2018-FEB-07
FSL version 7.6.1

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

22334 - (K15479471) F5 BIG-IP Mozilla NSS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-2834

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Mozilla Network Security Services. Successful exploitation could allow an attacker to cause a denial of service condition.

23037 - Google Chrome Multiple Vulnerabilities Prior To 64.0.3282.119

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

Risk Level: High

CVE: CVE-2017-15420, CVE-2018-6031, CVE-2018-6032, CVE-2018-6033, CVE-2018-6034, CVE-2018-6035, CVE-2018-6036, CVE-2018-6037, CVE-2018-6038, CVE-2018-6039, CVE-2018-6040, CVE-2018-6041, CVE-2018-6042, CVE-2018-6043, CVE-2018-6045, CVE-2018-6046, CVE-2018-6047, CVE-2018-6048, CVE-2018-6049, CVE-2018-6050, CVE-2018-6051, CVE-2018-6052, CVE-2018-6053, CVE-2018-6054

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to to obtain sensitive information, bypass multiple security measures or conduct different web-based attacks.

23038 - Google Chrome Multiple Vulnerabilities Prior To 64.0.3282.119

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-15420, CVE-2018-6031, CVE-2018-6032, CVE-2018-6033, CVE-2018-6034, CVE-2018-6035, CVE-2018-6036, CVE-2018-6037, CVE-2018-6038, CVE-2018-6039, CVE-2018-6040, CVE-2018-6041, CVE-2018-6042, CVE-2018-6043, CVE-2018-6045, CVE-2018-6046, CVE-2018-6047, CVE-2018-6048, CVE-2018-6049, CVE-2018-6050, CVE-2018-6051, CVE-2018-6052, CVE-2018-6053, CVE-2018-6054

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to to obtain sensitive information, bypass multiple security measures or conduct different web-based attacks.

23068 - (APSB18-03) Multiple Vulnerabilities In Adobe Flash Player

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

Risk Level: High

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

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in the Adobe Flash Player Runtime. Successful exploitation could allow an attacker to execute remote code and take control of the affected system.

23069 - (APSB18-03) Multiple Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

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

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in the Adobe Flash Player Runtime. Successful exploitation could allow an attacker to execute remote code and take control of the affected system.

146327 - SuSE Linux 42.3 openSUSE-SU-2018:0326-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4692, CVE-2016-4743, CVE-2016-7586, CVE-2016-7587, CVE-2016-7589, CVE-2016-7592, CVE-2016-7598, CVE-2016-7599, CVE-2016-7610, CVE-2016-7623, CVE-2016-7632, CVE-2016-7635, CVE-2016-7639, CVE-2016-7641, CVE-2016-7645, CVE-2016-7652, CVE-2016-7654, CVE-2016-7656, CVE-2017-13788, CVE-2017-13798, CVE-2017-13803, CVE-2017-13856, CVE-2017-13866, CVE-2017-13870, CVE-2017-2350, CVE-2017-2354, CVE-2017-2355, CVE-2017-2356, CVE-2017-2362, CVE-2017-2363, CVE-2017-2364, CVE-2017-2365, CVE-2017-2366, CVE-2017-2369, CVE-2017-2371, CVE-2017-2373, CVE-2017-2496, CVE-2017-2510, CVE-2017-2539, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7006, CVE-2017-7011, CVE-2017-7012, CVE-2017-7018, CVE-2017-7019, CVE-2017-7020, CVE-2017-7030, CVE-2017-7034, CVE-2017-7037, CVE-2017-7038, CVE-2017-7039, CVE-2017-7040, CVE-2017-7041, CVE-2017-7042, CVE-2017-7043, CVE-2017-7046, CVE-2017-7048, CVE-2017-7049, CVE-2017-7052, CVE-2017-7055, CVE-2017-7056, CVE-2017-7059, CVE-2017-7061, CVE-2017-7064, CVE-2017-7081, CVE-2017-7087, CVE-2017-7089, CVE-2017-7090, CVE-2017-7091, CVE-2017-7092, CVE-2017-7093, CVE-2017-7094, CVE-2017-7095, CVE-2017-

7096, CVE-2017-7098, CVE-2017-7099, CVE-2017-7100, CVE-2017-7102, CVE-2017-7104, CVE-2017-7107, CVE-2017-7109, CVE-2017-7111, CVE-2017-7117, CVE-2017-7120, CVE-2017-7142, CVE-2017-7156, CVE-2017-7157

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0326-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00124.html

SuSE Linux 42.3
i586
libwebkit2gtk-4_0-37-debuginfo-2.18.5-8.1
typelib-1_0-JavaScriptCore-4_0-2.18.5-8.1
webkit-jsc-4-debuginfo-2.18.5-8.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.5-8.1
webkit-jsc-4-2.18.5-8.1
webkit2gtk3-plugin-process-gtk2-2.18.5-8.1
typelib-1_0-WebKit2WebExtension-4_0-2.18.5-8.1
libwebkit2gtk-4_0-37-2.18.5-8.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.18.5-8.1
libjavascriptcoregtk-4_0-18-2.18.5-8.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.5-8.1
webkit2gtk3-devel-2.18.5-8.1
webkit2gtk-4_0-injected-bundles-2.18.5-8.1
typelib-1_0-WebKit2-4_0-2.18.5-8.1
webkit2gtk3-debugsource-2.18.5-8.1

noarch
libwebkit2gtk3-lang-2.18.5-8.1

x86_64
libwebkit2gtk-4_0-37-debuginfo-2.18.5-8.1
libjavascriptcoregtk-4_0-18-debuginfo-32bit-2.18.5-8.1
libjavascriptcoregtk-4_0-18-32bit-2.18.5-8.1
libwebkit2gtk-4_0-37-debuginfo-32bit-2.18.5-8.1
typelib-1_0-JavaScriptCore-4_0-2.18.5-8.1
webkit-jsc-4-debuginfo-2.18.5-8.1
libwebkit2gtk-4_0-37-32bit-2.18.5-8.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.5-8.1
webkit-jsc-4-2.18.5-8.1
webkit2gtk3-plugin-process-gtk2-2.18.5-8.1
typelib-1_0-WebKit2WebExtension-4_0-2.18.5-8.1
libwebkit2gtk-4_0-37-2.18.5-8.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.18.5-8.1
libjavascriptcoregtk-4_0-18-2.18.5-8.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.5-8.1
webkit2gtk3-devel-2.18.5-8.1
webkit2gtk-4_0-injected-bundles-2.18.5-8.1
typelib-1_0-WebKit2-4_0-2.18.5-8.1
webkit2gtk3-debugsource-2.18.5-8.1

23053 - (HT208475) Apple Safari Vulnerabilities Prior To 11.0.3

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

Risk Level: High

CVE: CVE-2018-4088, CVE-2018-4089, CVE-2018-4096

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

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

23055 - IBM WebSphere Application Server Admin Console Potential Privilege Escalation Vulnerability (swg22012345)

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

Risk Level: High

CVE: CVE-2017-1731

Description

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

Observation

IBM WebSphere Application Server is a Java application server.

A privilege escalation vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in Admin Console. Successful exploitation could allow an attacker to obtain elevated privileges on the system.

88913 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2018-032-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16548, CVE-2018-5764

Description

The scan detected that the host is missing the following update:
SSA:2018-032-02

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.556837

Slackware 14.0
x86_64
rsync-3.1.3-x86_64-1

Slackware 13.37
x86_64
rsync-3.1.3-x86_64-1

Slackware 14.1
x86_64

rsync-3.1.3-x86_64-1

Slackware 13.1
x86_64
rsync-3.1.3-x86_64-1

Slackware 14.2
x86_64
rsync-3.1.3-x86_64-1

i586
rsync-3.1.3-i586-1

Slackware 13.0
x86_64
rsync-3.1.3-x86_64-1

88915 - Slackware Linux 14.1, 14.2 SSA:2018-032-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2562, CVE-2018-2612, CVE-2018-2622, CVE-2018-2640, CVE-2018-2665, CVE-2018-2668

Description

The scan detected that the host is missing the following update:
SSA:2018-032-01

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.369464

Slackware 14.1
x86_64
mariadb-5.5.59-x86_64-1

Slackware 14.2
x86_64
mariadb-10.0.34-x86_64-1

i586
mariadb-10.0.34-i586-1

141866 - Red Hat Enterprise Linux RHSA-2018-0265 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6031, CVE-2018-6032, CVE-2018-6033, CVE-2018-6034, CVE-2018-6035, CVE-2018-6036, CVE-2018-6037, CVE-2018-6038, CVE-2018-6039, CVE-2018-6040, CVE-2018-6041, CVE-2018-6042, CVE-2018-6043, CVE-2018-6045, CVE-2018-6046, CVE-2018-6047, CVE-2018-6048, CVE-2018-6049, CVE-2018-6050, CVE-2018-6051, CVE-2018-6052, CVE-2018-6053, CVE-2018-6054

Description

The scan detected that the host is missing the following update:
RHSA-2018-0265

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-February/msg00001.html

RHEL6D
x86_64
chromium-browser-debuginfo-64.0.3282.119-1.el6_9
chromium-browser-64.0.3282.119-1.el6_9

i386
chromium-browser-debuginfo-64.0.3282.119-1.el6_9
chromium-browser-64.0.3282.119-1.el6_9

RHEL6S
x86_64
chromium-browser-debuginfo-64.0.3282.119-1.el6_9
chromium-browser-64.0.3282.119-1.el6_9

i386
chromium-browser-debuginfo-64.0.3282.119-1.el6_9
chromium-browser-64.0.3282.119-1.el6_9

RHEL6WS
x86_64
chromium-browser-debuginfo-64.0.3282.119-1.el6_9
chromium-browser-64.0.3282.119-1.el6_9

i386
chromium-browser-debuginfo-64.0.3282.119-1.el6_9
chromium-browser-64.0.3282.119-1.el6_9

141867 - Red Hat Enterprise Linux RHSA-2018-0262 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5089, CVE-2018-5095, CVE-2018-5096, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5117

Description

The scan detected that the host is missing the following update:
RHSA-2018-0262

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-February/msg00000.html

RHEL7S
x86_64
thunderbird-debuginfo-52.6.0-1.el7_4
thunderbird-52.6.0-1.el7_4

RHEL6S
i386

thunderbird-52.6.0-1.el6_9
thunderbird-debuginfo-52.6.0-1.el6_9

x86_64
thunderbird-52.6.0-1.el6_9
thunderbird-debuginfo-52.6.0-1.el6_9

RHEL6WS
x86_64
thunderbird-52.6.0-1.el6_9
thunderbird-debuginfo-52.6.0-1.el6_9

i386
thunderbird-52.6.0-1.el6_9
thunderbird-debuginfo-52.6.0-1.el6_9

RHEL7D
x86_64
thunderbird-debuginfo-52.6.0-1.el7_4
thunderbird-52.6.0-1.el7_4

RHEL6D
x86_64
thunderbird-52.6.0-1.el6_9
thunderbird-debuginfo-52.6.0-1.el6_9

i386
thunderbird-52.6.0-1.el6_9
thunderbird-debuginfo-52.6.0-1.el6_9

RHEL7WS
x86_64
thunderbird-debuginfo-52.6.0-1.el7_4
thunderbird-52.6.0-1.el7_4

146322 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0349-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0349-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003702.html

SuSE SLED 12 SP2
x86_64
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.33.1

libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.33.1
ImageMagick-6.8.8.1-71.33.1
ImageMagick-debuginfo-6.8.8.1-71.33.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.33.1
libMagick++-6_Q16-3-6.8.8.1-71.33.1
libMagickCore-6_Q16-1-6.8.8.1-71.33.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.33.1
ImageMagick-debugsource-6.8.8.1-71.33.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.33.1
libMagickWand-6_Q16-1-6.8.8.1-71.33.1

SuSE SLES 12 SP3
x86_64
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.33.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.33.1
libMagickWand-6_Q16-1-6.8.8.1-71.33.1
ImageMagick-debugsource-6.8.8.1-71.33.1
libMagickCore-6_Q16-1-6.8.8.1-71.33.1
ImageMagick-debuginfo-6.8.8.1-71.33.1

SuSE SLES 12 SP2
x86_64
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.33.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.33.1
libMagickWand-6_Q16-1-6.8.8.1-71.33.1
ImageMagick-debugsource-6.8.8.1-71.33.1
libMagickCore-6_Q16-1-6.8.8.1-71.33.1
ImageMagick-debuginfo-6.8.8.1-71.33.1

SuSE SLED 12 SP3
x86_64
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.33.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.33.1
ImageMagick-6.8.8.1-71.33.1
ImageMagick-debuginfo-6.8.8.1-71.33.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.33.1
libMagick++-6_Q16-3-6.8.8.1-71.33.1
libMagickCore-6_Q16-1-6.8.8.1-71.33.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.33.1
ImageMagick-debugsource-6.8.8.1-71.33.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.33.1
libMagickWand-6_Q16-1-6.8.8.1-71.33.1

146326 - SuSE SLES 12 SP2 SUSE-SU-2018:0311-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14970, CVE-2017-9214, CVE-2017-9263, CVE-2017-9265

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0311-1

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/003692.html

SuSE SLES 12 SP2
x86_64
openvswitch-dpdk-switch-debuginfo-2.5.1-25.12.8
openvswitch-dpdk-debuginfo-2.5.1-25.12.8
openvswitch-2.5.1-25.12.7
openvswitch-switch-2.5.1-25.12.7
openvswitch-debugsource-2.5.1-25.12.7
openvswitch-dpdk-2.5.1-25.12.8
openvswitch-dpdk-debugsource-2.5.1-25.12.8
openvswitch-switch-debuginfo-2.5.1-25.12.7
openvswitch-debuginfo-2.5.1-25.12.7
openvswitch-dpdk-switch-2.5.1-25.12.8

146328 - SuSE SLES 11 SP4 SUSE-SU-2018:0362-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0362-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003707.html

SuSE SLES 11 SP4
i586
bind-chrootenv-9.9.6P1-0.51.7.1
bind-libs-9.9.6P1-0.51.7.1
bind-doc-9.9.6P1-0.51.7.1
bind-9.9.6P1-0.51.7.1
bind-utils-9.9.6P1-0.51.7.1

x86_64
bind-doc-9.9.6P1-0.51.7.1
bind-utils-9.9.6P1-0.51.7.1
bind-chrootenv-9.9.6P1-0.51.7.1
bind-libs-9.9.6P1-0.51.7.1
bind-libs-32bit-9.9.6P1-0.51.7.1
bind-9.9.6P1-0.51.7.1

146329 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0374-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5089, CVE-2018-5091, CVE-2018-5095, CVE-2018-5096, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5117

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0374-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003710.html

SuSE SLES 12 SP2
x86_64
MozillaFirefox-52.6.0esr-109.13.1
MozillaFirefox-debugsource-52.6.0esr-109.13.1
MozillaFirefox-translations-52.6.0esr-109.13.1
MozillaFirefox-debuginfo-52.6.0esr-109.13.1

SuSE SLED 12 SP3
x86_64
MozillaFirefox-52.6.0esr-109.13.1
MozillaFirefox-debugsource-52.6.0esr-109.13.1
MozillaFirefox-translations-52.6.0esr-109.13.1
MozillaFirefox-debuginfo-52.6.0esr-109.13.1

SuSE SLED 12 SP2
x86_64
MozillaFirefox-52.6.0esr-109.13.1
MozillaFirefox-debugsource-52.6.0esr-109.13.1
MozillaFirefox-translations-52.6.0esr-109.13.1
MozillaFirefox-debuginfo-52.6.0esr-109.13.1

SuSE SLES 12 SP3
x86_64
MozillaFirefox-52.6.0esr-109.13.1
MozillaFirefox-debugsource-52.6.0esr-109.13.1
MozillaFirefox-translations-52.6.0esr-109.13.1
MozillaFirefox-debuginfo-52.6.0esr-109.13.1

146330 - SuSE SLES 11 SP4 SUSE-SU-2018:0361-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5089, CVE-2018-5091, CVE-2018-5095, CVE-2018-5096, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5117

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0361-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003706.html

SuSE SLES 11 SP4
i586
MozillaFirefox-translations-52.6.0esr-72.20.2
MozillaFirefox-52.6.0esr-72.20.2

x86_64
MozillaFirefox-translations-52.6.0esr-72.20.2

MozillaFirefox-52.6.0esr-72.20.2

146331 - SuSE Linux 42.3 openSUSE-SU-2018:0324-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6003

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0324-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00122.html

SuSE Linux 42.3
x86_64
libtasn1-6-4.9-3.1
libtasn1-4.9-3.1
libtasn1-devel-32bit-4.9-3.1
libtasn1-debugsource-4.9-3.1
libtasn1-devel-4.9-3.1
libtasn1-debuginfo-4.9-3.1
libtasn1-6-debuginfo-4.9-3.1
libtasn1-6-32bit-4.9-3.1
libtasn1-6-debuginfo-32bit-4.9-3.1

i586
libtasn1-6-4.9-3.1
libtasn1-4.9-3.1
libtasn1-debugsource-4.9-3.1
libtasn1-devel-4.9-3.1
libtasn1-debuginfo-4.9-3.1
libtasn1-6-debuginfo-4.9-3.1

146332 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0338-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2625

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0338-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003696.html

SuSE SLED 12 SP3
x86_64

libXdmcp6-1.1.1-12.1
libXdmcp-debugsource-1.1.1-12.1
libXdmcp6-debuginfo-32bit-1.1.1-12.1
libXdmcp6-32bit-1.1.1-12.1
libXdmcp6-debuginfo-1.1.1-12.1

SuSE SLES 12 SP3
x86_64
libXdmcp6-1.1.1-12.1
libXdmcp-debugsource-1.1.1-12.1
libXdmcp6-debuginfo-32bit-1.1.1-12.1
libXdmcp6-32bit-1.1.1-12.1
libXdmcp6-debuginfo-1.1.1-12.1

146334 - SuSE Linux 42.3 openSUSE-SU-2018:0360-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6406

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0360-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00009.html

SuSE Linux 42.3
x86_64
chromium-debuginfo-64.0.3282.140-138.1
chromedriver-debuginfo-64.0.3282.140-138.1
re2-debugsource-20180201-12.1
libre2-0-20180201-12.1
chromedriver-64.0.3282.140-138.1
re2-devel-20180201-12.1
libre2-0-debuginfo-32bit-20180201-12.1
libre2-0-32bit-20180201-12.1
chromium-64.0.3282.140-138.1
libre2-0-debuginfo-20180201-12.1
chromium-debugsource-64.0.3282.140-138.1

i586
re2-debugsource-20180201-12.1
libre2-0-debuginfo-20180201-12.1
re2-devel-20180201-12.1
libre2-0-20180201-12.1

146338 - SuSE SLES 11 SP4 SUSE-SU-2018:0350-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10995, CVE-2017-11505, CVE-2017-11525, CVE-2017-11526, CVE-2017-11539, CVE-2017-11639, CVE-2017-11750, CVE-2017-12565, CVE-2017-12640, CVE-2017-12641, CVE-2017-12643, CVE-2017-12671, CVE-2017-12673, CVE-2017-12676, CVE-2017-12935, CVE-2017-13141, CVE-2017-13142, CVE-2017-13147, CVE-2017-14103, CVE-2017-14649, CVE-2017-

15218, CVE-2017-17504, CVE-2017-17879, CVE-2017-17884, CVE-2017-17914, CVE-2017-18027, CVE-2017-18029, CVE-2017-9261, CVE-2017-9262, CVE-2018-5685

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0350-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003703.html

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.78.29.2

x86_64
libMagickCore1-32bit-6.4.3.6-7.78.29.2
libMagickCore1-6.4.3.6-7.78.29.2

146342 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0337-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2626

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0337-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003695.html

SuSE SLED 12 SP3
x86_64
libICE-debugsource-1.0.8-12.1
libICE6-debuginfo-1.0.8-12.1
libICE6-32bit-1.0.8-12.1
libICE6-debuginfo-32bit-1.0.8-12.1
libICE6-1.0.8-12.1

SuSE SLES 12 SP3
x86_64
libICE-debugsource-1.0.8-12.1
libICE6-debuginfo-1.0.8-12.1
libICE6-32bit-1.0.8-12.1
libICE6-debuginfo-32bit-1.0.8-12.1
libICE6-1.0.8-12.1

146343 - SuSE Linux 42.3 openSUSE-SU-2018:0364-1 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-2018:0364-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00010.html

SuSE Linux 42.3
noarch
translate-toolkit-devel-doc-2.2.4-4.1
translate-toolkit-2.2.4-4.1

146346 - SuSE Linux 42.3 openSUSE-SU-2018:0323-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0323-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00121.html

SuSE Linux 42.3
i586
bind-debugsource-9.9.9P1-53.1
bind-utils-9.9.9P1-53.1
bind-lwresd-debuginfo-9.9.9P1-53.1
bind-utils-debuginfo-9.9.9P1-53.1
bind-devel-9.9.9P1-53.1
bind-debuginfo-9.9.9P1-53.1
bind-lwresd-9.9.9P1-53.1
bind-chrootenv-9.9.9P1-53.1
bind-9.9.9P1-53.1
bind-libs-9.9.9P1-53.1
bind-libs-debuginfo-9.9.9P1-53.1

noarch
bind-doc-9.9.9P1-53.1

x86_64
bind-libs-debuginfo-9.9.9P1-53.1
bind-devel-9.9.9P1-53.1
bind-utils-debuginfo-9.9.9P1-53.1
bind-debuginfo-9.9.9P1-53.1
bind-libs-32bit-9.9.9P1-53.1

bind-libs-debuginfo-32bit-9.9.9P1-53.1
bind-utils-9.9.9P1-53.1
bind-9.9.9P1-53.1
bind-libs-9.9.9P1-53.1
bind-lwresd-9.9.9P1-53.1
bind-lwresd-debuginfo-9.9.9P1-53.1
bind-chrootenv-9.9.9P1-53.1
bind-debugsource-9.9.9P1-53.1

146348 - SuSE Linux 42.3 openSUSE-SU-2018:0322-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5748

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0322-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00120.html

SuSE Linux 42.3
x86_64
libvirt-daemon-xen-3.3.0-12.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-12.1
libvirt-nss-3.3.0-12.1
libvirt-admin-debuginfo-3.3.0-12.1
libvirt-daemon-driver-network-3.3.0-12.1
libvirt-daemon-driver-uml-3.3.0-12.1
libvirt-daemon-config-network-3.3.0-12.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-scsi-3.3.0-12.1
libvirt-daemon-qemu-3.3.0-12.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-iscsi-3.3.0-12.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-12.1
libvirt-daemon-driver-lxc-3.3.0-12.1
libvirt-daemon-driver-nodedev-3.3.0-12.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-12.1
libvirt-daemon-driver-interface-3.3.0-12.1
libvirt-daemon-driver-storage-rbd-3.3.0-12.1
libvirt-daemon-driver-storage-disk-3.3.0-12.1
libvirt-debugsource-3.3.0-12.1
libvirt-devel-3.3.0-12.1
libvirt-daemon-uml-3.3.0-12.1
libvirt-3.3.0-12.1
libvirt-devel-32bit-3.3.0-12.1
libvirt-daemon-driver-uml-debuginfo-3.3.0-12.1
libvirt-client-debuginfo-32bit-3.3.0-12.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-mpath-3.3.0-12.1
libvirt-daemon-hooks-3.3.0-12.1
libvirt-libs-debuginfo-3.3.0-12.1
libvirt-daemon-driver-qemu-3.3.0-12.1

libvirt-daemon-config-nwfilter-3.3.0-12.1
libvirt-doc-3.3.0-12.1
libvirt-daemon-debuginfo-3.3.0-12.1
libvirt-client-3.3.0-12.1
libvirt-daemon-3.3.0-12.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-core-3.3.0-12.1
libvirt-daemon-driver-vbox-3.3.0-12.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-12.1
libvirt-admin-3.3.0-12.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-12.1
libvirt-daemon-driver-nwfilter-3.3.0-12.1
libvirt-daemon-driver-secret-3.3.0-12.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-12.1
libvirt-client-debuginfo-3.3.0-12.1
libvirt-daemon-vbox-3.3.0-12.1
libvirt-daemon-driver-storage-logical-3.3.0-12.1
libvirt-lock-sanlock-3.3.0-12.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-3.3.0-12.1
libvirt-daemon-driver-network-debuginfo-3.3.0-12.1
libvirt-nss-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-12.1
libvirt-daemon-driver-vbox-debuginfo-3.3.0-12.1
libvirt-lock-sanlock-debuginfo-3.3.0-12.1
libvirt-libs-3.3.0-12.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-12.1
libvirt-daemon-driver-libxl-3.3.0-12.1
libvirt-daemon-lxc-3.3.0-12.1

i586
libvirt-daemon-driver-qemu-debuginfo-3.3.0-12.1
libvirt-nss-3.3.0-12.1
libvirt-admin-debuginfo-3.3.0-12.1
libvirt-daemon-driver-network-3.3.0-12.1
libvirt-daemon-driver-uml-3.3.0-12.1
libvirt-daemon-config-network-3.3.0-12.1
libvirt-daemon-driver-storage-scsi-3.3.0-12.1
libvirt-daemon-qemu-3.3.0-12.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-iscsi-3.3.0-12.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-12.1
libvirt-daemon-driver-lxc-3.3.0-12.1
libvirt-daemon-driver-nodedev-3.3.0-12.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-12.1
libvirt-daemon-driver-interface-3.3.0-12.1
libvirt-daemon-driver-storage-disk-3.3.0-12.1
libvirt-debugsource-3.3.0-12.1
libvirt-devel-3.3.0-12.1
libvirt-daemon-uml-3.3.0-12.1
libvirt-3.3.0-12.1
libvirt-daemon-driver-uml-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-mpath-3.3.0-12.1
libvirt-daemon-hooks-3.3.0-12.1
libvirt-libs-debuginfo-3.3.0-12.1
libvirt-daemon-driver-qemu-3.3.0-12.1
libvirt-daemon-config-nwfilter-3.3.0-12.1
libvirt-doc-3.3.0-12.1

libvirt-daemon-debuginfo-3.3.0-12.1
libvirt-client-3.3.0-12.1
libvirt-daemon-3.3.0-12.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-core-3.3.0-12.1
libvirt-daemon-driver-vbox-3.3.0-12.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-12.1
libvirt-admin-3.3.0-12.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-12.1
libvirt-daemon-driver-nwfilter-3.3.0-12.1
libvirt-daemon-driver-secret-3.3.0-12.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-12.1
libvirt-client-debuginfo-3.3.0-12.1
libvirt-daemon-vbox-3.3.0-12.1
libvirt-daemon-driver-storage-logical-3.3.0-12.1
libvirt-lock-sanlock-3.3.0-12.1
libvirt-daemon-driver-storage-3.3.0-12.1
libvirt-daemon-driver-network-debuginfo-3.3.0-12.1
libvirt-nss-debuginfo-3.3.0-12.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-12.1
libvirt-daemon-driver-vbox-debuginfo-3.3.0-12.1
libvirt-lock-sanlock-debuginfo-3.3.0-12.1
libvirt-libs-3.3.0-12.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-12.1
libvirt-daemon-lxc-3.3.0-12.1

146349 - SuSE Linux 42.3 openSUSE-SU-2018:0370-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1294

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0370-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00015.html

SuSE Linux 42.3
noarch
apache-commons-email-javadoc-1.2-10.1
apache-commons-email-1.2-10.1

160357 - CentOS 6 CESA-2018-0169 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

CESA-2018-0169

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022756.html

CentOS 6
i686
kernel-debug-2.6.32-696.20.1.el6
kernel-devel-2.6.32-696.20.1.el6
perf-2.6.32-696.20.1.el6
kernel-2.6.32-696.20.1.el6
kernel-debug-devel-2.6.32-696.20.1.el6
python-perf-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6

noarch
kernel-firmware-2.6.32-696.20.1.el6
kernel-doc-2.6.32-696.20.1.el6
kernel-abi-whitelists-2.6.32-696.20.1.el6

x86_64
kernel-debug-2.6.32-696.20.1.el6
kernel-devel-2.6.32-696.20.1.el6
perf-2.6.32-696.20.1.el6
kernel-2.6.32-696.20.1.el6
kernel-debug-devel-2.6.32-696.20.1.el6
python-perf-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6

160359 - CentOS 6, 7 CESA-2018-0262 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5089, CVE-2018-5095, CVE-2018-5096, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5117

Description

The scan detected that the host is missing the following update:
CESA-2018-0262

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-February/022762.html
http://lists.centos.org/pipermail/centos-announce/2018-February/022761.html

CentOS 7
x86_64
thunderbird-52.6.0-1.el7.centos

CentOS 6
x86_64
thunderbird-52.6.0-1.el6.centos

i686
thunderbird-52.6.0-1.el6.centos

163543 - Oracle Enterprise Linux ELSA-2018-0262 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5089, CVE-2018-5095, CVE-2018-5096, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5117

Description

The scan detected that the host is missing the following update:
ELSA-2018-0262

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-February/007523.html
http://oss.oracle.com/pipermail/el-errata/2018-February/007522.html

OEL7
x86_64
thunderbird-52.6.0-1.0.1.el7_4

OEL6
x86_64
thunderbird-52.6.0-1.0.1.el6_9

i386
thunderbird-52.6.0-1.0.1.el6_9

170918 - Amazon Linux AMI ALAS-2018-944 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17448, CVE-2017-17450, CVE-2017-17712, CVE-2017-17741, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
ALAS-2018-944

Observation

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

https://alas.aws.amazon.com/ALAS-2018-944.html

Amazon Linux AMI
i686
kernel-tools-debuginfo-4.9.77-31.58.amzn1
kernel-tools-4.9.77-31.58.amzn1
kernel-devel-4.9.77-31.58.amzn1
perf-debuginfo-4.9.77-31.58.amzn1
kernel-tools-devel-4.9.77-31.58.amzn1
kernel-debuginfo-4.9.77-31.58.amzn1

kernel-headers-4.9.77-31.58.amzn1
perf-4.9.77-31.58.amzn1
kernel-debuginfo-common-i686-4.9.77-31.58.amzn1
kernel-4.9.77-31.58.amzn1

noarch
kernel-doc-4.9.77-31.58.amzn1

x86_64
kernel-tools-debuginfo-4.9.77-31.58.amzn1
kernel-tools-4.9.77-31.58.amzn1
kernel-devel-4.9.77-31.58.amzn1
kernel-tools-devel-4.9.77-31.58.amzn1
kernel-debuginfo-4.9.77-31.58.amzn1
kernel-debuginfo-common-x86_64-4.9.77-31.58.amzn1
kernel-headers-4.9.77-31.58.amzn1
perf-4.9.77-31.58.amzn1
perf-debuginfo-4.9.77-31.58.amzn1
kernel-4.9.77-31.58.amzn1

170920 - Amazon Linux AMI ALAS-2018-943 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
ALAS-2018-943

Observation

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

https://alas.aws.amazon.com/ALAS-2018-943.html

Amazon Linux AMI
x86_64
python35-devel-3.5.4-13.10.amzn1
python34-debuginfo-3.4.7-1.37.amzn1
python35-tools-3.5.4-13.10.amzn1
python35-test-3.5.4-13.10.amzn1
python34-devel-3.4.7-1.37.amzn1
python35-3.5.4-13.10.amzn1
python35-debuginfo-3.5.4-13.10.amzn1
python35-libs-3.5.4-13.10.amzn1
python34-3.4.7-1.37.amzn1
python34-test-3.4.7-1.37.amzn1
python34-tools-3.4.7-1.37.amzn1
python34-libs-3.4.7-1.37.amzn1

i686
python35-test-3.5.4-13.10.amzn1
python34-devel-3.4.7-1.37.amzn1
python35-tools-3.5.4-13.10.amzn1
python35-3.5.4-13.10.amzn1
python35-debuginfo-3.5.4-13.10.amzn1
python35-libs-3.5.4-13.10.amzn1

python34-libs-3.4.7-1.37.amzn1
python34-tools-3.4.7-1.37.amzn1
python34-3.4.7-1.37.amzn1
python34-debuginfo-3.4.7-1.37.amzn1
python34-test-3.4.7-1.37.amzn1
python35-devel-3.5.4-13.10.amzn1

175323 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86_64 (1802-79)

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

Risk Level: High

CVE: CVE-2018-5089, CVE-2018-5095, CVE-2018-5096, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5117

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86_64 (1802-79)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1802&L=scientific-linux-errata&F=&S=&P=79

SL7
x86_64
thunderbird-debuginfo-52.6.0-1.el7_4
thunderbird-52.6.0-1.el7_4

SL6
x86_64
thunderbird-52.6.0-1.el6_9
thunderbird-debuginfo-52.6.0-1.el6_9

i386
thunderbird-52.6.0-1.el6_9
thunderbird-debuginfo-52.6.0-1.el6_9

193240 - Fedora Linux 27 FEDORA-2018-d09a73ce72 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000004, CVE-2018-5750

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d09a73ce72

Observation

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

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

Fedora Core 27

kernel-4.14.16-300.fc27

193243 - Fedora Linux 26 FEDORA-2018-bfb9835edd Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11102, CVE-2017-11139, CVE-2017-11140, CVE-2017-11636, CVE-2017-11637, CVE-2017-11641, CVE-2017-11643, CVE-2017-13147, CVE-2017-16353, CVE-2017-16669, CVE-2017-17782, CVE-2017-17783, CVE-2017-17912, CVE-2017-17913, CVE-2017-17915

Description

The scan detected that the host is missing the following update:
FEDORA-2018-bfb9835edd

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 26

GraphicsMagick-1.3.28-1.fc26

193254 - Fedora Linux 26 FEDORA-2018-d82b617d6c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000004, CVE-2018-5750

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d82b617d6c

Observation

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

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

Fedora Core 26

kernel-4.14.16-200.fc26

193257 - Fedora Linux 27 FEDORA-2018-7c61d08c4f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11102, CVE-2017-11139, CVE-2017-11140, CVE-2017-11636, CVE-2017-11637, CVE-2017-11641, CVE-2017-11643, CVE-2017-13147, CVE-2017-16353, CVE-2017-16669, CVE-2017-17782, CVE-2017-17783, CVE-2017-17912, CVE-2017-17913, CVE-2017-17915

Description

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

FEDORA-2018-7c61d08c4f

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

GraphicsMagick-1.3.28-1.fc27

193262 - Fedora Linux 27 FEDORA-2018-d553b29a30 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2565, CVE-2018-2573, CVE-2018-2576, CVE-2018-2583, CVE-2018-2586, CVE-2018-2590, CVE-2018-2600, CVE-2018-2612, CVE-2018-2622, CVE-2018-2640, CVE-2018-2645, CVE-2018-2646, CVE-2018-2647, CVE-2018-2665, CVE-2018-2667, CVE-2018-2668, CVE-2018-2696, CVE-2018-2703

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d553b29a30

Observation

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

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

Fedora Core 27

community-mysql-5.7.21-1.fc27

23046 - Advantech WebAccess Two Vulnerabilities Prior To 8.2.20170817 (ICSA-18-023-01)

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: Medium

CVE: CVE-2018-5443, CVE-2018-5445

Description

Two vulnerabilities are present in some versions of Advantech WebAccess.

Observation

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

Two vulnerabilities are present in some versions of Advantech WebAccess. The flaws exist in multiple components. Successful exploitation could allow a remote attacker to execute arbitrary code or disclose information.

141865 - Red Hat Enterprise Linux RHSA-2018-0279 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5617, CVE-2016-6664, CVE-2017-10268, CVE-2017-10286, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384,

CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3636, CVE-2017-3641, CVE-2017-3653

Description

The scan detected that the host is missing the following update:
RHSA-2018-0279

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-February/msg00008.html

RHEL7S
x86_64
rh-mariadb100-mariadb-bench-10.0.33-3.el7
rh-mariadb100-mariadb-errmsg-10.0.33-3.el7
rh-mariadb100-mariadb-devel-10.0.33-3.el7
rh-mariadb100-mariadb-debuginfo-10.0.33-3.el7
rh-mariadb100-mariadb-oqgraph-engine-10.0.33-3.el7
rh-mariadb100-mariadb-common-10.0.33-3.el7
rh-mariadb100-mariadb-config-10.0.33-3.el7
rh-mariadb100-mariadb-server-10.0.33-3.el7
rh-mariadb100-mariadb-10.0.33-3.el7
rh-mariadb100-mariadb-test-10.0.33-3.el7

RHEL6S
x86_64
rh-mariadb100-mariadb-bench-10.0.33-3.el6
rh-mariadb100-mariadb-common-10.0.33-3.el6
rh-mariadb100-mariadb-oqgraph-engine-10.0.33-3.el6
rh-mariadb100-mariadb-devel-10.0.33-3.el6
rh-mariadb100-mariadb-debuginfo-10.0.33-3.el6
rh-mariadb100-mariadb-config-10.0.33-3.el6
rh-mariadb100-mariadb-errmsg-10.0.33-3.el6
rh-mariadb100-mariadb-server-10.0.33-3.el6
rh-mariadb100-mariadb-10.0.33-3.el6
rh-mariadb100-mariadb-test-10.0.33-3.el6

RHEL6WS
x86_64
rh-mariadb100-mariadb-bench-10.0.33-3.el6
rh-mariadb100-mariadb-common-10.0.33-3.el6
rh-mariadb100-mariadb-oqgraph-engine-10.0.33-3.el6
rh-mariadb100-mariadb-devel-10.0.33-3.el6
rh-mariadb100-mariadb-debuginfo-10.0.33-3.el6
rh-mariadb100-mariadb-config-10.0.33-3.el6
rh-mariadb100-mariadb-errmsg-10.0.33-3.el6
rh-mariadb100-mariadb-server-10.0.33-3.el6
rh-mariadb100-mariadb-10.0.33-3.el6
rh-mariadb100-mariadb-test-10.0.33-3.el6

RHEL6_7S
x86_64
rh-mariadb100-mariadb-bench-10.0.33-3.el6
rh-mariadb100-mariadb-common-10.0.33-3.el6
rh-mariadb100-mariadb-oqgraph-engine-10.0.33-3.el6
rh-mariadb100-mariadb-devel-10.0.33-3.el6

rh-mariadb100-mariadb-debuginfo-10.0.33-3.el6
rh-mariadb100-mariadb-config-10.0.33-3.el6
rh-mariadb100-mariadb-errmsg-10.0.33-3.el6
rh-mariadb100-mariadb-server-10.0.33-3.el6
rh-mariadb100-mariadb-10.0.33-3.el6
rh-mariadb100-mariadb-test-10.0.33-3.el6

RHEL7_3S
x86_64
rh-mariadb100-mariadb-bench-10.0.33-3.el7
rh-mariadb100-mariadb-errmsg-10.0.33-3.el7
rh-mariadb100-mariadb-devel-10.0.33-3.el7
rh-mariadb100-mariadb-debuginfo-10.0.33-3.el7
rh-mariadb100-mariadb-oqgraph-engine-10.0.33-3.el7
rh-mariadb100-mariadb-common-10.0.33-3.el7
rh-mariadb100-mariadb-config-10.0.33-3.el7
rh-mariadb100-mariadb-server-10.0.33-3.el7
rh-mariadb100-mariadb-10.0.33-3.el7
rh-mariadb100-mariadb-test-10.0.33-3.el7

RHEL7WS
x86_64
rh-mariadb100-mariadb-bench-10.0.33-3.el7
rh-mariadb100-mariadb-errmsg-10.0.33-3.el7
rh-mariadb100-mariadb-devel-10.0.33-3.el7
rh-mariadb100-mariadb-debuginfo-10.0.33-3.el7
rh-mariadb100-mariadb-oqgraph-engine-10.0.33-3.el7
rh-mariadb100-mariadb-common-10.0.33-3.el7
rh-mariadb100-mariadb-config-10.0.33-3.el7
rh-mariadb100-mariadb-server-10.0.33-3.el7
rh-mariadb100-mariadb-10.0.33-3.el7
rh-mariadb100-mariadb-test-10.0.33-3.el7

146337 - SuSE Linux 42.3 openSUSE-SU-2018:0315-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14919, CVE-2017-15896, CVE-2017-3735, CVE-2017-3736, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0315-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00113.html

SuSE Linux 42.3
i586
nodejs6-devel-6.12.2-6.1
npm6-6.12.2-6.1
nodejs6-debuginfo-6.12.2-6.1
nodejs6-debugsource-6.12.2-6.1
nodejs6-6.12.2-6.1

noarch

nodejs6-docs-6.12.2-6.1

x86_64
nodejs6-devel-6.12.2-6.1
npm6-6.12.2-6.1
nodejs6-debuginfo-6.12.2-6.1
nodejs6-debugsource-6.12.2-6.1
nodejs6-6.12.2-6.1

146339 - SuSE Linux 42.3 openSUSE-SU-2018:0329-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5684

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0329-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00001.html

SuSE Linux 42.3
x86_64
libfreeimage3-3.17.0-5.1
libfreeimageplus3-3.17.0-5.1
freeimage-debugsource-3.17.0-5.1
freeimage-devel-3.17.0-5.1
libfreeimageplus3-debuginfo-3.17.0-5.1
libfreeimage3-debuginfo-3.17.0-5.1

146344 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0352-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0352-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003705.html

SuSE SLES 12 SP2
x86_64
libsndfile1-debuginfo-1.0.25-36.7.2
libsndfile-debugsource-1.0.25-36.7.2
libsndfile1-debuginfo-32bit-1.0.25-36.7.2
libsndfile1-32bit-1.0.25-36.7.2

libsndfile1-1.0.25-36.7.2

SuSE SLED 12 SP3
x86_64
libsndfile1-debuginfo-1.0.25-36.7.2
libsndfile-debugsource-1.0.25-36.7.2
libsndfile1-debuginfo-32bit-1.0.25-36.7.2
libsndfile1-32bit-1.0.25-36.7.2
libsndfile1-1.0.25-36.7.2

SuSE SLED 12 SP2
x86_64
libsndfile1-debuginfo-1.0.25-36.7.2
libsndfile-debugsource-1.0.25-36.7.2
libsndfile1-debuginfo-32bit-1.0.25-36.7.2
libsndfile1-32bit-1.0.25-36.7.2
libsndfile1-1.0.25-36.7.2

SuSE SLES 12 SP3
x86_64
libsndfile1-debuginfo-1.0.25-36.7.2
libsndfile-debugsource-1.0.25-36.7.2
libsndfile1-debuginfo-32bit-1.0.25-36.7.2
libsndfile1-32bit-1.0.25-36.7.2
libsndfile1-1.0.25-36.7.2

193250 - Fedora Linux 26 FEDORA-2018-958b22c73f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12374, CVE-2017-12375, CVE-2017-12376, CVE-2017-12377, CVE-2017-12378, CVE-2017-12379, CVE-2017-12380, CVE-2017-6418, CVE-2017-6419, CVE-2017-6420

Description

The scan detected that the host is missing the following update:
FEDORA-2018-958b22c73f

Observation

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

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

Fedora Core 26

clamav-0.99.3-1.fc26

193253 - Fedora Linux 26 FEDORA-2018-43712163de Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13884, CVE-2017-13885, CVE-2017-7153, CVE-2017-7160, CVE-2017-7161, CVE-2017-7165, CVE-2018-4088, CVE-2018-4096

Description

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

FEDORA-2018-43712163de

Observation

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

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

Fedora Core 26

webkitgtk4-2.18.6-1.fc26

23048 - (VMSA-2018-0002) VMware ESXi Multiple Vulnerabilities

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

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of VMware ESXi.

Observation

VMware ESXi is a popular virtualization platform.

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

23049 - (VMSA-2018-0002) VMware ESXi 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 ESXi.

Observation

VMware ESXi is a popular virtualization platform.

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

23051 - Oracle Application Express Critical Patch Update January 2018

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

Risk Level: Medium

CVE: CVE-2018-2699

Description

A vulnerability is present in some versions of Oracle Application Express.

Observation

Oracle Application Express is an Oracle web-based software development environment that runs on an Oracle database.

A vulnerability is present in some versions of Oracle Application Express. The flaw lies in an undetermined component. Successful exploitation could allow an attacker to compromise integrity of data or obtain sensitive information.

23054 - (K81137982) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6136

Description

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

Observation

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

A denial-of-service vulnerability is present in some versions of F5 BIG-IP products. The flaw is due to improper handling of malicious requests made to virtual servers. Successful exploitation could allow an attacker to cause a denial of service condition.

141864 - Red Hat Enterprise Linux RHSA-2018-0260 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1049

Description

The scan detected that the host is missing the following update:
RHSA-2018-0260

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/msg00092.html

RHEL7D
x86_64
systemd-python-219-42.el7_4.7
systemd-sysv-219-42.el7_4.7
libgudev1-devel-219-42.el7_4.7
systemd-debuginfo-219-42.el7_4.7
systemd-219-42.el7_4.7
systemd-resolved-219-42.el7_4.7
libgudev1-219-42.el7_4.7
systemd-networkd-219-42.el7_4.7
systemd-libs-219-42.el7_4.7
systemd-journal-gateway-219-42.el7_4.7
systemd-devel-219-42.el7_4.7

RHEL7S
x86_64
systemd-python-219-42.el7_4.7
systemd-sysv-219-42.el7_4.7
libgudev1-devel-219-42.el7_4.7
systemd-debuginfo-219-42.el7_4.7
systemd-219-42.el7_4.7

systemd-resolved-219-42.el7_4.7
libgudev1-219-42.el7_4.7
systemd-networkd-219-42.el7_4.7
systemd-libs-219-42.el7_4.7
systemd-journal-gateway-219-42.el7_4.7
systemd-devel-219-42.el7_4.7

RHEL7WS
x86_64
systemd-python-219-42.el7_4.7
systemd-sysv-219-42.el7_4.7
libgudev1-devel-219-42.el7_4.7
systemd-debuginfo-219-42.el7_4.7
systemd-219-42.el7_4.7
systemd-resolved-219-42.el7_4.7
libgudev1-219-42.el7_4.7
systemd-networkd-219-42.el7_4.7
systemd-libs-219-42.el7_4.7
systemd-journal-gateway-219-42.el7_4.7
systemd-devel-219-42.el7_4.7

146323 - SuSE Linux 42.3 openSUSE-SU-2018:0320-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15908, CVE-2018-1049

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0320-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00118.html

SuSE Linux 42.3
i586
udev-228-41.1
systemd-debugsource-228-41.1
libudev-mini-devel-228-41.1
libsystemd0-mini-debuginfo-228-41.1
systemd-debuginfo-228-41.1
nss-myhostname-debuginfo-228-41.1
libudev1-debuginfo-228-41.1
nss-myhostname-228-41.1
nss-mymachines-228-41.1
systemd-mini-sysvinit-228-41.1
systemd-devel-228-41.1
nss-mymachines-debuginfo-228-41.1
libsystemd0-228-41.1
udev-mini-debuginfo-228-41.1
libsystemd0-mini-228-41.1
libsystemd0-debuginfo-228-41.1
systemd-mini-debugsource-228-41.1
udev-debuginfo-228-41.1
libudev-devel-228-41.1

udev-mini-228-41.1
libudev-mini1-228-41.1
systemd-mini-228-41.1
libudev-mini1-debuginfo-228-41.1
systemd-mini-devel-228-41.1
systemd-sysvinit-228-41.1
systemd-logger-228-41.1
systemd-mini-debuginfo-228-41.1
libudev1-228-41.1
systemd-228-41.1

noarch
systemd-mini-bash-completion-228-41.1
systemd-bash-completion-228-41.1

x86_64
udev-228-41.1
systemd-debugsource-228-41.1
systemd-debuginfo-32bit-228-41.1
libudev-mini-devel-228-41.1
libsystemd0-mini-debuginfo-228-41.1
systemd-debuginfo-228-41.1
nss-myhostname-debuginfo-228-41.1
libudev1-debuginfo-228-41.1
nss-myhostname-228-41.1
libudev1-32bit-228-41.1
nss-mymachines-228-41.1
systemd-mini-sysvinit-228-41.1
systemd-32bit-228-41.1
systemd-devel-228-41.1
nss-mymachines-debuginfo-228-41.1
libsystemd0-228-41.1
udev-mini-debuginfo-228-41.1
libsystemd0-mini-228-41.1
libsystemd0-debuginfo-228-41.1
systemd-mini-debugsource-228-41.1
udev-debuginfo-228-41.1
libudev-devel-228-41.1
udev-mini-228-41.1
nss-myhostname-32bit-228-41.1
libsystemd0-debuginfo-32bit-228-41.1
libudev-mini1-228-41.1
systemd-mini-228-41.1
libudev-mini1-debuginfo-228-41.1
systemd-mini-devel-228-41.1
nss-myhostname-debuginfo-32bit-228-41.1
systemd-sysvinit-228-41.1
systemd-logger-228-41.1
libudev1-debuginfo-32bit-228-41.1
libsystemd0-32bit-228-41.1
systemd-mini-debuginfo-228-41.1
libudev1-228-41.1
systemd-228-41.1

146324 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0339-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9262, CVE-2016-9388, CVE-2016-9389, CVE-2016-9390, CVE-2016-9391, CVE-2016-9392, CVE-2016-9393, CVE-

2016-9394, CVE-2017-1000050

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0339-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003697.html

SuSE SLED 12 SP3
x86_64
libjasper1-1.900.14-195.5.1
libjasper1-debuginfo-32bit-1.900.14-195.5.1
libjasper1-debuginfo-1.900.14-195.5.1
jasper-debuginfo-1.900.14-195.5.1
jasper-debugsource-1.900.14-195.5.1
libjasper1-32bit-1.900.14-195.5.1

SuSE SLES 12 SP3
x86_64
libjasper1-1.900.14-195.5.1
libjasper1-debuginfo-32bit-1.900.14-195.5.1
libjasper1-debuginfo-1.900.14-195.5.1
jasper-debuginfo-1.900.14-195.5.1
jasper-debugsource-1.900.14-195.5.1
libjasper1-32bit-1.900.14-195.5.1

146345 - SuSE SLES 11 SP4 SUSE-SU-2018:0351-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0351-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003704.html

SuSE SLES 11 SP4
i586
libsndfile-1.0.20-2.19.7.3

x86_64
libsndfile-1.0.20-2.19.7.3
libsndfile-32bit-1.0.20-2.19.7.3

160358 - CentOS 7 CESA-2018-0260 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1049

Description

The scan detected that the host is missing the following update:
CESA-2018-0260

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-February/022760.html

CentOS 7
x86_64
systemd-python-219-42.el7_4.7
systemd-networkd-219-42.el7_4.7
libgudev1-devel-219-42.el7_4.7
systemd-sysv-219-42.el7_4.7
systemd-219-42.el7_4.7
libgudev1-219-42.el7_4.7
systemd-resolved-219-42.el7_4.7
systemd-libs-219-42.el7_4.7
systemd-journal-gateway-219-42.el7_4.7
systemd-devel-219-42.el7_4.7

i686
systemd-libs-219-42.el7_4.7
systemd-resolved-219-42.el7_4.7
libgudev1-devel-219-42.el7_4.7
libgudev1-219-42.el7_4.7
systemd-devel-219-42.el7_4.7

163544 - Oracle Enterprise Linux ELSA-2018-0260 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1049

Description

The scan detected that the host is missing the following update:
ELSA-2018-0260

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-February/007521.html

OEL7
x86_64
libgudev1-devel-219-42.0.2.el7_4.7
systemd-networkd-219-42.0.2.el7_4.7
libgudev1-219-42.0.2.el7_4.7
systemd-journal-gateway-219-42.0.2.el7_4.7

systemd-python-219-42.0.2.el7_4.7
systemd-libs-219-42.0.2.el7_4.7
systemd-sysv-219-42.0.2.el7_4.7
systemd-devel-219-42.0.2.el7_4.7
systemd-219-42.0.2.el7_4.7
systemd-resolved-219-42.0.2.el7_4.7

175324 - Scientific Linux Security ERRATA Moderate: systemd on SL7.x x86_64 (1801-10196)

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

Risk Level: Medium

CVE: CVE-2018-1049

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: systemd on SL7.x x86_64 (1801-10196)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=10196

SL7
x86_64
systemd-python-219-42.el7_4.7
systemd-sysv-219-42.el7_4.7
libgudev1-devel-219-42.el7_4.7
systemd-debuginfo-219-42.el7_4.7
systemd-219-42.el7_4.7
systemd-resolved-219-42.el7_4.7
libgudev1-219-42.el7_4.7
systemd-networkd-219-42.el7_4.7
systemd-libs-219-42.el7_4.7
systemd-journal-gateway-219-42.el7_4.7
systemd-devel-219-42.el7_4.7

186079 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3557-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2569, CVE-2016-2570, CVE-2016-2571, CVE-2016-3948, CVE-2018-1000024, CVE-2018-1000027

Description

The scan detected that the host is missing the following update:
USN-3557-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004265.html

Ubuntu 16.04

squid3_3.5.12-1ubuntu7.5

Ubuntu 14.04

squid3_3.3.8-1ubuntu6.11

Ubuntu 17.10

squid3_3.5.23-5ubuntu1.1

186084 - Ubuntu Linux 14.04, 16.04 USN-3558-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15908, CVE-2018-1049

Description

The scan detected that the host is missing the following update:
USN-3558-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004266.html

Ubuntu 14.04

systemd_204-5ubuntu20.26

Ubuntu 16.04

systemd_229-4ubuntu21.1

193244 - Fedora Linux 26 FEDORA-2018-034101216d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5764

Description

The scan detected that the host is missing the following update:
FEDORA-2018-034101216d

Observation

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

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

Fedora Core 26

rsync-3.1.3-2.fc26

193247 - Fedora Linux 27 FEDORA-2018-d0ebfab3f3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5764

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d0ebfab3f3

Observation

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

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

Fedora Core 27

rsync-3.1.3-1.fc27

88914 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-034-01 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
SSA:2018-034-01

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.428639

Slackware 14.0
x86_64
php-5.6.33-x86_64-1

Slackware 14.2
x86_64
php-5.6.33-x86_64-1

i586
php-5.6.33-i586-1

Slackware 14.1
x86_64
php-5.6.33-x86_64-1

146321 - SuSE Linux 42.3 openSUSE-SU-2018:0318-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0318-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00116.html

SuSE Linux 42.3
i586
php7-posix-debuginfo-7.0.7-28.1
php7-enchant-debuginfo-7.0.7-28.1
php7-shmop-debuginfo-7.0.7-28.1
php7-imap-debuginfo-7.0.7-28.1
php7-readline-debuginfo-7.0.7-28.1
php7-xmlrpc-7.0.7-28.1
php7-gd-debuginfo-7.0.7-28.1
php7-firebird-7.0.7-28.1
php7-pspell-debuginfo-7.0.7-28.1
php7-fastcgi-7.0.7-28.1
php7-xmlreader-7.0.7-28.1
php7-sysvsem-7.0.7-28.1
php7-dom-7.0.7-28.1
php7-opcache-7.0.7-28.1
php7-enchant-7.0.7-28.1
php7-snmp-7.0.7-28.1
php7-xmlrpc-debuginfo-7.0.7-28.1
php7-sockets-debuginfo-7.0.7-28.1
php7-intl-7.0.7-28.1
php7-bz2-debuginfo-7.0.7-28.1
php7-ctype-7.0.7-28.1
php7-gettext-debuginfo-7.0.7-28.1
php7-soap-debuginfo-7.0.7-28.1
php7-pgsql-7.0.7-28.1
php7-opcache-debuginfo-7.0.7-28.1
php7-sockets-7.0.7-28.1
php7-ftp-7.0.7-28.1
php7-odbc-7.0.7-28.1
php7-gd-7.0.7-28.1
php7-intl-debuginfo-7.0.7-28.1
php7-phar-debuginfo-7.0.7-28.1
php7-pspell-7.0.7-28.1
php7-xmlreader-debuginfo-7.0.7-28.1
apache2-mod_php7-7.0.7-28.1
php7-mysql-debuginfo-7.0.7-28.1
php7-xmlwriter-7.0.7-28.1
php7-calendar-7.0.7-28.1
php7-readline-7.0.7-28.1
php7-tidy-debuginfo-7.0.7-28.1
php7-mcrypt-7.0.7-28.1
php7-curl-debuginfo-7.0.7-28.1
php7-pgsql-debuginfo-7.0.7-28.1
php7-posix-7.0.7-28.1
php7-tokenizer-7.0.7-28.1
php7-7.0.7-28.1
php7-mcrypt-debuginfo-7.0.7-28.1
php7-xsl-7.0.7-28.1
php7-bz2-7.0.7-28.1
php7-dom-debuginfo-7.0.7-28.1

php7-json-debuginfo-7.0.7-28.1
php7-devel-7.0.7-28.1
php7-dba-7.0.7-28.1
php7-dba-debuginfo-7.0.7-28.1
php7-sysvshm-7.0.7-28.1
php7-sqlite-debuginfo-7.0.7-28.1
apache2-mod_php7-debuginfo-7.0.7-28.1
php7-pcntl-debuginfo-7.0.7-28.1
php7-phar-7.0.7-28.1
php7-gmp-debuginfo-7.0.7-28.1
php7-tidy-7.0.7-28.1
php7-pdo-debuginfo-7.0.7-28.1
php7-fpm-7.0.7-28.1
php7-openssl-7.0.7-28.1
php7-gmp-7.0.7-28.1
php7-exif-7.0.7-28.1
php7-ctype-debuginfo-7.0.7-28.1
php7-zip-7.0.7-28.1
php7-firebird-debuginfo-7.0.7-28.1
php7-sysvmsg-debuginfo-7.0.7-28.1
php7-iconv-7.0.7-28.1
php7-xmlwriter-debuginfo-7.0.7-28.1
php7-zlib-debuginfo-7.0.7-28.1
php7-soap-7.0.7-28.1
php7-openssl-debuginfo-7.0.7-28.1
php7-sysvmsg-7.0.7-28.1
php7-imap-7.0.7-28.1
php7-mbstring-debuginfo-7.0.7-28.1
php7-fastcgi-debuginfo-7.0.7-28.1
php7-mbstring-7.0.7-28.1
php7-calendar-debuginfo-7.0.7-28.1
php7-exif-debuginfo-7.0.7-28.1
php7-sysvsem-debuginfo-7.0.7-28.1
php7-tokenizer-debuginfo-7.0.7-28.1
php7-sysvshm-debuginfo-7.0.7-28.1
php7-ldap-debuginfo-7.0.7-28.1
php7-bcmath-7.0.7-28.1
php7-fileinfo-debuginfo-7.0.7-28.1
php7-snmp-debuginfo-7.0.7-28.1
php7-zip-debuginfo-7.0.7-28.1
php7-curl-7.0.7-28.1
php7-debuginfo-7.0.7-28.1
php7-wddx-7.0.7-28.1
php7-sqlite-7.0.7-28.1
php7-fileinfo-7.0.7-28.1
php7-pdo-7.0.7-28.1
php7-odbc-debuginfo-7.0.7-28.1
php7-mysql-7.0.7-28.1
php7-debugsource-7.0.7-28.1
php7-ldap-7.0.7-28.1
php7-pcntl-7.0.7-28.1
php7-wddx-debuginfo-7.0.7-28.1
php7-ftp-debuginfo-7.0.7-28.1
php7-xsl-debuginfo-7.0.7-28.1
php7-shmop-7.0.7-28.1
php7-iconv-debuginfo-7.0.7-28.1
php7-bcmath-debuginfo-7.0.7-28.1
php7-json-7.0.7-28.1
php7-fpm-debuginfo-7.0.7-28.1
php7-zlib-7.0.7-28.1

php7-gettext-7.0.7-28.1

noarch
php7-pear-7.0.7-28.1
php7-pear-Archive_Tar-7.0.7-28.1

x86_64
php7-posix-debuginfo-7.0.7-28.1
php7-enchant-debuginfo-7.0.7-28.1
php7-shmop-debuginfo-7.0.7-28.1
php7-imap-debuginfo-7.0.7-28.1
php7-readline-debuginfo-7.0.7-28.1
php7-xmlrpc-7.0.7-28.1
php7-gd-debuginfo-7.0.7-28.1
php7-firebird-7.0.7-28.1
php7-pspell-debuginfo-7.0.7-28.1
php7-fastcgi-7.0.7-28.1
php7-xmlreader-7.0.7-28.1
php7-sysvsem-7.0.7-28.1
php7-dom-7.0.7-28.1
php7-opcache-7.0.7-28.1
php7-enchant-7.0.7-28.1
php7-snmp-7.0.7-28.1
php7-xmlrpc-debuginfo-7.0.7-28.1
php7-sockets-debuginfo-7.0.7-28.1
php7-intl-7.0.7-28.1
php7-bz2-debuginfo-7.0.7-28.1
php7-ctype-7.0.7-28.1
php7-gettext-debuginfo-7.0.7-28.1
php7-soap-debuginfo-7.0.7-28.1
php7-pgsql-7.0.7-28.1
php7-opcache-debuginfo-7.0.7-28.1
php7-sockets-7.0.7-28.1
php7-ftp-7.0.7-28.1
php7-odbc-7.0.7-28.1
php7-gd-7.0.7-28.1
php7-intl-debuginfo-7.0.7-28.1
php7-phar-debuginfo-7.0.7-28.1
php7-pspell-7.0.7-28.1
php7-xmlreader-debuginfo-7.0.7-28.1
apache2-mod_php7-7.0.7-28.1
php7-mysql-debuginfo-7.0.7-28.1
php7-xmlwriter-7.0.7-28.1
php7-calendar-7.0.7-28.1
php7-readline-7.0.7-28.1
php7-tidy-debuginfo-7.0.7-28.1
php7-mcrypt-7.0.7-28.1
php7-curl-debuginfo-7.0.7-28.1
php7-pgsql-debuginfo-7.0.7-28.1
php7-posix-7.0.7-28.1
php7-tokenizer-7.0.7-28.1
php7-7.0.7-28.1
php7-mcrypt-debuginfo-7.0.7-28.1
php7-xsl-7.0.7-28.1
php7-bz2-7.0.7-28.1
php7-dom-debuginfo-7.0.7-28.1
php7-json-debuginfo-7.0.7-28.1
php7-devel-7.0.7-28.1
php7-dba-7.0.7-28.1
php7-dba-debuginfo-7.0.7-28.1

php7-sysvshm-7.0.7-28.1
php7-sqlite-debuginfo-7.0.7-28.1
apache2-mod_php7-debuginfo-7.0.7-28.1
php7-pcntl-debuginfo-7.0.7-28.1
php7-phar-7.0.7-28.1
php7-gmp-debuginfo-7.0.7-28.1
php7-tidy-7.0.7-28.1
php7-pdo-debuginfo-7.0.7-28.1
php7-fpm-7.0.7-28.1
php7-openssl-7.0.7-28.1
php7-gmp-7.0.7-28.1
php7-exif-7.0.7-28.1
php7-ctype-debuginfo-7.0.7-28.1
php7-zip-7.0.7-28.1
php7-firebird-debuginfo-7.0.7-28.1
php7-sysvmsg-debuginfo-7.0.7-28.1
php7-iconv-7.0.7-28.1
php7-xmlwriter-debuginfo-7.0.7-28.1
php7-zlib-debuginfo-7.0.7-28.1
php7-soap-7.0.7-28.1
php7-openssl-debuginfo-7.0.7-28.1
php7-sysvmsg-7.0.7-28.1
php7-imap-7.0.7-28.1
php7-mbstring-debuginfo-7.0.7-28.1
php7-fastcgi-debuginfo-7.0.7-28.1
php7-mbstring-7.0.7-28.1
php7-calendar-debuginfo-7.0.7-28.1
php7-exif-debuginfo-7.0.7-28.1
php7-sysvsem-debuginfo-7.0.7-28.1
php7-tokenizer-debuginfo-7.0.7-28.1
php7-sysvshm-debuginfo-7.0.7-28.1
php7-ldap-debuginfo-7.0.7-28.1
php7-bcmath-7.0.7-28.1
php7-fileinfo-debuginfo-7.0.7-28.1
php7-snmp-debuginfo-7.0.7-28.1
php7-zip-debuginfo-7.0.7-28.1
php7-curl-7.0.7-28.1
php7-debuginfo-7.0.7-28.1
php7-wddx-7.0.7-28.1
php7-sqlite-7.0.7-28.1
php7-fileinfo-7.0.7-28.1
php7-pdo-7.0.7-28.1
php7-odbc-debuginfo-7.0.7-28.1
php7-mysql-7.0.7-28.1
php7-debugsource-7.0.7-28.1
php7-ldap-7.0.7-28.1
php7-pcntl-7.0.7-28.1
php7-wddx-debuginfo-7.0.7-28.1
php7-ftp-debuginfo-7.0.7-28.1
php7-xsl-debuginfo-7.0.7-28.1
php7-shmop-7.0.7-28.1
php7-iconv-debuginfo-7.0.7-28.1
php7-bcmath-debuginfo-7.0.7-28.1
php7-json-7.0.7-28.1
php7-fpm-debuginfo-7.0.7-28.1
php7-zlib-7.0.7-28.1
php7-gettext-7.0.7-28.1

146325 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0372-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15108

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0372-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003708.html

SuSE SLES 12 SP2
x86_64
spice-vdagent-debuginfo-0.16.0-8.5.15
spice-vdagent-debugsource-0.16.0-8.5.15
spice-vdagent-0.16.0-8.5.15

SuSE SLED 12 SP3
x86_64
spice-vdagent-debuginfo-0.16.0-8.5.15
spice-vdagent-debugsource-0.16.0-8.5.15
spice-vdagent-0.16.0-8.5.15

SuSE SLED 12 SP2
x86_64
spice-vdagent-debuginfo-0.16.0-8.5.15
spice-vdagent-debugsource-0.16.0-8.5.15
spice-vdagent-0.16.0-8.5.15

SuSE SLES 12 SP3
x86_64
spice-vdagent-debuginfo-0.16.0-8.5.15
spice-vdagent-debugsource-0.16.0-8.5.15
spice-vdagent-0.16.0-8.5.15

146333 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0373-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15232

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0373-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003709.html

SuSE SLES 12 SP2
x86_64

libturbojpeg0-debuginfo-8.1.2-31.7.4
libjpeg-turbo-debugsource-1.5.3-31.7.4
libjpeg-turbo-debuginfo-1.5.3-31.7.4
libjpeg8-debuginfo-32bit-8.1.2-31.7.4
libjpeg8-32bit-8.1.2-31.7.4
libjpeg62-turbo-1.5.3-31.7.4
libjpeg62-32bit-62.2.0-31.7.4
libjpeg-turbo-1.5.3-31.7.4
libjpeg62-debuginfo-32bit-62.2.0-31.7.4
libjpeg8-debuginfo-8.1.2-31.7.4
libturbojpeg0-8.1.2-31.7.4
libjpeg8-8.1.2-31.7.4
libjpeg62-debuginfo-62.2.0-31.7.4
libjpeg62-turbo-debugsource-1.5.3-31.7.4
libjpeg62-62.2.0-31.7.4

SuSE SLED 12 SP3
x86_64
libturbojpeg0-debuginfo-8.1.2-31.7.4
libjpeg-turbo-debugsource-1.5.3-31.7.4
libjpeg-turbo-debuginfo-1.5.3-31.7.4
libjpeg8-debuginfo-32bit-8.1.2-31.7.4
libjpeg8-32bit-8.1.2-31.7.4
libjpeg62-turbo-1.5.3-31.7.4
libjpeg62-32bit-62.2.0-31.7.4
libjpeg-turbo-1.5.3-31.7.4
libjpeg62-debuginfo-32bit-62.2.0-31.7.4
libjpeg8-debuginfo-8.1.2-31.7.4
libturbojpeg0-8.1.2-31.7.4
libjpeg8-8.1.2-31.7.4
libjpeg62-debuginfo-62.2.0-31.7.4
libjpeg62-turbo-debugsource-1.5.3-31.7.4
libjpeg62-62.2.0-31.7.4

SuSE SLED 12 SP2
x86_64
libturbojpeg0-debuginfo-8.1.2-31.7.4
libjpeg-turbo-debugsource-1.5.3-31.7.4
libjpeg-turbo-debuginfo-1.5.3-31.7.4
libjpeg8-debuginfo-32bit-8.1.2-31.7.4
libjpeg8-32bit-8.1.2-31.7.4
libjpeg62-turbo-1.5.3-31.7.4
libjpeg62-32bit-62.2.0-31.7.4
libjpeg-turbo-1.5.3-31.7.4
libjpeg62-debuginfo-32bit-62.2.0-31.7.4
libjpeg8-debuginfo-8.1.2-31.7.4
libturbojpeg0-8.1.2-31.7.4
libjpeg8-8.1.2-31.7.4
libjpeg62-debuginfo-62.2.0-31.7.4
libjpeg62-turbo-debugsource-1.5.3-31.7.4
libjpeg62-62.2.0-31.7.4

SuSE SLES 12 SP3
x86_64
libturbojpeg0-debuginfo-8.1.2-31.7.4
libjpeg-turbo-debugsource-1.5.3-31.7.4
libjpeg-turbo-debuginfo-1.5.3-31.7.4
libjpeg8-debuginfo-32bit-8.1.2-31.7.4
libjpeg8-32bit-8.1.2-31.7.4
libjpeg62-turbo-1.5.3-31.7.4

libjpeg62-32bit-62.2.0-31.7.4
libjpeg-turbo-1.5.3-31.7.4
libjpeg62-debuginfo-32bit-62.2.0-31.7.4
libjpeg8-debuginfo-8.1.2-31.7.4
libturbojpeg0-8.1.2-31.7.4
libjpeg8-8.1.2-31.7.4
libjpeg62-debuginfo-62.2.0-31.7.4
libjpeg62-turbo-debugsource-1.5.3-31.7.4
libjpeg62-62.2.0-31.7.4

146336 - SuSE Linux 42.3 openSUSE-SU-2018:0316-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5711

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0316-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00114.html

SuSE Linux 42.3
x86_64
gd-debuginfo-32bit-2.1.0-24.1
gd-devel-2.1.0-24.1
gd-2.1.0-24.1
gd-32bit-2.1.0-24.1
gd-debuginfo-2.1.0-24.1
gd-debugsource-2.1.0-24.1

i586
gd-debuginfo-2.1.0-24.1
gd-devel-2.1.0-24.1
gd-2.1.0-24.1
gd-debugsource-2.1.0-24.1

146340 - SuSE Linux 42.3 openSUSE-SU-2018:0328-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13063, CVE-2017-13065, CVE-2017-18027, CVE-2017-18029, CVE-2018-5685

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0328-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00000.html

SuSE Linux 42.3
x86_64
perl-GraphicsMagick-1.3.25-63.1
libGraphicsMagick++-Q16-12-1.3.25-63.1
libGraphicsMagickWand-Q16-2-1.3.25-63.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-63.1
libGraphicsMagick++-devel-1.3.25-63.1
GraphicsMagick-debuginfo-1.3.25-63.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-63.1
GraphicsMagick-debugsource-1.3.25-63.1
GraphicsMagick-devel-1.3.25-63.1
libGraphicsMagick-Q16-3-1.3.25-63.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-63.1
perl-GraphicsMagick-debuginfo-1.3.25-63.1
libGraphicsMagick3-config-1.3.25-63.1
GraphicsMagick-1.3.25-63.1

i586
perl-GraphicsMagick-1.3.25-63.1
libGraphicsMagick++-Q16-12-1.3.25-63.1
libGraphicsMagickWand-Q16-2-1.3.25-63.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-63.1
libGraphicsMagick++-devel-1.3.25-63.1
GraphicsMagick-debuginfo-1.3.25-63.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-63.1
GraphicsMagick-debugsource-1.3.25-63.1
GraphicsMagick-devel-1.3.25-63.1
libGraphicsMagick-Q16-3-1.3.25-63.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-63.1
perl-GraphicsMagick-debuginfo-1.3.25-63.1
libGraphicsMagick3-config-1.3.25-63.1
GraphicsMagick-1.3.25-63.1

170919 - Amazon Linux AMI ALAS-2018-942 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
ALAS-2018-942

Observation

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

https://alas.aws.amazon.com/ALAS-2018-942.html

Amazon Linux AMI
x86_64
qemu-img-1.5.3-141.6.amzn1
qemu-kvm-tools-1.5.3-141.6.amzn1
qemu-kvm-common-1.5.3-141.6.amzn1
qemu-kvm-1.5.3-141.6.amzn1
qemu-kvm-debuginfo-1.5.3-141.6.amzn1

170921 - Amazon Linux AMI ALAS-2018-941 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14992

Description

The scan detected that the host is missing the following update:
ALAS-2018-941

Observation

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

https://alas.aws.amazon.com/ALAS-2018-941.html

Amazon Linux AMI
x86_64
docker-debuginfo-17.09.1ce-1.111.amzn1
docker-17.09.1ce-1.111.amzn1

193245 - Fedora Linux 27 FEDORA-2018-7982ad5f2a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17858, CVE-2018-5686

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7982ad5f2a

Observation

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

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

Fedora Core 27

mupdf-1.12.0-2.fc27

193259 - Fedora Linux 26 FEDORA-2018-7151603128 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17858, CVE-2018-5686

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7151603128

Observation

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

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

Fedora Core 26

mupdf-1.12.0-2.fc26

193264 - Fedora Linux 27 FEDORA-2018-c587c0a62d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1042, CVE-2018-1043, CVE-2018-1044, CVE-2018-1045

Description

The scan detected that the host is missing the following update:
FEDORA-2018-c587c0a62d

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

moodle-3.3.4-1.fc27

193265 - Fedora Linux 26 FEDORA-2018-7e086e3309 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1042, CVE-2018-1043, CVE-2018-1044, CVE-2018-1045

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7e086e3309

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 26

moodle-3.2.7-1.fc26

131011 - Debian Linux 8.0, 9.0 DSA-4104-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17969

Description

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

DSA-4104-1

Observation

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

http://www.debian.org/security/2018/dsa-4104

Debian 8.0
all
p7zip_9.20.1~dfsg.1-4.1+deb8u3

Debian 9.0
all
p7zip_16.02+dfsg-3+deb9u1

131012 - Debian Linux 9.0 DSA-4103-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15420, CVE-2017-15429, CVE-2018-6031, CVE-2018-6032, CVE-2018-6033, CVE-2018-6034, CVE-2018-6035, CVE-2018-6036, CVE-2018-6037, CVE-2018-6038, CVE-2018-6039, CVE-2018-6040, CVE-2018-6041, CVE-2018-6042, CVE-2018-6043, CVE-2018-6045, CVE-2018-6046, CVE-2018-6047, CVE-2018-6048, CVE-2018-6049, CVE-2018-6050, CVE-2018-6051, CVE-2018-6052, CVE-2018-6053, CVE-2018-6054

Description

The scan detected that the host is missing the following update:
DSA-4103-1

Observation

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

http://www.debian.org/security/2018/dsa-4103

Debian 9.0
all
chromium-shell_64.0.3282.119-1~deb9u1
chromium_64.0.3282.119-1~deb9u1
chromium-widevine_64.0.3282.119-1~deb9u1
chromium-driver_64.0.3282.119-1~deb9u1
chromium-l10n_64.0.3282.119-1~deb9u1
chromedriver_64.0.3282.119-1~deb9u1

146341 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0334-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13720, CVE-2017-13722

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0334-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003693.html

SuSE SLES 12 SP2
x86_64
libXfont-debugsource-1.5.1-11.3.12
libXfont1-debuginfo-1.5.1-11.3.12
libXfont1-1.5.1-11.3.12

SuSE SLED 12 SP3
x86_64
libXfont-debugsource-1.5.1-11.3.12
libXfont1-debuginfo-1.5.1-11.3.12
libXfont1-1.5.1-11.3.12

SuSE SLED 12 SP2
x86_64
libXfont-debugsource-1.5.1-11.3.12
libXfont1-debuginfo-1.5.1-11.3.12
libXfont1-1.5.1-11.3.12

SuSE SLES 12 SP3
x86_64
libXfont-debugsource-1.5.1-11.3.12
libXfont1-debuginfo-1.5.1-11.3.12
libXfont1-1.5.1-11.3.12

146350 - SuSE Linux 42.3 openSUSE-SU-2018:0343-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13720, CVE-2017-13722

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0343-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00005.html

SuSE Linux 42.3
x86_64
libXfont-devel-32bit-1.5.1-13.1
libXfont1-debuginfo-1.5.1-13.1
libXfont1-32bit-1.5.1-13.1
libXfont1-1.5.1-13.1
libXfont1-debuginfo-32bit-1.5.1-13.1
libXfont-devel-1.5.1-13.1
libXfont-debugsource-1.5.1-13.1

i586
libXfont1-debuginfo-1.5.1-13.1
libXfont-debugsource-1.5.1-13.1

libXfont-devel-1.5.1-13.1
libXfont1-1.5.1-13.1

182588 - FreeBSD Django Information Leakage (d696473f-9f32-42c5-a106-bf4536fb1f74)

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

Risk Level: Low

CVE: CVE-2018-6188

Description

The scan detected that the host is missing the following update:
Django -- information leakage (d696473f-9f32-42c5-a106-bf4536fb1f74)

Observation

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

http://www.vuxml.org/freebsd/d696473f-9f32-42c5-a106-bf4536fb1f74.html

Affected packages:
py27-django111 < 1.11.10
py34-django111 < 1.11.10
py35-django111 < 1.11.10
py36-django111 < 1.11.10
py27-django20 < 2.0.2
py34-django20 < 2.0.2
py35-django20 < 2.0.2
py36-django20 < 2.0.2

182589 - FreeBSD palemoon Multiple Vulnerabilities (5044bd23-08cb-11e8-b08f-00012e582166)

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

Risk Level: Low

CVE: CVE-2018-5102, CVE-2018-5122

Description

The scan detected that the host is missing the following update:
palemoon -- multiple vulnerabilities (5044bd23-08cb-11e8-b08f-00012e582166)

Observation

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

http://www.vuxml.org/freebsd/5044bd23-08cb-11e8-b08f-00012e582166.html

Affected packages:
palemoon < 27.7.2

182590 - FreeBSD W3m - Multiple Vulnerabilities (e72d5bf5-07a0-11e8-8248-0021ccb9e74d)

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
w3m - multiple vulnerabilities (e72d5bf5-07a0-11e8-8248-0021ccb9e74d)

Observation

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

http://www.vuxml.org/freebsd/e72d5bf5-07a0-11e8-8248-0021ccb9e74d.html

Affected packages:
w3m < 0.5.3.20180125
w3m-img < 0.5.3.20180125
ja-w3m < 0.5.3.20180125
ja-w3m-img < 0.5.3.20180125

182591 - FreeBSD Flash Player Multiple Vulnerabilities (756a8631-0b84-11e8-a986-6451062f0f7a)

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
Flash Player -- multiple vulnerabilities (756a8631-0b84-11e8-a986-6451062f0f7a)

Observation

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

http://www.vuxml.org/freebsd/756a8631-0b84-11e8-a986-6451062f0f7a.html

Affected packages:
linux-flashplayer < 28.0.0.161

182592 - FreeBSD shadowsocks-libev Command Injection Via Shell Metacharacters (3746de31-0a1a-11e8-83e7-485b3931c969)

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:
shadowsocks-libev -- command injection via shell metacharacters (3746de31-0a1a-11e8-83e7-485b3931c969)

Observation

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

http://www.vuxml.org/freebsd/3746de31-0a1a-11e8-83e7-485b3931c969.html

Affected packages:
3.1.0 <= shadowsocks-libev < 3.1.1

182593 - FreeBSD mini_httpd,thttpd Buffer Overflow In Htpasswd (f5524753-67b1-4c88-8114-29c2d258b383)

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:
mini_httpd,thttpd -- Buffer overflow in htpasswd (f5524753-67b1-4c88-8114-29c2d258b383)

Observation

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

http://www.vuxml.org/freebsd/f5524753-67b1-4c88-8114-29c2d258b383.html

Affected packages:
mini_httpd < 1.28
thttpd < 2.28

186087 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3552-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5124

Description

The scan detected that the host is missing the following update:
USN-3552-1

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/004257.html

Ubuntu 16.04

firefox_58.0.1+build1-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_58.0.1+build1-0ubuntu0.14.04.1

Ubuntu 17.10

firefox_58.0.1+build1-0ubuntu0.17.10.1

193239 - Fedora Linux 27 FEDORA-2018-a24be2586d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6381

Description

The scan detected that the host is missing the following update:
FEDORA-2018-a24be2586d

Observation

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

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

Fedora Core 27

zziplib-0.13.67-1.fc27

193241 - Fedora Linux 26 FEDORA-2018-cd4311d4d6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17969

Description

The scan detected that the host is missing the following update:
FEDORA-2018-cd4311d4d6

Observation

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

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

Fedora Core 26

p7zip-16.02-9.fc26

193242 - Fedora Linux 27 FEDORA-2018-74bb00f644 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-2018-74bb00f644

Observation

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

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

Fedora Core 27

thunderbird-52.6.0-1.fc27

193246 - Fedora Linux 27 FEDORA-2018-f8ad787538 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17969

Description

The scan detected that the host is missing the following update:
FEDORA-2018-f8ad787538

Observation

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

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

Fedora Core 27

p7zip-16.02-9.fc27

193248 - Fedora Linux 26 FEDORA-2018-b5ecac9405 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-b5ecac9405

Observation

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

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

Fedora Core 26

flatpak-0.10.3-1.fc26

193249 - Fedora Linux 27 FEDORA-2018-0b48740047 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15706

Description

The scan detected that the host is missing the following update:
FEDORA-2018-0b48740047

Observation

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

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

Fedora Core 27

tomcat-8.0.49-1.fc27

193251 - Fedora Linux 27 FEDORA-2018-4fabf63492 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000024, CVE-2018-1000027

Description

The scan detected that the host is missing the following update:
FEDORA-2018-4fabf63492

Observation

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

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

Fedora Core 27

squid-4.0.23-2.fc27

193252 - Fedora Linux 27 FEDORA-2017-d7c0748c1b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15091

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d7c0748c1b

Observation

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

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

Fedora Core 27

pdns-4.1.0-1.fc27

193255 - Fedora Linux 26 FEDORA-2018-ef303deec6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6003

Description

The scan detected that the host is missing the following update:
FEDORA-2018-ef303deec6

Observation

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

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

Fedora Core 26

libtasn1-4.13-1.fc26

193256 - Fedora Linux 27 FEDORA-2018-79db828bff 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-2018-79db828bff

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

firefox-58.0.1-1.fc27

193258 - Fedora Linux 26 FEDORA-2018-9780220f7d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15107

Description

The scan detected that the host is missing the following update:
FEDORA-2018-9780220f7d

Observation

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

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

Fedora Core 26

dnsmasq-2.76-6.fc26

193260 - Fedora Linux 26 FEDORA-2018-d9706e9f1f 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-d9706e9f1f

Observation

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

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

Fedora Core 26

firefox-58.0.1-1.fc26

193261 - Fedora Linux 26 FEDORA-2018-a10a19e06a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15105

Description

The scan detected that the host is missing the following update:
FEDORA-2018-a10a19e06a

Observation

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

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

Fedora Core 26

unbound-1.6.8-1.fc26

193263 - Fedora Linux 27 FEDORA-2018-bd651734da 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-bd651734da

Observation

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

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

Fedora Core 27

flatpak-0.10.3-1.fc27

146335 - SuSE Linux 42.3 openSUSE-SU-2018:0344-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8946, CVE-2016-6224

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0344-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-02/msg00006.html

SuSE Linux 42.3
x86_64
ecryptfs-utils-32bit-103-7.1
ecryptfs-utils-debuginfo-103-7.1
ecryptfs-utils-103-7.1
ecryptfs-utils-debuginfo-32bit-103-7.1
ecryptfs-utils-debugsource-103-7.1

i586
ecryptfs-utils-debuginfo-103-7.1
ecryptfs-utils-103-7.1
ecryptfs-utils-debugsource-103-7.1

146347 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0336-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8946, CVE-2016-6224

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0336-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-February/003694.html

SuSE SLES 12 SP2
x86_64
ecryptfs-utils-debuginfo-32bit-103-8.3.1
ecryptfs-utils-32bit-103-8.3.1
ecryptfs-utils-103-8.3.1
ecryptfs-utils-debuginfo-103-8.3.1
ecryptfs-utils-debugsource-103-8.3.1

SuSE SLED 12 SP3
x86_64

ecryptfs-utils-debuginfo-32bit-103-8.3.1
ecryptfs-utils-103-8.3.1
ecryptfs-utils-32bit-103-8.3.1
ecryptfs-utils-debuginfo-103-8.3.1
ecryptfs-utils-debugsource-103-8.3.1

SuSE SLED 12 SP2
x86_64
ecryptfs-utils-debuginfo-32bit-103-8.3.1
ecryptfs-utils-103-8.3.1
ecryptfs-utils-32bit-103-8.3.1
ecryptfs-utils-debuginfo-103-8.3.1
ecryptfs-utils-debugsource-103-8.3.1

SuSE SLES 12 SP3
x86_64
ecryptfs-utils-debuginfo-32bit-103-8.3.1
ecryptfs-utils-32bit-103-8.3.1
ecryptfs-utils-103-8.3.1
ecryptfs-utils-debuginfo-103-8.3.1
ecryptfs-utils-debugsource-103-8.3.1

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

22640 - Oracle Database Server Critical Patch Update October 2017

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

Risk Level: High

CVE: CVE-2016-6814, CVE-2016-8735, CVE-2017-10190, CVE-2017-10261, CVE-2017-10292, CVE-2017-10321

Update Details

FASLScript is updated

182255 - FreeBSD groovy Remote Execution Of Untrusted Code/DoS Vulnerability (4af92a40-db33-11e6-ae1b-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-6814

Update Details

Risk is updated

191642 - Fedora Linux 24 FEDORA-2017-1ce2a05ff1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6814

Update Details

Risk is updated

191647 - Fedora Linux 25 FEDORA-2017-cc0e0daf0f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6814

Update Details

Risk is updated

192560 - Fedora Linux 25 FEDORA-2017-33c8085c5d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6814

Update Details

Risk is updated

192565 - Fedora Linux 26 FEDORA-2017-661dddc462 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6814

Update Details

Risk is updated

22197 - Oracle Database Server Critical Patch Update July 2017

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

Risk Level: Medium

CVE: CVE-2014-3566, CVE-2016-2183, CVE-2017-10120, CVE-2017-10202

Update Details

FASLScript is updated

130934 - Debian Linux 8.0, 9.0 DSA-4025-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12197

Update Details

Risk is updated

146288 - SuSE SLES 11 SP4 SUSE-SU-2018:0235-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5711

Update Details

Risk is updated

146303 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0260-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5711

Update Details

Risk is updated

146317 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0248-1 Update Is Not Installed

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

Risk Level: Medium

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

Update Details

Risk is updated

182574 - FreeBSD powerdns-recursor Insufficient Validation Of DNSSEC Signatures (24a82876-002e-11e8-9a95-0cc47a02c232)

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

Risk Level: Medium

CVE: CVE-2018-1000003

Update Details

Risk is updated

182583 - FreeBSD firefox Arbitrary Code Execution Through Unsanitized Browser UI (103bf96a-6211-45ab-b567-1555ebb3a86a)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

182585 - FreeBSD dovecot Abort Of SASL Authentication Results In A Memory Leak (92b8b284-a3a2-41b1-956c-f9cf8b74f500)

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

Risk Level: Low

CVE: CVE-2017-15132

Update Details

FASLScript is updated

DELETED CHECKS

23060 - (APSA18-01) Vulnerability In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2018-4878

23061 - (APSA18-01) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-4878

ADDITIONAL NOTES

- **23060** - is replaced by FID 23068.
- **23061** - is replaced by FID 23069.

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.