-32bit-10.0.32-20.10.1

i586
mariadb-debuginfo-10.0.32-20.10.1
mariadb-tools-10.0.32-20.10.1
mariadb-debugsource-10.0.32-20.10.1
mariadb-tools-debuginfo-10.0.32-20.10.1
mariadb-test-10.0.32-20.10.1
libmysqld18-10.0.32-20.10.1
libmysqld18-debuginfo-10.0.32-20.10.1
libmysqlclient18-debuginfo-10.0.32-20.10.1
libmysqld-devel-10.0.32-20.10.1
mariadb-errormessages-10.0.32-20.10.1
libmysqlclient-devel-10.0.32-20.10.1
mariadb-10.0.32-20.10.1
mariadb-test-debuginfo-10.0.32-20.10.1
mariadb-bench-10.0.32-20.10.1
mariadb-client-10.0.32-20.10.1
mariadb-bench-debuginfo-10.0.32-20.10.1
mariadb-client-debuginfo-10.0.32-20.10.1
libmysqlclient_r18-10.0.32-20.10.1
libmysqlclient18-10.0.32-20.10.1

SuSE Linux 42.3
x86_64
libmysqld18-10.0.32-26.1
mariadb-errormessages-10.0.32-26.1
mariadb-test-debuginfo-10.0.32-26.1
libmysqlclient18-10.0.32-26.1
mariadb-client-10.0.32-26.1
mariadb-client-debuginfo-10.0.32-26.1
mariadb-debugsource-10.0.32-26.1
libmysqld-devel-10.0.32-26.1

mariadb-10.0.32-26.1
libmysqlclient18-32bit-10.0.32-26.1
mariadb-debuginfo-10.0.32-26.1
mariadb-bench-10.0.32-26.1
mariadb-tools-10.0.32-26.1
libmysqlclient_r18-10.0.32-26.1
libmysqlclient18-debuginfo-32bit-10.0.32-26.1
libmysqlclient18-debuginfo-10.0.32-26.1
mariadb-test-10.0.32-26.1
mariadb-tools-debuginfo-10.0.32-26.1
libmysqld18-debuginfo-10.0.32-26.1
libmysqlclient_r18-32bit-10.0.32-26.1
mariadb-bench-debuginfo-10.0.32-26.1
libmysqlclient-devel-10.0.32-26.1

i586
libmysqld18-10.0.32-26.1
mariadb-errormessages-10.0.32-26.1
mariadb-test-debuginfo-10.0.32-26.1
libmysqlclient18-10.0.32-26.1
mariadb-client-10.0.32-26.1
mariadb-client-debuginfo-10.0.32-26.1
mariadb-debugsource-10.0.32-26.1
libmysqld-devel-10.0.32-26.1
mariadb-10.0.32-26.1
mariadb-debuginfo-10.0.32-26.1
mariadb-bench-10.0.32-26.1
mariadb-tools-10.0.32-26.1
libmysqlclient_r18-10.0.32-26.1
libmysqlclient18-debuginfo-10.0.32-26.1
mariadb-test-10.0.32-26.1
mariadb-tools-debuginfo-10.0.32-26.1
libmysqld18-debuginfo-10.0.32-26.1
mariadb-bench-debuginfo-10.0.32-26.1
libmysqlclient-devel-10.0.32-26.1

146235 - SuSE Linux 42.2 openSUSE-SU-2018:0059-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0059-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00020.html

SuSE Linux 42.2
i586
qemu-2.6.2-31.18.1
qemu-arm-debuginfo-2.6.2-31.18.1
qemu-x86-2.6.2-31.18.1
qemu-debugsource-2.6.2-31.18.1

qemu-s390-debuginfo-2.6.2-31.18.1
qemu-guest-agent-debuginfo-2.6.2-31.18.1
qemu-guest-agent-2.6.2-31.18.1
qemu-ppc-2.6.2-31.18.1
qemu-block-dmg-2.6.2-31.18.1
qemu-block-iscsi-debuginfo-2.6.2-31.18.1
qemu-x86-debuginfo-2.6.2-31.18.1
qemu-ppc-debuginfo-2.6.2-31.18.1
qemu-linux-user-debugsource-2.6.2-31.18.1
qemu-block-ssh-debuginfo-2.6.2-31.18.1
qemu-linux-user-debuginfo-2.6.2-31.18.1
qemu-block-curl-debuginfo-2.6.2-31.18.1
qemu-linux-user-2.6.2-31.18.1
qemu-kvm-2.6.2-31.18.1
qemu-arm-2.6.2-31.18.1
qemu-testsuite-2.6.2-31.18.1
qemu-tools-2.6.2-31.18.1
qemu-extra-2.6.2-31.18.1
qemu-tools-debuginfo-2.6.2-31.18.1
qemu-block-iscsi-2.6.2-31.18.1
qemu-extra-debuginfo-2.6.2-31.18.1
qemu-block-dmg-debuginfo-2.6.2-31.18.1
qemu-block-curl-2.6.2-31.18.1
qemu-lang-2.6.2-31.18.1
qemu-s390-2.6.2-31.18.1
qemu-block-ssh-2.6.2-31.18.1

noarch
qemu-vgabios-1.9.1-31.18.1
qemu-ipxe-1.0.0-31.18.1
qemu-seabios-1.9.1-31.18.1
qemu-sgabios-8-31.18.1

x86_64
qemu-2.6.2-31.18.1
qemu-arm-debuginfo-2.6.2-31.18.1
qemu-x86-2.6.2-31.18.1
qemu-debugsource-2.6.2-31.18.1
qemu-s390-debuginfo-2.6.2-31.18.1
qemu-guest-agent-debuginfo-2.6.2-31.18.1
qemu-guest-agent-2.6.2-31.18.1
qemu-ppc-2.6.2-31.18.1
qemu-block-dmg-2.6.2-31.18.1
qemu-block-iscsi-debuginfo-2.6.2-31.18.1
qemu-x86-debuginfo-2.6.2-31.18.1
qemu-ppc-debuginfo-2.6.2-31.18.1
qemu-linux-user-debugsource-2.6.2-31.18.1
qemu-block-ssh-debuginfo-2.6.2-31.18.1
qemu-linux-user-debuginfo-2.6.2-31.18.1
qemu-block-curl-debuginfo-2.6.2-31.18.1
qemu-linux-user-2.6.2-31.18.1
qemu-block-rbd-2.6.2-31.18.1
qemu-kvm-2.6.2-31.18.1
qemu-arm-2.6.2-31.18.1
qemu-testsuite-2.6.2-31.18.1
qemu-tools-2.6.2-31.18.1
qemu-extra-2.6.2-31.18.1
qemu-tools-debuginfo-2.6.2-31.18.1
qemu-block-iscsi-2.6.2-31.18.1
qemu-block-rbd-debuginfo-2.6.2-31.18.1

qemu-extra-debuginfo-2.6.2-31.18.1
qemu-block-dmg-debuginfo-2.6.2-31.18.1
qemu-block-curl-2.6.2-31.18.1
qemu-lang-2.6.2-31.18.1
qemu-s390-2.6.2-31.18.1
qemu-block-ssh-2.6.2-31.18.1

146237 - SuSE SLES 12 SP3 SUSE-SU-2018:0113-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
SUSE-SU-2018:0113-1

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-January/003600.html

SuSE SLES 12 SP3
noarch
kernel-source-4.4.103-94.6.1
kernel-macros-4.4.103-94.6.1
kernel-devel-4.4.103-94.6.1

146242 - SuSE SLES 11 SP4 SUSE-SU-2018:0068-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0068-1

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-January/003587.html

SuSE SLES 11 SP4
x86_64
microcode_ctl-1.17-102.83.9.1

i586
microcode_ctl-1.17-102.83.9.1

146244 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0066-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0066-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00025.html

SuSE Linux 42.2
x86_64
ucode-intel-20180108-7.12.1
ucode-intel-blob-20180108-7.12.1
ucode-intel-debuginfo-20180108-7.12.1
ucode-intel-debugsource-20180108-7.12.1

i586
ucode-intel-20180108-7.12.1
ucode-intel-blob-20180108-7.12.1
ucode-intel-debuginfo-20180108-7.12.1
ucode-intel-debugsource-20180108-7.12.1

SuSE Linux 42.3
x86_64
ucode-intel-debugsource-20180108-16.1
ucode-intel-debuginfo-20180108-16.1
ucode-intel-20180108-16.1
ucode-intel-blob-20180108-16.1

i586
ucode-intel-debugsource-20180108-16.1
ucode-intel-debuginfo-20180108-16.1
ucode-intel-20180108-16.1
ucode-intel-blob-20180108-16.1

146245 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0067-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0067-1

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-January/003586.html

SuSE SLES 12 SP2
x86_64

ucode-intel-debuginfo-20180108-13.11.1
ucode-intel-20180108-13.11.1
ucode-intel-debugsource-20180108-13.11.1

SuSE SLED 12 SP3
x86_64
ucode-intel-debuginfo-20180108-13.11.1
ucode-intel-20180108-13.11.1
ucode-intel-debugsource-20180108-13.11.1

SuSE SLED 12 SP2
x86_64
ucode-intel-debuginfo-20180108-13.11.1
ucode-intel-20180108-13.11.1
ucode-intel-debugsource-20180108-13.11.1

SuSE SLES 12 SP3
x86_64
ucode-intel-debuginfo-20180108-13.11.1
ucode-intel-20180108-13.11.1
ucode-intel-debugsource-20180108-13.11.1

146250 - SuSE SLES 12 SP2 SUSE-SU-2018:0069-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
SUSE-SU-2018:0069-1

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-January/003588.html

SuSE SLES 12 SP2
noarch
kernel-source-4.4.103-92.59.1
kernel-macros-4.4.103-92.59.1
kernel-devel-4.4.103-92.59.1

146251 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0079-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3636, CVE-2017-3641, CVE-2017-3653

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0079-1

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-January/003596.html

SuSE SLED 12 SP2
x86_64
mariadb-errormessages-10.0.32-29.10.1
libmysqlclient_r18-10.0.32-29.10.1
libmysqlclient18-10.0.32-29.10.1
mariadb-client-debuginfo-10.0.32-29.10.1
mariadb-client-10.0.32-29.10.1
libmysqlclient18-32bit-10.0.32-29.10.1
mariadb-debuginfo-10.0.32-29.10.1
libmysqlclient_r18-32bit-10.0.32-29.10.1
libmysqlclient18-debuginfo-32bit-10.0.32-29.10.1
mariadb-10.0.32-29.10.1
mariadb-debugsource-10.0.32-29.10.1
libmysqlclient18-debuginfo-10.0.32-29.10.1

SuSE SLES 12 SP3
x86_64
libmysqlclient18-32bit-10.0.32-29.10.1
mariadb-tools-10.0.32-29.10.1
libmysqlclient18-10.0.32-29.10.1
mariadb-client-debuginfo-10.0.32-29.10.1
mariadb-tools-debuginfo-10.0.32-29.10.1
mariadb-errormessages-10.0.32-29.10.1
mariadb-debuginfo-10.0.32-29.10.1
mariadb-debugsource-10.0.32-29.10.1
libmysqlclient18-debuginfo-32bit-10.0.32-29.10.1
mariadb-10.0.32-29.10.1
mariadb-client-10.0.32-29.10.1
libmysqlclient18-debuginfo-10.0.32-29.10.1

SuSE SLES 12 SP2
x86_64
libmysqlclient18-32bit-10.0.32-29.10.1
mariadb-tools-10.0.32-29.10.1
libmysqlclient18-10.0.32-29.10.1
mariadb-client-debuginfo-10.0.32-29.10.1
mariadb-tools-debuginfo-10.0.32-29.10.1
mariadb-errormessages-10.0.32-29.10.1
mariadb-debuginfo-10.0.32-29.10.1
mariadb-debugsource-10.0.32-29.10.1
libmysqlclient18-debuginfo-32bit-10.0.32-29.10.1
mariadb-10.0.32-29.10.1
mariadb-client-10.0.32-29.10.1
libmysqlclient18-debuginfo-10.0.32-29.10.1

SuSE SLED 12 SP3
x86_64
mariadb-errormessages-10.0.32-29.10.1
libmysqlclient_r18-10.0.32-29.10.1
libmysqlclient18-10.0.32-29.10.1
mariadb-client-debuginfo-10.0.32-29.10.1
mariadb-client-10.0.32-29.10.1
libmysqlclient18-32bit-10.0.32-29.10.1
mariadb-debuginfo-10.0.32-29.10.1
libmysqlclient_r18-32bit-10.0.32-29.10.1
libmysqlclient18-debuginfo-32bit-10.0.32-29.10.1

mariadb-10.0.32-29.10.1
mariadb-debugsource-10.0.32-29.10.1
libmysqlclient18-debuginfo-10.0.32-29.10.1

163525 - Oracle Enterprise Linux ELSA-2018-4011 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ELSA-2018-4011

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007456.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007457.html

OEL7
x86_64
kernel-uek-doc-4.1.12-112.14.11.el7uek
kernel-uek-firmware-4.1.12-112.14.11.el7uek
kernel-uek-4.1.12-112.14.11.el7uek
kernel-uek-devel-4.1.12-112.14.11.el7uek
kernel-uek-debug-devel-4.1.12-112.14.11.el7uek
kernel-uek-debug-4.1.12-112.14.11.el7uek

OEL6
x86_64
kernel-uek-4.1.12-112.14.11.el6uek
kernel-uek-doc-4.1.12-112.14.11.el6uek
kernel-uek-debug-devel-4.1.12-112.14.11.el6uek
kernel-uek-devel-4.1.12-112.14.11.el6uek
kernel-uek-firmware-4.1.12-112.14.11.el6uek
kernel-uek-debug-4.1.12-112.14.11.el6uek

163526 - Oracle Enterprise Linux ELSA-2018-4006 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ELSA-2018-4006

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007453.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007454.html

OEL7
x86_64
kernel-uek-debug-4.1.12-112.14.10.el7uek
kernel-uek-debug-devel-4.1.12-112.14.10.el7uek
kernel-uek-4.1.12-112.14.10.el7uek
kernel-uek-doc-4.1.12-112.14.10.el7uek
kernel-uek-firmware-4.1.12-112.14.10.el7uek
kernel-uek-devel-4.1.12-112.14.10.el7uek

OEL6
x86_64
kernel-uek-devel-4.1.12-112.14.10.el6uek
kernel-uek-debug-devel-4.1.12-112.14.10.el6uek
kernel-uek-debug-4.1.12-112.14.10.el6uek
kernel-uek-firmware-4.1.12-112.14.10.el6uek
kernel-uek-doc-4.1.12-112.14.10.el6uek
kernel-uek-4.1.12-112.14.10.el6uek

163527 - Oracle Enterprise Linux ELSA-2018-4004 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ELSA-2018-4004

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007451.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007452.html

OEL7
x86_64
kernel-uek-debug-4.1.12-112.14.5.el7uek
kernel-uek-debug-devel-4.1.12-112.14.5.el7uek
kernel-uek-4.1.12-112.14.5.el7uek
kernel-uek-devel-4.1.12-112.14.5.el7uek
kernel-uek-firmware-4.1.12-112.14.5.el7uek
kernel-uek-doc-4.1.12-112.14.5.el7uek

OEL6
x86_64
kernel-uek-devel-4.1.12-112.14.5.el6uek
kernel-uek-4.1.12-112.14.5.el6uek
kernel-uek-doc-4.1.12-112.14.5.el6uek
kernel-uek-debug-devel-4.1.12-112.14.5.el6uek
kernel-uek-debug-4.1.12-112.14.5.el6uek
kernel-uek-firmware-4.1.12-112.14.5.el6uek

186039 - Ubuntu Linux 16.04 USN-3522-3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3522-3

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004223.html

Ubuntu 16.04

linux-image-4.4.0-109-lowlatency_4.4.0-109.132
linux-image-generic_4.4.0.109.114
linux-image-4.4.0-109-generic_4.4.0-109.132
linux-image-lowlatency_4.4.0.109.114

186041 - Ubuntu Linux 12.04 USN-3525-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3525-1

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-January/004217.html

Ubuntu 12.04

linux-image-generic-pae_3.2.0.132.146
linux-image-generic_3.2.0.132.146
linux-image-3.2.0-132-generic_3.2.0-132.178
linux-image-3.2.0-132-generic-pae_3.2.0-132.178

186045 - Ubuntu Linux 16.04, 17.04, 17.10 USN-3530-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
USN-3530-1

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-January/004225.html

Ubuntu 16.04

libwebkit2gtk-4.0-37_2.18.5-0ubuntu0.16.04.1
libjavascriptcoregtk-4.0-18_2.18.5-0ubuntu0.16.04.1

Ubuntu 17.04

libjavascriptcoregtk-4.0-18_2.18.5-0ubuntu0.17.04.1
libwebkit2gtk-4.0-37_2.18.5-0ubuntu0.17.04.1

Ubuntu 17.10

libwebkit2gtk-4.0-37_2.18.5-0ubuntu0.17.10.1
libjavascriptcoregtk-4.0-18_2.18.5-0ubuntu0.17.10.1

186047 - Ubuntu Linux 14.04 USN-3522-4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3522-4

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-January/004224.html

Ubuntu 14.04

linux-image-generic-lts-xenial_4.4.0.109.92
linux-image-lowlatency-lts-xenial_4.4.0.109.92
linux-image-4.4.0-109-lowlatency_4.4.0-109.132~14.04.1
linux-image-4.4.0-109-generic_4.4.0-109.132~14.04.1

186048 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3531-1 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-3531-1

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-January/004226.html

Ubuntu 16.04

intel-microcode_3.20180108.0~ubuntu16.04.2

Ubuntu 14.04

intel-microcode_3.20180108.0~ubuntu14.04.2

Ubuntu 17.04

intel-microcode_3.20180108.0~ubuntu17.04.1

Ubuntu 17.10

intel-microcode_3.20180108.0~ubuntu17.10.1

186051 - Ubuntu Linux 12.04 USN-3524-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3524-2

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-January/004216.html

Ubuntu 12.04

linux-image-generic-lpae-lts-trusty_3.13.0.139.129
linux-image-3.13.0-139-generic-lpae_3.13.0-139.188~precise1
linux-image-generic-lts-trusty_3.13.0.139.129
linux-image-3.13.0-139-generic_3.13.0-139.188~precise1

193171 - Fedora Linux 27 FEDORA-2018-0590e4af13 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2018-0590e4af13

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/2018/1/?count=200&page=3

Fedora Core 27

webkitgtk4-2.18.5-1.fc27

33379 - Oracle Solaris 149175-13 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
149175-13

Observation

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

https://getupdates.oracle.com/readme/149175-13

SunOS 5.10: qlc patch

SOLARIS_10

SUNWqlc:11.10.0,REV=2005.01.04.14.31
SUNWqlcu:11.10.0,REV=2006.02.21.03.25

33380 - Oracle Solaris 149176-13 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
149176-13

Observation

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

https://getupdates.oracle.com/readme/149176-13

SunOS 5.10(x86): qlc patch

SOLARIS_10_x86

SUNWqlc:11.10.0,REV=2005.01.04.14.30
SUNWqlcu:11.10.0,REV=2006.02.21.05.35

130991 - Debian Linux 8.0, 9.0 DSA-4084-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000421

Description

The scan detected that the host is missing the following update:
DSA-4084-1

Observation

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

http://www.debian.org/security/2018/dsa-4084

Debian 8.0
all
gifsicle_1.86-1+deb8u1

Debian 9.0
all
gifsicle_1.88-3+deb9u1

130992 - Debian Linux 8.0, 9.0 DSA-4086-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15412

Description

The scan detected that the host is missing the following update:
DSA-4086-1

Observation

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

http://www.debian.org/security/2018/dsa-4086

Debian 8.0
all
libxml2_2.9.1+dfsg1-5+deb8u6

Debian 9.0
all
libxml2_2.9.4+dfsg1-2.2+deb9u2

130993 - Debian Linux 8.0, 9.0 DSA-4089-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
DSA-4089-1

Observation

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

For more information see:

http://www.debian.org/security/2018/dsa-4089

Debian 8.0
all
bind9_1:9.9.5.dfsg-9+deb8u15

Debian 9.0
all
bind9_1:9.10.3.dfsg.P4-12.3+deb9u4

130994 - Debian Linux 8.0 DSA-4085-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-0486

Description

The scan detected that the host is missing the following update:
DSA-4085-1

Observation

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

http://www.debian.org/security/2018/dsa-4085

Debian 8.0
all
libxmltooling6_1.5.3-2+deb8u2
libxmltooling-dev_1.5.3-2+deb8u2
libxmltooling-doc_1.5.3-2+deb8u2
xmltooling-schemas_1.5.3-2+deb8u2

130995 - Debian Linux 8.0, 9.0 DSA-4087-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5702

Description

The scan detected that the host is missing the following update:
DSA-4087-1

Observation

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

http://www.debian.org/security/2018/dsa-4087

Debian 8.0
all
transmission_2.84-0.2+deb8u1

Debian 9.0

all
transmission_2.92-2+deb9u1

130996 - Debian Linux 8.0, 9.0 DSA-4083-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000472

Description

The scan detected that the host is missing the following update:
DSA-4083-1

Observation

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

http://www.debian.org/security/2018/dsa-4083

Debian 8.0
all
libpocoxml9-dbg_1.3.6p1-5+deb8u1
libpocodata9_1.3.6p1-5+deb8u1
libpocomysql9-dbg_1.3.6p1-5+deb8u1
libpocoodbc9_1.3.6p1-5+deb8u1
libpococrypto9-dbg_1.3.6p1-5+deb8u1
libpocodata9-dbg_1.3.6p1-5+deb8u1
libpoconetssl9-dbg_1.3.6p1-5+deb8u1
libpocozip9_1.3.6p1-5+deb8u1
libpoconet9_1.3.6p1-5+deb8u1
libpocoodbc9-dbg_1.3.6p1-5+deb8u1
libpoconetssl9_1.3.6p1-5+deb8u1
libpocoxml9_1.3.6p1-5+deb8u1
libpocozip9-dbg_1.3.6p1-5+deb8u1
libpococrypto9_1.3.6p1-5+deb8u1
libpocomysql9_1.3.6p1-5+deb8u1
libpoconet9-dbg_1.3.6p1-5+deb8u1
libpocoutil9-dbg_1.3.6p1-5+deb8u1
libpocoutil9_1.3.6p1-5+deb8u1
libpocosqlite9-dbg_1.3.6p1-5+deb8u1
libpocofoundation9_1.3.6p1-5+deb8u1
libpoco-dev_1.3.6p1-5+deb8u1
libpocofoundation9-dbg_1.3.6p1-5+deb8u1
libpocosqlite9_1.3.6p1-5+deb8u1

Debian 9.0
all
libpococrypto46_1.7.6+dfsg1-5+deb9u1
libpocodataodbc46_1.7.6+dfsg1-5+deb9u1
libpocodata46_1.7.6+dfsg1-5+deb9u1
libpoconetssl46_1.7.6+dfsg1-5+deb9u1
libpocodatamysql46_1.7.6+dfsg1-5+deb9u1
libpocoxml46_1.7.6+dfsg1-5+deb9u1
libpoconet46_1.7.6+dfsg1-5+deb9u1
libpocofoundation46_1.7.6+dfsg1-5+deb9u1
libpocodatasqlite46_1.7.6+dfsg1-5+deb9u1
libpocozip46_1.7.6+dfsg1-5+deb9u1
libpoco-dev_1.7.6+dfsg1-5+deb9u1

libpocomongodb46_1.7.6+dfsg1-5+deb9u1
libpocoutil46_1.7.6+dfsg1-5+deb9u1

130997 - Debian Linux 8.0, 9.0 DSA-4088-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000422

Description

The scan detected that the host is missing the following update:
DSA-4088-1

Observation

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

http://www.debian.org/security/2018/dsa-4088

Debian 8.0
all
libgdk-pixbuf2.0-0-dbg_2.31.1-2+deb8u7
libgdk-pixbuf2.0-dev_2.31.1-2+deb8u7
libgdk-pixbuf2.0-0_2.31.1-2+deb8u7
libgdk-pixbuf2.0-doc_2.31.1-2+deb8u7
libgdk-pixbuf2.0-common_2.31.1-2+deb8u7
libgdk-pixbuf2.0-0-udeb_2.31.1-2+deb8u7
gir1.2-gdkpixbuf-2.0_2.31.1-2+deb8u7

Debian 9.0
all
gir1.2-gdkpixbuf-2.0_2.36.5-2+deb9u2
libgdk-pixbuf2.0-0-udeb_2.36.5-2+deb9u2
libgdk-pixbuf2.0-0_2.36.5-2+deb9u2
libgdk-pixbuf2.0-common_2.36.5-2+deb9u2
libgdk-pixbuf2.0-dev_2.36.5-2+deb9u2
libgdk-pixbuf2.0-doc_2.36.5-2+deb9u2

182571 - FreeBSD shibboleth-sp Vulnerable To Forged User Attribute Data (3dbe9492-f7b8-11e7-a12d-6cc21735f730)

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

Risk Level: Low

CVE: CVE-2018-0486

Description

The scan detected that the host is missing the following update:
shibboleth-sp -- vulnerable to forged user attribute data (3dbe9492-f7b8-11e7-a12d-6cc21735f730)

Observation

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

http://www.vuxml.org/freebsd/3dbe9492-f7b8-11e7-a12d-6cc21735f730.html

Affected packages:
xmltooling < 1.6.3

182572 - FreeBSD transmission-daemon Vulnerable To Dns Rebinding Attacks (3e5b8bd3-0c32-452f-a60e-beab7b762351)

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:
transmission-daemon -- vulnerable to dns rebinding attacks (3e5b8bd3-0c32-452f-a60e-beab7b762351)

Observation

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

http://www.vuxml.org/freebsd/3e5b8bd3-0c32-452f-a60e-beab7b762351.html

Affected packages:
transmission-daemon <= 2.92_3

186043 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3527-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5205, CVE-2018-5206, CVE-2018-5207, CVE-2018-5208

Description

The scan detected that the host is missing the following update:
USN-3527-1

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-January/004221.html

Ubuntu 16.04

irssi_0.8.19-1ubuntu1.6

Ubuntu 14.04

irssi_0.8.15-5ubuntu3.4

Ubuntu 17.04

irssi_0.8.20-2ubuntu2.3

Ubuntu 17.10

irssi_1.0.4-1ubuntu2.2

193163 - Fedora Linux 26 FEDORA-2018-5aa21dc9a3 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-2018-5aa21dc9a3

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/2018/1/?count=200&page=3

Fedora Core 26

qtpass-1.2.1-1.fc26

193164 - Fedora Linux 27 FEDORA-2018-d034538627 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-2018-d034538627

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/2018/1/?count=200&page=2

Fedora Core 27

php-7.1.13-1.fc27

193166 - Fedora Linux 26 FEDORA-2018-c4e9207c31 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-2018-c4e9207c31

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/2018/1/?count=200&page=2

Fedora Core 26

php-7.1.13-1.fc26

193167 - Fedora Linux 27 FEDORA-2017-14f5c6cdac Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-0203

Description

The scan detected that the host is missing the following update:
FEDORA-2017-14f5c6cdac

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/2018/1/?count=200&page=3

Fedora Core 27

qpid-cpp-1.37.0-1.fc27

193168 - Fedora Linux 27 FEDORA-2018-21a7ad920c 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-2018-21a7ad920c

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/2018/1/?count=200&page=3

Fedora Core 27

kernel-4.14.13-300.fc27

193169 - Fedora Linux 27 FEDORA-2018-9e37c33e3f 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-2018-9e37c33e3f

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/2018/1/?count=200&page=3

Fedora Core 27

electron-cash-3.1.2-1.fc27

193170 - Fedora Linux 26 FEDORA-2018-6b319763ab 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-2018-6b319763ab

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/2018/1/?count=200&page=2

Fedora Core 26

microcode_ctl-2.1-20.fc26

193172 - Fedora Linux 26 FEDORA-2018-e6fe35524d 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-2018-e6fe35524d

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/2018/1/?count=200&page=3

Fedora Core 26

kernel-4.14.13-200.fc26

193175 - Fedora Linux 26 FEDORA-2018-92de33f3b9 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-2018-92de33f3b9

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/2018/1/?count=200&page=3

Fedora Core 26

python-jsonrpclib-0.3.1-1.fc26

193176 - Fedora Linux 26 FEDORA-2018-903354c26c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-9274

Description

The scan detected that the host is missing the following update:
FEDORA-2018-903354c26c

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/2018/1/?count=200&page=2

Fedora Core 26

osc-0.162.1-230.1.1.fc26
osc-source_validator-0.10-1.fc26

193177 - Fedora Linux 26 FEDORA-2018-6cd2e0e292 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000421

Description

The scan detected that the host is missing the following update:
FEDORA-2018-6cd2e0e292

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/2018/1/?count=200&page=2

Fedora Core 26

gifsicle-1.90-1.fc26

193180 - Fedora Linux 27 FEDORA-2018-7e17849364 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-2018-7e17849364

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/2018/1/?count=200&page=3

Fedora Core 27

microcode_ctl-2.1-20.fc27

193181 - Fedora Linux 26 FEDORA-2018-b7e606d011 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-2018-b7e606d011

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/2018/1/?count=200&page=3

Fedora Core 26

electrum-3.0.5-1.fc26

193182 - Fedora Linux 27 FEDORA-2018-ac8aab1f7a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-9274

Description

The scan detected that the host is missing the following update:
FEDORA-2018-ac8aab1f7a

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/2018/1/?count=200&page=1

Fedora Core 27

osc-0.162.1-230.1.1.fc27
osc-source_validator-0.10-1.fc27

193183 - Fedora Linux 26 FEDORA-2017-d1213cef30 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17866

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d1213cef30

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/2018/1/?count=200&page=2

Fedora Core 26

mupdf-1.12.0-1.fc26

193184 - Fedora Linux 26 FEDORA-2017-7bac3ba7c3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-0203

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7bac3ba7c3

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/2018/1/?count=200&page=3

Fedora Core 26

qpid-cpp-1.37.0-1.fc26

193185 - Fedora Linux 26 FEDORA-2018-fb582aabcc 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-2018-fb582aabcc

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/2018/1/?count=200&page=3

Fedora Core 26

firefox-57.0.4-1.fc26

193187 - Fedora Linux 27 FEDORA-2018-57c3a424eb 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-2018-57c3a424eb

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/2018/1/?count=200&page=2

Fedora Core 27

qtpass-1.2.1-1.fc27

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.

33312 - Oracle Solaris 152078-81 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

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

33313 - Oracle Solaris 152076-81 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

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

33314 - Oracle Solaris 152079-81 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

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

33315 - Oracle Solaris 152077-81 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

Update Details

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

33145 - Oracle Solaris 150401-59 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5544, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122

Update Details

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

33162 - Oracle Solaris 150400-59 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122

Update Details

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

33319 - Oracle Solaris 151913-11 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33323 - Oracle Solaris 151912-11 Update Is Not Installed

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

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

33336 - Oracle Solaris 152099-71 Update Is Not Installed

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

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

33339 - Oracle Solaris 152097-71 Update Is Not Installed

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

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

33340 - Oracle Solaris 152098-71 Update Is Not Installed

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

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

33341 - Oracle Solaris 152096-71 Update Is Not Installed

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

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

33349 - Oracle Solaris 152101-61 Update Is Not Installed

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

Update Details

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

33350 - Oracle Solaris 152100-61 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70087 - hp.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70088 - ibm.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.