2018-FEB-1
FSL version 7.5.998

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

132435 - Oracle VM OVMSA-2018-0015 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10044, CVE-2016-10200, CVE-2016-10229, CVE-2016-6213, CVE-2016-9604, CVE-2017-1000111, CVE-2017-1000251, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-1000407, CVE-2017-11176, CVE-2017-11473, CVE-2017-12134, CVE-2017-2671, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7273, CVE-2017-7308, CVE-2017-7533, CVE-2017-7645, CVE-2017-7895, CVE-2017-8797, CVE-2017-8890, CVE-2017-9059, CVE-2017-9074, CVE-2017-9075, CVE-2017-9077, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0015

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000826.html

OVM3.4
x86_64
kernel-uek-4.1.12-61.63.1.el6uek
kernel-uek-firmware-4.1.12-61.63.1.el6uek

141861 - Red Hat Enterprise Linux RHSA-2018-0169 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11176, CVE-2017-7542, CVE-2017-9074

Description

The scan detected that the host is missing the following update:
RHSA-2018-0169

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/msg00083.html

RHEL6D
i386
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-debuginfo-2.6.32-696.20.1.el6
python-perf-debuginfo-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-2.6.32-696.20.1.el6
perf-debuginfo-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6
kernel-debug-debuginfo-2.6.32-696.20.1.el6
kernel-debuginfo-common-i686-2.6.32-696.20.1.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
python-perf-2.6.32-696.20.1.el6
kernel-2.6.32-696.20.1.el6
perf-debuginfo-2.6.32-696.20.1.el6
python-perf-debuginfo-2.6.32-696.20.1.el6
kernel-debuginfo-common-i686-2.6.32-696.20.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.20.1.el6
kernel-debug-debuginfo-2.6.32-696.20.1.el6
perf-2.6.32-696.20.1.el6
kernel-debug-devel-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6
kernel-debuginfo-2.6.32-696.20.1.el6

RHEL6S
i386
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-debuginfo-2.6.32-696.20.1.el6
python-perf-debuginfo-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-2.6.32-696.20.1.el6
perf-debuginfo-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6
kernel-debug-debuginfo-2.6.32-696.20.1.el6
kernel-debuginfo-common-i686-2.6.32-696.20.1.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
python-perf-2.6.32-696.20.1.el6
kernel-2.6.32-696.20.1.el6
perf-debuginfo-2.6.32-696.20.1.el6
python-perf-debuginfo-2.6.32-696.20.1.el6
kernel-debuginfo-common-i686-2.6.32-696.20.1.el6

kernel-debuginfo-common-x86_64-2.6.32-696.20.1.el6
kernel-debug-debuginfo-2.6.32-696.20.1.el6
perf-2.6.32-696.20.1.el6
kernel-debug-devel-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6
kernel-debuginfo-2.6.32-696.20.1.el6

RHEL6WS
i386
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-debuginfo-2.6.32-696.20.1.el6
python-perf-debuginfo-2.6.32-696.20.1.el6
kernel-debug-devel-2.6.32-696.20.1.el6
kernel-2.6.32-696.20.1.el6
perf-debuginfo-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6
kernel-debug-debuginfo-2.6.32-696.20.1.el6
kernel-debuginfo-common-i686-2.6.32-696.20.1.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-debuginfo-2.6.32-696.20.1.el6
python-perf-debuginfo-2.6.32-696.20.1.el6
kernel-debug-devel-2.6.32-696.20.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.20.1.el6
kernel-2.6.32-696.20.1.el6
perf-debuginfo-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6
kernel-debug-debuginfo-2.6.32-696.20.1.el6
kernel-debuginfo-common-i686-2.6.32-696.20.1.el6

163538 - Oracle Enterprise Linux ELSA-2018-0169 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11176, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7542, CVE-2017-9074

Description

The scan detected that the host is missing the following update:
ELSA-2018-0169

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007509.html

OEL6
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-abi-whitelists-2.6.32-696.20.1.el6
kernel-doc-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-2.6.32-696.20.1.el6
kernel-firmware-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6

i386
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-abi-whitelists-2.6.32-696.20.1.el6
kernel-doc-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-2.6.32-696.20.1.el6
kernel-firmware-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6

175321 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1801-9818)

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

Risk Level: High

CVE: CVE-2017-11176, CVE-2017-7542, CVE-2017-9074

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1801-9818)

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=9818

SL6
i386
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-debuginfo-2.6.32-696.20.1.el6
python-perf-debuginfo-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-2.6.32-696.20.1.el6
perf-debuginfo-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6
kernel-debug-debuginfo-2.6.32-696.20.1.el6
kernel-debuginfo-common-i686-2.6.32-696.20.1.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
python-perf-2.6.32-696.20.1.el6
kernel-2.6.32-696.20.1.el6
perf-debuginfo-2.6.32-696.20.1.el6
python-perf-debuginfo-2.6.32-696.20.1.el6
kernel-debuginfo-common-i686-2.6.32-696.20.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.20.1.el6
kernel-debug-debuginfo-2.6.32-696.20.1.el6
perf-2.6.32-696.20.1.el6
kernel-debug-devel-2.6.32-696.20.1.el6
kernel-headers-2.6.32-696.20.1.el6
kernel-debuginfo-2.6.32-696.20.1.el6

193221 - Fedora Linux 27 FEDORA-2018-db610fff5b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4658, CVE-2016-5131, CVE-2017-8872, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050

Description

The scan detected that the host is missing the following update:
FEDORA-2018-db610fff5b

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

libxml2-2.9.7-1.fc27

141860 - Red Hat Enterprise Linux RHSA-2018-0122 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux 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:
RHSA-2018-0122

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/msg00078.html

RHEL7S
x86_64
firefox-debuginfo-52.6.0-1.el7_4

firefox-52.6.0-1.el7_4

RHEL6S
i386
firefox-debuginfo-52.6.0-1.el6_9
firefox-52.6.0-1.el6_9

x86_64
firefox-debuginfo-52.6.0-1.el6_9
firefox-52.6.0-1.el6_9

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

i386
firefox-debuginfo-52.6.0-1.el6_9
firefox-52.6.0-1.el6_9

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

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

i386
firefox-debuginfo-52.6.0-1.el6_9
firefox-52.6.0-1.el6_9

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

146314 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0219-1 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:

SUSE-SU-2018:0219-1

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/003633.html

SuSE SLED 12 SP2
x86_64
typelib-1_0-JavaScriptCore-4_0-2.18.5-2.18.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.5-2.18.1
libwebkit2gtk-4_0-37-2.18.5-2.18.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.5-2.18.1
webkit2gtk-4_0-injected-bundles-2.18.5-2.18.1
libwebkit2gtk-4_0-37-debuginfo-2.18.5-2.18.1
typelib-1_0-WebKit2-4_0-2.18.5-2.18.1
webkit2gtk3-debugsource-2.18.5-2.18.1
libjavascriptcoregtk-4_0-18-2.18.5-2.18.1

noarch
libwebkit2gtk3-lang-2.18.5-2.18.1

SuSE SLES 12 SP3
x86_64
typelib-1_0-JavaScriptCore-4_0-2.18.5-2.18.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.5-2.18.1
libwebkit2gtk-4_0-37-2.18.5-2.18.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.5-2.18.1
webkit2gtk-4_0-injected-bundles-2.18.5-2.18.1
libwebkit2gtk-4_0-37-debuginfo-2.18.5-2.18.1
typelib-1_0-WebKit2-4_0-2.18.5-2.18.1
webkit2gtk3-debugsource-2.18.5-2.18.1
libjavascriptcoregtk-4_0-18-2.18.5-2.18.1

SuSE SLES 12 SP2
x86_64
typelib-1_0-JavaScriptCore-4_0-2.18.5-2.18.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.5-2.18.1
libwebkit2gtk-4_0-37-2.18.5-2.18.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.5-2.18.1
webkit2gtk-4_0-injected-bundles-2.18.5-2.18.1
libwebkit2gtk-4_0-37-debuginfo-2.18.5-2.18.1
typelib-1_0-WebKit2-4_0-2.18.5-2.18.1
webkit2gtk3-debugsource-2.18.5-2.18.1
libjavascriptcoregtk-4_0-18-2.18.5-2.18.1

SuSE SLED 12 SP3
x86_64
typelib-1_0-JavaScriptCore-4_0-2.18.5-2.18.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.5-2.18.1
libwebkit2gtk-4_0-37-2.18.5-2.18.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.5-2.18.1
webkit2gtk-4_0-injected-bundles-2.18.5-2.18.1
libwebkit2gtk-4_0-37-debuginfo-2.18.5-2.18.1
typelib-1_0-WebKit2-4_0-2.18.5-2.18.1
webkit2gtk3-debugsource-2.18.5-2.18.1
libjavascriptcoregtk-4_0-18-2.18.5-2.18.1

noarch

libwebkit2gtk3-lang-2.18.5-2.18.1

160352 - CentOS 6, 7 CESA-2018-0122 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS 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:
CESA-2018-0122

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/022716.html
http://lists.centos.org/pipermail/centos-announce/2018-January/022717.html

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

i686
firefox-52.6.0-1.el7.centos

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

i686
firefox-52.6.0-1.el6.centos

163535 - Oracle Enterprise Linux ELSA-2018-0122 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux 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:
ELSA-2018-0122

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007472.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007473.html

OEL7
x86_64
firefox-52.6.0-1.0.1.el7_4

OEL6
x86_64
firefox-52.6.0-1.0.1.el6_9

i386
firefox-52.6.0-1.0.1.el6_9

175320 - Scientific Linux Security ERRATA Critical: firefox on SL6.x, SL7.x i386/x86_64 (1801-7859)

Category: SSH Module -> NonIntrusive -> Scientific Linux 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:
Security ERRATA Critical: firefox on SL6.x, SL7.x i386/x86_64 (1801-7859)

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=7859

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

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

i386
firefox-debuginfo-52.6.0-1.el6_9
firefox-52.6.0-1.el6_9

23018 - (K20087443) F5 BIG-IP BIG-IP APM VPN Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6129

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 VPN. Successful exploitation could allow an attacker to cause a denial of service.

23029 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.6

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

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

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

Observation

Mozilla Firefox ESR is a popular web browser.

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

23030 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.6

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

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

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

Observation

Mozilla Firefox ESR is a popular web browser.

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

23043 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52.6

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

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

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

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

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

23044 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52.6

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

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

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

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

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

22979 - Advantech WebAccess Multiple Vulnerabilities Prior To 8.3

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

Risk Level: High

CVE: CVE-2017-16716, CVE-2017-16720, CVE-2017-16724, CVE-2017-16728, CVE-2017-16753

Description

Multiple vulnerabilities are present in some versions of Advantech WebAccess.

Observation

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

Multiple vulnerabilities are present in some versions of Advantech WebAccess. The flaws lie in multiple components. Successful exploitation could allow a remote attacker to bypass authentication, to execute arbitrary code or cause denial of service condition.

23006 - Oracle WebCenter Portal Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2015-7940, CVE-2016-1182, CVE-2018-2713

Description

A vulnerability is present in Oracle WebCenter Portal.

Observation

Oracle WebCenter Portal is a web platform that helps organizations in fast and easy creation of intranets, extranets, composite applications, and self-service portals.

A vulnerability is present in Oracle WebCenter Portal. The flaw lies in the WebCenter Portal component. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

23008 - WordPress Multiple Vulnerabilities Prior To 4.9.2

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of WordPress.

Observation

WordPress is a popular blog application.

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

23009 - Cisco NX-OS Software Pong Packet Denial Of Service Vulnerability (cisco-sa-20180117-nx-os)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-0102

Description

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

Observation

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

A denial-of-service vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the Pong tool of Cisco NX-OS Software. Successful exploitation could allow an attacker to cause a denial-of-service condition.

23016 - (SB10222) McAfee Web Gateway Dirty Cow Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-1000405

Description

A vulnerability is present in some versions of McAfee Web Gateway.

Observation

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

A vulnerability is present in some versions of McAfee Web Gateway. The flaw lies in the patches used to fix the "Dirty Cow" vulnerability. Successful exploitation could allow an attacker to make unauthorized modifications on the target system.

23017 - Cisco Nexus 9000 Series Switches GNU glibc Vulnerability (CSCuy36553)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-7547

Description

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

Observation

Cisco NX-OS is a network operating system.

A buffer overflow vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in glibc. Successful exploitation could allow an attacker to cause a denial of service or execute arbitrary code on an affected device.

23019 - Oracle MySQL Enterprise Monitor Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2017-12617, CVE-2017-3736

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL Enterprise Monitor.

Observation

Oracle MySQL Enterprise Monitor enables monitoring of multiple Oracle MySQL instances.

Multiple vulnerabilities are present in some versions of Oracle MySQL Enterprise Monitor. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute remote code or disclose sensitive information.

23020 - Oracle iPlanet Web Server Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2017-5461

Description

A vulnerability is present in some versions of Oracle iPlanet Web Server.

Observation

Oracle iPlanet Web Server is an enterprise web application server.

A vulnerability is present in some versions of Oracle iPlanet Web Server. The flaw lies in the Network Security Services (NSS) component. Successful exploitation could allow an attacker to cause a denial of service or other unspecified impact.

23021 - Oracle iPlanet Web Server Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2017-5461

Description

A vulnerability is present in some versions of Oracle iPlanet Web Server.

Observation

Oracle iPlanet Web Server is an enterprise web application server.

A vulnerability is present in some versions of Oracle iPlanet Web Server. The flaw lies in the Network Security Services (NSS) component. Successful exploitation could allow an attacker to cause a denial of service or other unspecified impact.

23022 - Oracle Directory Server Enterprise Edition Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2017-5461

Description

A vulnerability is present in some versions of Oracle Directory Server Enterprise Edition.

Observation

Oracle Directory Server Enterprise Edition provides a core directory service for enterprise environments.

A vulnerability is present in some versions of Oracle Directory Server Enterprise Edition. The flaw lies in the Admin Console component. Successful exploitation could allow an attacker to cause a denial of service condition, or possibly have unspecified other impact.

23023 - Oracle JRockit Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2637, CVE-2018-2657, CVE-2018-2663, CVE-2018-2678

Description

Multiple vulnerabilities are present in some versions of Oracle JRockit.

Observation

Oracle JRockit is a Java Virtual Machine (JVM).

Multiple vulnerabilities are present in some versions of Oracle JRockit. The flaws lie in several components. Successful exploitation could allow an attacker to disclose sensitive information or cause a partial denial of service condition.

23032 - Oracle MySQL Server Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2017-3737, CVE-2018-2562, CVE-2018-2565, CVE-2018-2573, CVE-2018-2576, CVE-2018-2583, CVE-2018-2586, CVE-2018-2590, CVE-2018-2591, 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

Multiple vulnerabilities are present in some versions of Oracle MySQL Server.

Observation

Oracle MySQL Server is a popular open source database.

Multiple vulnerabilities are present in some versions of Oracle MySQL Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or have unauthorized access to the target system.

23035 - Mozilla Firefox Multiple Vulnerabilities Prior To 58

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

Risk Level: High

CVE: CVE-2018-5089, CVE-2018-5090, CVE-2018-5091, CVE-2018-5092, CVE-2018-5093, CVE-2018-5094, CVE-2018-5095, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5100, CVE-2018-5101, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5105, CVE-2018-5106, CVE-2018-5107, CVE-2018-5108, CVE-2018-5109, CVE-2018-5110, CVE-2018-

5111, CVE-2018-5112, CVE-2018-5113, CVE-2018-5114, CVE-2018-5115, CVE-2018-5116, CVE-2018-5117, CVE-2018-5118, CVE-2018-5119, CVE-2018-5121, CVE-2018-5122

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

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

23036 - Mozilla Firefox Multiple Vulnerabilities Prior To 58

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-5089, CVE-2018-5090, CVE-2018-5091, CVE-2018-5092, CVE-2018-5093, CVE-2018-5094, CVE-2018-5095, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5100, CVE-2018-5101, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5105, CVE-2018-5106, CVE-2018-5107, CVE-2018-5108, CVE-2018-5109, CVE-2018-5110, CVE-2018-5111, CVE-2018-5112, CVE-2018-5113, CVE-2018-5114, CVE-2018-5115, CVE-2018-5116, CVE-2018-5117, CVE-2018-5118, CVE-2018-5119, CVE-2018-5121, CVE-2018-5122

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

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

132434 - Oracle VM OVMSA-2018-0016 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5157, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0016

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000827.html

OVM3.3
x86_64
kernel-uek-3.8.13-118.20.2.el6uek
kernel-uek-firmware-3.8.13-118.20.2.el6uek

141858 - Red Hat Enterprise Linux RHSA-2018-0151 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8539, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7472

Description

The scan detected that the host is missing the following update:
RHSA-2018-0151

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/msg00080.html

RHEL7D
x86_64
kernel-debug-debuginfo-3.10.0-693.17.1.el7
kernel-tools-debuginfo-3.10.0-693.17.1.el7
perf-debuginfo-3.10.0-693.17.1.el7
kernel-headers-3.10.0-693.17.1.el7
python-perf-3.10.0-693.17.1.el7
kernel-tools-libs-3.10.0-693.17.1.el7
kernel-3.10.0-693.17.1.el7
kernel-debuginfo-3.10.0-693.17.1.el7
kernel-debug-devel-3.10.0-693.17.1.el7
kernel-tools-libs-devel-3.10.0-693.17.1.el7
perf-3.10.0-693.17.1.el7
kernel-debug-3.10.0-693.17.1.el7
kernel-devel-3.10.0-693.17.1.el7
kernel-debuginfo-common-x86_64-3.10.0-693.17.1.el7
kernel-tools-3.10.0-693.17.1.el7
python-perf-debuginfo-3.10.0-693.17.1.el7

noarch
kernel-abi-whitelists-3.10.0-693.17.1.el7
kernel-doc-3.10.0-693.17.1.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-693.17.1.el7
kernel-doc-3.10.0-693.17.1.el7

x86_64
kernel-debug-debuginfo-3.10.0-693.17.1.el7
kernel-tools-debuginfo-3.10.0-693.17.1.el7
perf-debuginfo-3.10.0-693.17.1.el7
kernel-headers-3.10.0-693.17.1.el7
python-perf-3.10.0-693.17.1.el7
kernel-tools-libs-3.10.0-693.17.1.el7
kernel-3.10.0-693.17.1.el7
kernel-debuginfo-3.10.0-693.17.1.el7
kernel-debug-devel-3.10.0-693.17.1.el7
kernel-tools-libs-devel-3.10.0-693.17.1.el7
perf-3.10.0-693.17.1.el7
kernel-debug-3.10.0-693.17.1.el7
kernel-devel-3.10.0-693.17.1.el7

kernel-debuginfo-common-x86_64-3.10.0-693.17.1.el7
kernel-tools-3.10.0-693.17.1.el7
python-perf-debuginfo-3.10.0-693.17.1.el7

RHEL7WS
x86_64
kernel-debug-debuginfo-3.10.0-693.17.1.el7
kernel-tools-debuginfo-3.10.0-693.17.1.el7
perf-debuginfo-3.10.0-693.17.1.el7
kernel-headers-3.10.0-693.17.1.el7
python-perf-3.10.0-693.17.1.el7
kernel-tools-libs-3.10.0-693.17.1.el7
kernel-3.10.0-693.17.1.el7
kernel-debuginfo-3.10.0-693.17.1.el7
kernel-debug-devel-3.10.0-693.17.1.el7
kernel-tools-libs-devel-3.10.0-693.17.1.el7
perf-3.10.0-693.17.1.el7
kernel-debug-3.10.0-693.17.1.el7
kernel-devel-3.10.0-693.17.1.el7
kernel-debuginfo-common-x86_64-3.10.0-693.17.1.el7
kernel-tools-3.10.0-693.17.1.el7
python-perf-debuginfo-3.10.0-693.17.1.el7

noarch
kernel-abi-whitelists-3.10.0-693.17.1.el7
kernel-doc-3.10.0-693.17.1.el7

141859 - Red Hat Enterprise Linux RHSA-2018-0163 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15134

Description

The scan detected that the host is missing the following update:
RHSA-2018-0163

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/msg00084.html

RHEL7D
x86_64
389-ds-base-snmp-1.3.6.1-26.el7_4
389-ds-base-debuginfo-1.3.6.1-26.el7_4
389-ds-base-libs-1.3.6.1-26.el7_4
389-ds-base-devel-1.3.6.1-26.el7_4
389-ds-base-1.3.6.1-26.el7_4

RHEL7S
x86_64
389-ds-base-snmp-1.3.6.1-26.el7_4
389-ds-base-debuginfo-1.3.6.1-26.el7_4
389-ds-base-libs-1.3.6.1-26.el7_4
389-ds-base-devel-1.3.6.1-26.el7_4
389-ds-base-1.3.6.1-26.el7_4

RHEL7WS
x86_64
389-ds-base-snmp-1.3.6.1-26.el7_4
389-ds-base-debuginfo-1.3.6.1-26.el7_4
389-ds-base-libs-1.3.6.1-26.el7_4
389-ds-base-devel-1.3.6.1-26.el7_4
389-ds-base-1.3.6.1-26.el7_4

146282 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0222-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8859

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0222-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00093.html

SuSE Linux 42.2
i586
tre-0.8.0_git201402282055-7.3.1
libtre5-debuginfo-0.8.0_git201402282055-7.3.1
agrep-debuginfo-0.8.0_git201402282055-7.3.1
libtre5-0.8.0_git201402282055-7.3.1
python-tre-debuginfo-0.8.0_git201402282055-7.3.1
python-tre-0.8.0_git201402282055-7.3.1
agrep-0.8.0_git201402282055-7.3.1
tre-devel-0.8.0_git201402282055-7.3.1
tre-debugsource-0.8.0_git201402282055-7.3.1

noarch
tre-lang-0.8.0_git201402282055-7.3.1

x86_64
tre-0.8.0_git201402282055-7.3.1
libtre5-debuginfo-0.8.0_git201402282055-7.3.1
agrep-debuginfo-0.8.0_git201402282055-7.3.1
libtre5-0.8.0_git201402282055-7.3.1
python-tre-debuginfo-0.8.0_git201402282055-7.3.1
python-tre-0.8.0_git201402282055-7.3.1
agrep-0.8.0_git201402282055-7.3.1
tre-devel-0.8.0_git201402282055-7.3.1
tre-debugsource-0.8.0_git201402282055-7.3.1

SuSE Linux 42.3
i586
tre-0.8.0_git201402282055-10.1
tre-debugsource-0.8.0_git201402282055-10.1
tre-devel-0.8.0_git201402282055-10.1
libtre5-debuginfo-0.8.0_git201402282055-10.1
libtre5-0.8.0_git201402282055-10.1

agrep-0.8.0_git201402282055-10.1
agrep-debuginfo-0.8.0_git201402282055-10.1
python-tre-debuginfo-0.8.0_git201402282055-10.1
python-tre-0.8.0_git201402282055-10.1

noarch
tre-lang-0.8.0_git201402282055-10.1

x86_64
tre-0.8.0_git201402282055-10.1
tre-debugsource-0.8.0_git201402282055-10.1
tre-devel-0.8.0_git201402282055-10.1
libtre5-debuginfo-0.8.0_git201402282055-10.1
libtre5-0.8.0_git201402282055-10.1
agrep-0.8.0_git201402282055-10.1
agrep-debuginfo-0.8.0_git201402282055-10.1
python-tre-debuginfo-0.8.0_git201402282055-10.1
python-tre-0.8.0_git201402282055-10.1

146284 - SuSE Linux 42.3 openSUSE-SU-2018:0257-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
openSUSE-SU-2018:0257-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00105.html

SuSE Linux 42.3
x86_64
MozillaThunderbird-debuginfo-52.6-56.2
MozillaThunderbird-debugsource-52.6-56.2
MozillaThunderbird-translations-other-52.6-56.2
MozillaThunderbird-buildsymbols-52.6-56.2
MozillaThunderbird-52.6-56.2
MozillaThunderbird-translations-common-52.6-56.2
MozillaThunderbird-devel-52.6-56.2

i586
MozillaThunderbird-buildsymbols-52.6-56.1
MozillaThunderbird-debuginfo-52.6-56.1
MozillaThunderbird-52.6-56.1
MozillaThunderbird-devel-52.6-56.1
MozillaThunderbird-translations-common-52.6-56.1
MozillaThunderbird-debugsource-52.6-56.1
MozillaThunderbird-translations-other-52.6-56.1

146285 - SuSE Linux 42.3 openSUSE-SU-2018:0259-1 Update Is Not Installed

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

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

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0259-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00107.html

SuSE Linux 42.3
x86_64
chromium-debugsource-64.0.3282.119-135.1
re2-debugsource-20180101-9.1
chromedriver-64.0.3282.119-135.1
chromedriver-debuginfo-64.0.3282.119-135.1
libre2-0-debuginfo-20180101-9.1
libre2-0-20180101-9.1
libre2-0-debuginfo-32bit-20180101-9.1
chromium-64.0.3282.119-135.1
re2-devel-20180101-9.1
libre2-0-32bit-20180101-9.1
chromium-debuginfo-64.0.3282.119-135.1

i586
libre2-0-debuginfo-20180101-9.1
re2-debugsource-20180101-9.1
libre2-0-20180101-9.1
re2-devel-20180101-9.1

146286 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0217-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000007

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0217-1

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/003632.html

SuSE SLES 12 SP2
x86_64
curl-debugsource-7.37.0-37.14.1
curl-7.37.0-37.14.1

libcurl4-7.37.0-37.14.1
libcurl4-debuginfo-32bit-7.37.0-37.14.1
curl-debuginfo-7.37.0-37.14.1
libcurl4-debuginfo-7.37.0-37.14.1
libcurl4-32bit-7.37.0-37.14.1

SuSE SLED 12 SP3
x86_64
curl-debugsource-7.37.0-37.14.1
curl-7.37.0-37.14.1
libcurl4-7.37.0-37.14.1
libcurl4-debuginfo-32bit-7.37.0-37.14.1
curl-debuginfo-7.37.0-37.14.1
libcurl4-debuginfo-7.37.0-37.14.1
libcurl4-32bit-7.37.0-37.14.1

SuSE SLED 12 SP2
x86_64
curl-debugsource-7.37.0-37.14.1
curl-7.37.0-37.14.1
libcurl4-7.37.0-37.14.1
libcurl4-debuginfo-32bit-7.37.0-37.14.1
curl-debuginfo-7.37.0-37.14.1
libcurl4-debuginfo-7.37.0-37.14.1
libcurl4-32bit-7.37.0-37.14.1

SuSE SLES 12 SP3
x86_64
curl-debugsource-7.37.0-37.14.1
curl-7.37.0-37.14.1
libcurl4-7.37.0-37.14.1
libcurl4-debuginfo-32bit-7.37.0-37.14.1
curl-debuginfo-7.37.0-37.14.1
libcurl4-debuginfo-7.37.0-37.14.1
libcurl4-32bit-7.37.0-37.14.1

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

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

Risk Level: High

CVE: CVE-2018-5711

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0235-1

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/003638.html

SuSE SLES 11 SP4
i586
gd-2.0.36.RC1-52.33.5.1

x86_64
gd-2.0.36.RC1-52.33.5.1

146290 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0200-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0200-1

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/003628.html

SuSE SLES 12 SP2
x86_64
libevent-debugsource-2.0.21-6.3.1
libevent-2_0-5-debuginfo-2.0.21-6.3.1
libevent-2_0-5-2.0.21-6.3.1

SuSE SLED 12 SP3
x86_64
libevent-debugsource-2.0.21-6.3.1
libevent-2_0-5-debuginfo-2.0.21-6.3.1
libevent-2_0-5-2.0.21-6.3.1

SuSE SLED 12 SP2
x86_64
libevent-debugsource-2.0.21-6.3.1
libevent-2_0-5-debuginfo-2.0.21-6.3.1
libevent-2_0-5-2.0.21-6.3.1

SuSE SLES 12 SP3
x86_64
libevent-debugsource-2.0.21-6.3.1
libevent-2_0-5-debuginfo-2.0.21-6.3.1
libevent-2_0-5-2.0.21-6.3.1

146292 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0279-1 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:
SUSE-SU-2018:0279-1

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/003674.html

SuSE SLED 12 SP3
x86_64
libvirt-daemon-config-nwfilter-3.3.0-5.13.1
libvirt-admin-3.3.0-5.13.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-nwfilter-3.3.0-5.13.1
libvirt-daemon-driver-storage-logical-3.3.0-5.13.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-5.13.1
libvirt-daemon-3.3.0-5.13.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-interface-3.3.0-5.13.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-lxc-3.3.0-5.13.1
libvirt-daemon-driver-network-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-libxl-3.3.0-5.13.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-core-3.3.0-5.13.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-5.13.1
libvirt-debugsource-3.3.0-5.13.1
libvirt-daemon-lxc-3.3.0-5.13.1
libvirt-libs-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-5.13.1
libvirt-doc-3.3.0-5.13.1
libvirt-daemon-qemu-3.3.0-5.13.1
libvirt-daemon-driver-secret-3.3.0-5.13.1
libvirt-client-3.3.0-5.13.1
libvirt-daemon-driver-storage-3.3.0-5.13.1
libvirt-3.3.0-5.13.1
libvirt-libs-3.3.0-5.13.1
libvirt-daemon-xen-3.3.0-5.13.1
libvirt-daemon-driver-storage-mpath-3.3.0-5.13.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-scsi-3.3.0-5.13.1
libvirt-daemon-driver-qemu-3.3.0-5.13.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-5.13.1
libvirt-admin-debuginfo-3.3.0-5.13.1
libvirt-daemon-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-network-3.3.0-5.13.1
libvirt-daemon-driver-nodedev-3.3.0-5.13.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-disk-3.3.0-5.13.1
libvirt-client-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-rbd-3.3.0-5.13.1
libvirt-daemon-driver-storage-iscsi-3.3.0-5.13.1
libvirt-daemon-config-network-3.3.0-5.13.1

SuSE SLES 12 SP3
x86_64
libvirt-daemon-config-nwfilter-3.3.0-5.13.1
libvirt-admin-3.3.0-5.13.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-nwfilter-3.3.0-5.13.1
libvirt-daemon-driver-storage-logical-3.3.0-5.13.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-5.13.1
libvirt-daemon-3.3.0-5.13.1

libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-interface-3.3.0-5.13.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-lxc-3.3.0-5.13.1
libvirt-daemon-driver-network-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-libxl-3.3.0-5.13.1
libvirt-nss-3.3.0-5.13.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-core-3.3.0-5.13.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-5.13.1
libvirt-daemon-xen-3.3.0-5.13.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-5.13.1
libvirt-daemon-lxc-3.3.0-5.13.1
libvirt-lock-sanlock-debuginfo-3.3.0-5.13.1
libvirt-libs-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-5.13.1
libvirt-doc-3.3.0-5.13.1
libvirt-daemon-qemu-3.3.0-5.13.1
libvirt-daemon-driver-secret-3.3.0-5.13.1
libvirt-client-3.3.0-5.13.1
libvirt-daemon-driver-storage-3.3.0-5.13.1
libvirt-3.3.0-5.13.1
libvirt-libs-3.3.0-5.13.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-5.13.1
libvirt-lock-sanlock-3.3.0-5.13.1
libvirt-daemon-driver-storage-mpath-3.3.0-5.13.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-scsi-3.3.0-5.13.1
libvirt-daemon-driver-qemu-3.3.0-5.13.1
libvirt-daemon-driver-storage-rbd-3.3.0-5.13.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-5.13.1
libvirt-admin-debuginfo-3.3.0-5.13.1
libvirt-daemon-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-network-3.3.0-5.13.1
libvirt-daemon-driver-nodedev-3.3.0-5.13.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-5.13.1
libvirt-nss-debuginfo-3.3.0-5.13.1
libvirt-daemon-driver-storage-disk-3.3.0-5.13.1
libvirt-client-debuginfo-3.3.0-5.13.1
libvirt-debugsource-3.3.0-5.13.1
libvirt-daemon-driver-storage-iscsi-3.3.0-5.13.1
libvirt-daemon-config-network-3.3.0-5.13.1

146295 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0220-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0220-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00091.html

SuSE Linux 42.2
x86_64
libevent-2_0-5-debuginfo-32bit-2.0.21-7.3.1
libevent-2_0-5-32bit-2.0.21-7.3.1
libevent-2_0-5-2.0.21-7.3.1
libevent-2_0-5-debuginfo-2.0.21-7.3.1
libevent-debugsource-2.0.21-7.3.1
libevent-devel-2.0.21-7.3.1

i586
libevent-devel-2.0.21-7.3.1
libevent-2_0-5-debuginfo-2.0.21-7.3.1
libevent-debugsource-2.0.21-7.3.1
libevent-2_0-5-2.0.21-7.3.1

SuSE Linux 42.3
x86_64
libevent-devel-2.0.21-10.1
libevent-2_0-5-2.0.21-10.1
libevent-debugsource-2.0.21-10.1
libevent-2_0-5-32bit-2.0.21-10.1
libevent-2_0-5-debuginfo-2.0.21-10.1
libevent-2_0-5-debuginfo-32bit-2.0.21-10.1

i586
libevent-debugsource-2.0.21-10.1
libevent-devel-2.0.21-10.1
libevent-2_0-5-debuginfo-2.0.21-10.1
libevent-2_0-5-2.0.21-10.1

146296 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0203-1 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:
openSUSE-SU-2018:0203-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00081.html

SuSE Linux 42.2
x86_64
MozillaFirefox-buildsymbols-52.6-57.30.1
MozillaFirefox-translations-other-52.6-57.30.1
MozillaFirefox-debuginfo-52.6-57.30.1
MozillaFirefox-debugsource-52.6-57.30.1
MozillaFirefox-52.6-57.30.1
MozillaFirefox-devel-52.6-57.30.1

MozillaFirefox-branding-upstream-52.6-57.30.1
MozillaFirefox-translations-common-52.6-57.30.1

SuSE Linux 42.3
x86_64
MozillaFirefox-52.6-75.1
MozillaFirefox-debugsource-52.6-75.1
MozillaFirefox-devel-52.6-75.1
MozillaFirefox-translations-common-52.6-75.1
MozillaFirefox-buildsymbols-52.6-75.1
MozillaFirefox-translations-other-52.6-75.1
MozillaFirefox-debuginfo-52.6-75.1
MozillaFirefox-branding-upstream-52.6-75.1

146297 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0236-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000007

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0236-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00101.html

SuSE Linux 42.2
x86_64
libcurl4-debuginfo-7.37.0-16.15.1
libcurl4-debuginfo-32bit-7.37.0-16.15.1
curl-debuginfo-7.37.0-16.15.1
libcurl-devel-32bit-7.37.0-16.15.1
libcurl4-7.37.0-16.15.1
libcurl-devel-7.37.0-16.15.1
curl-7.37.0-16.15.1
libcurl4-32bit-7.37.0-16.15.1
curl-debugsource-7.37.0-16.15.1

i586
libcurl4-debuginfo-7.37.0-16.15.1
curl-debuginfo-7.37.0-16.15.1
libcurl4-7.37.0-16.15.1
libcurl-devel-7.37.0-16.15.1
curl-7.37.0-16.15.1
curl-debugsource-7.37.0-16.15.1

SuSE Linux 42.3
x86_64
libcurl4-debuginfo-7.37.0-30.1
libcurl-devel-32bit-7.37.0-30.1
curl-debugsource-7.37.0-30.1
libcurl4-7.37.0-30.1
libcurl4-32bit-7.37.0-30.1
curl-debuginfo-7.37.0-30.1

libcurl-devel-7.37.0-30.1
libcurl4-debuginfo-32bit-7.37.0-30.1
curl-7.37.0-30.1

i586
libcurl4-debuginfo-7.37.0-30.1
curl-debugsource-7.37.0-30.1
libcurl4-7.37.0-30.1
curl-debuginfo-7.37.0-30.1
libcurl-devel-7.37.0-30.1
curl-7.37.0-30.1

146301 - SuSE SLES 12 SP2 SUSE-SU-2018:0213-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-1000410, CVE-2017-11600, CVE-2017-12193, CVE-2017-15115, CVE-2017-16528, CVE-2017-16536, CVE-2017-16537, CVE-2017-16645, CVE-2017-16646, CVE-2017-16939, CVE-2017-16994, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17805, CVE-2017-17806, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7482, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0213-1

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/003629.html

SuSE SLES 12 SP2
x86_64
kernel-syms-rt-4.4.104-24.1
kernel-rt_debug-devel-4.4.104-24.1
cluster-md-kmp-rt-4.4.104-24.1
dlm-kmp-rt-debuginfo-4.4.104-24.1
kernel-rt_debug-devel-debuginfo-4.4.104-24.1
kernel-rt_debug-debugsource-4.4.104-24.1
kernel-rt-debuginfo-4.4.104-24.1
kernel-rt-devel-4.4.104-24.1
cluster-md-kmp-rt-debuginfo-4.4.104-24.1
dlm-kmp-rt-4.4.104-24.1
kernel-rt-base-4.4.104-24.1
kernel-rt-4.4.104-24.1
gfs2-kmp-rt-debuginfo-4.4.104-24.1
kernel-rt_debug-debuginfo-4.4.104-24.1
ocfs2-kmp-rt-debuginfo-4.4.104-24.1
cluster-network-kmp-rt-4.4.104-24.1
kernel-rt-base-debuginfo-4.4.104-24.1
kernel-rt-debugsource-4.4.104-24.1
cluster-network-kmp-rt-debuginfo-4.4.104-24.1
gfs2-kmp-rt-4.4.104-24.1
ocfs2-kmp-rt-4.4.104-24.1

noarch
kernel-devel-rt-4.4.104-24.1
kernel-source-rt-4.4.104-24.1

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: High

CVE: CVE-2018-5711

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0260-1

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/003656.html

SuSE SLED 12 SP2
x86_64
gd-debugsource-2.1.0-24.6.1
gd-debuginfo-32bit-2.1.0-24.6.1
gd-32bit-2.1.0-24.6.1
gd-debuginfo-2.1.0-24.6.1
gd-2.1.0-24.6.1

SuSE SLES 12 SP3
x86_64
gd-debugsource-2.1.0-24.6.1
gd-debuginfo-2.1.0-24.6.1
gd-2.1.0-24.6.1

SuSE SLES 12 SP2
x86_64
gd-debugsource-2.1.0-24.6.1
gd-debuginfo-2.1.0-24.6.1
gd-2.1.0-24.6.1

SuSE SLED 12 SP3
x86_64
gd-debugsource-2.1.0-24.6.1
gd-debuginfo-32bit-2.1.0-24.6.1
gd-32bit-2.1.0-24.6.1
gd-debuginfo-2.1.0-24.6.1
gd-2.1.0-24.6.1

146304 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0210-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13194

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0210-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00088.html

SuSE Linux 42.2
x86_64
libvpx1-1.3.0-5.3.1
libvpx-devel-1.3.0-5.3.1
libvpx-debugsource-1.3.0-5.3.1
libvpx1-32bit-1.3.0-5.3.1
vpx-tools-debuginfo-1.3.0-5.3.1
vpx-tools-1.3.0-5.3.1
libvpx1-debuginfo-1.3.0-5.3.1
libvpx1-debuginfo-32bit-1.3.0-5.3.1

i586
libvpx1-1.3.0-5.3.1
libvpx-devel-1.3.0-5.3.1
libvpx-debugsource-1.3.0-5.3.1
vpx-tools-debuginfo-1.3.0-5.3.1
vpx-tools-1.3.0-5.3.1
libvpx1-debuginfo-1.3.0-5.3.1

SuSE Linux 42.3
x86_64
libvpx1-1.3.0-8.1
libvpx1-debuginfo-32bit-1.3.0-8.1
vpx-tools-1.3.0-8.1
libvpx1-32bit-1.3.0-8.1
vpx-tools-debuginfo-1.3.0-8.1
libvpx-devel-1.3.0-8.1
libvpx-debugsource-1.3.0-8.1
libvpx1-debuginfo-1.3.0-8.1

i586
libvpx1-1.3.0-8.1
vpx-tools-1.3.0-8.1
vpx-tools-debuginfo-1.3.0-8.1
libvpx-devel-1.3.0-8.1
libvpx-debugsource-1.3.0-8.1
libvpx1-debuginfo-1.3.0-8.1

146306 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0223-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3737, CVE-2018-2562, CVE-2018-2573, CVE-2018-2583, CVE-2018-2590, CVE-2018-2591, CVE-2018-2612, CVE-2018-2622, CVE-2018-2640, CVE-2018-2645, CVE-2018-2647, CVE-2018-2665, CVE-2018-2668, CVE-2018-2696, CVE-2018-2703

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0223-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00094.html

SuSE Linux 42.2
i586
mysql-community-server-debugsource-5.6.39-24.15.1
mysql-community-server-debuginfo-5.6.39-24.15.1
mysql-community-server-test-debuginfo-5.6.39-24.15.1
mysql-community-server-bench-debuginfo-5.6.39-24.15.1
mysql-community-server-tools-5.6.39-24.15.1
mysql-community-server-client-debuginfo-5.6.39-24.15.1
mysql-community-server-5.6.39-24.15.1
mysql-community-server-bench-5.6.39-24.15.1
libmysql56client_r18-5.6.39-24.15.1
libmysql56client18-5.6.39-24.15.1
mysql-community-server-tools-debuginfo-5.6.39-24.15.1
mysql-community-server-test-5.6.39-24.15.1
libmysql56client18-debuginfo-5.6.39-24.15.1
mysql-community-server-client-5.6.39-24.15.1

noarch
mysql-community-server-errormessages-5.6.39-24.15.1

x86_64
mysql-community-server-debugsource-5.6.39-24.15.1
mysql-community-server-debuginfo-5.6.39-24.15.1
mysql-community-server-test-debuginfo-5.6.39-24.15.1
libmysql56client18-debuginfo-32bit-5.6.39-24.15.1
mysql-community-server-bench-debuginfo-5.6.39-24.15.1
mysql-community-server-tools-5.6.39-24.15.1
mysql-community-server-client-debuginfo-5.6.39-24.15.1
libmysql56client_r18-32bit-5.6.39-24.15.1
mysql-community-server-5.6.39-24.15.1
mysql-community-server-bench-5.6.39-24.15.1
libmysql56client_r18-5.6.39-24.15.1
libmysql56client18-5.6.39-24.15.1
mysql-community-server-tools-debuginfo-5.6.39-24.15.1
mysql-community-server-test-5.6.39-24.15.1
libmysql56client18-32bit-5.6.39-24.15.1
libmysql56client18-debuginfo-5.6.39-24.15.1
mysql-community-server-client-5.6.39-24.15.1

SuSE Linux 42.3
i586
mysql-community-server-test-5.6.39-33.1
mysql-community-server-client-debuginfo-5.6.39-33.1
libmysql56client18-5.6.39-33.1
mysql-community-server-tools-debuginfo-5.6.39-33.1
mysql-community-server-bench-debuginfo-5.6.39-33.1
libmysql56client18-debuginfo-5.6.39-33.1
libmysql56client_r18-5.6.39-33.1
mysql-community-server-debuginfo-5.6.39-33.1
mysql-community-server-test-debuginfo-5.6.39-33.1
mysql-community-server-debugsource-5.6.39-33.1
mysql-community-server-tools-5.6.39-33.1
mysql-community-server-5.6.39-33.1
mysql-community-server-client-5.6.39-33.1
mysql-community-server-bench-5.6.39-33.1

noarch

mysql-community-server-errormessages-5.6.39-33.1

x86_64
mysql-community-server-test-5.6.39-33.1
mysql-community-server-client-debuginfo-5.6.39-33.1
libmysql56client18-5.6.39-33.1
mysql-community-server-tools-debuginfo-5.6.39-33.1
libmysql56client18-debuginfo-32bit-5.6.39-33.1
mysql-community-server-bench-debuginfo-5.6.39-33.1
libmysql56client18-debuginfo-5.6.39-33.1
libmysql56client_r18-5.6.39-33.1
mysql-community-server-debuginfo-5.6.39-33.1
mysql-community-server-test-debuginfo-5.6.39-33.1
libmysql56client_r18-32bit-5.6.39-33.1
mysql-community-server-debugsource-5.6.39-33.1
libmysql56client18-32bit-5.6.39-33.1
mysql-community-server-tools-5.6.39-33.1
mysql-community-server-5.6.39-33.1
mysql-community-server-client-5.6.39-33.1
mysql-community-server-bench-5.6.39-33.1

146307 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0295-1 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:
SUSE-SU-2018:0295-1

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/003682.html

SuSE SLED 12 SP3
x86_64
libtasn1-debuginfo-4.9-3.5.1
libtasn1-debugsource-4.9-3.5.1
libtasn1-6-32bit-4.9-3.5.1
libtasn1-6-debuginfo-4.9-3.5.1
libtasn1-6-4.9-3.5.1
libtasn1-4.9-3.5.1
libtasn1-6-debuginfo-32bit-4.9-3.5.1

SuSE SLES 12 SP3
x86_64
libtasn1-debuginfo-4.9-3.5.1
libtasn1-debugsource-4.9-3.5.1
libtasn1-6-32bit-4.9-3.5.1
libtasn1-6-debuginfo-4.9-3.5.1
libtasn1-6-4.9-3.5.1
libtasn1-4.9-3.5.1
libtasn1-6-debuginfo-32bit-4.9-3.5.1

146310 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0228-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15047

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0228-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00099.html

SuSE Linux 42.2
x86_64
redis-4.0.6-8.6.1
redis-debugsource-4.0.6-8.6.1
redis-debuginfo-4.0.6-8.6.1

i586
redis-4.0.6-8.6.1
redis-debugsource-4.0.6-8.6.1
redis-debuginfo-4.0.6-8.6.1

SuSE Linux 42.3
x86_64
redis-debuginfo-4.0.6-14.1
redis-4.0.6-14.1
redis-debugsource-4.0.6-14.1

i586
redis-debuginfo-4.0.6-14.1
redis-4.0.6-14.1
redis-debugsource-4.0.6-14.1

146311 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0303-1 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-2018:0303-1

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/003688.html

SuSE SLES 12 SP2
noarch

bind-doc-9.9.9P1-63.7.1

x86_64
bind-9.9.9P1-63.7.1
bind-chrootenv-9.9.9P1-63.7.1
bind-debuginfo-9.9.9P1-63.7.1
bind-libs-debuginfo-32bit-9.9.9P1-63.7.1
bind-utils-9.9.9P1-63.7.1
bind-libs-9.9.9P1-63.7.1
bind-debugsource-9.9.9P1-63.7.1
bind-utils-debuginfo-9.9.9P1-63.7.1
bind-libs-debuginfo-9.9.9P1-63.7.1
bind-libs-32bit-9.9.9P1-63.7.1

SuSE SLED 12 SP3
x86_64
bind-libs-9.9.9P1-63.7.1
bind-debuginfo-9.9.9P1-63.7.1
bind-utils-debuginfo-9.9.9P1-63.7.1
bind-utils-9.9.9P1-63.7.1
bind-debugsource-9.9.9P1-63.7.1
bind-libs-debuginfo-32bit-9.9.9P1-63.7.1
bind-libs-debuginfo-9.9.9P1-63.7.1
bind-libs-32bit-9.9.9P1-63.7.1

SuSE SLED 12 SP2
x86_64
bind-libs-9.9.9P1-63.7.1
bind-debuginfo-9.9.9P1-63.7.1
bind-utils-debuginfo-9.9.9P1-63.7.1
bind-utils-9.9.9P1-63.7.1
bind-debugsource-9.9.9P1-63.7.1
bind-libs-debuginfo-32bit-9.9.9P1-63.7.1
bind-libs-debuginfo-9.9.9P1-63.7.1
bind-libs-32bit-9.9.9P1-63.7.1

SuSE SLES 12 SP3
noarch
bind-doc-9.9.9P1-63.7.1

x86_64
bind-9.9.9P1-63.7.1
bind-chrootenv-9.9.9P1-63.7.1
bind-debuginfo-9.9.9P1-63.7.1
bind-libs-debuginfo-32bit-9.9.9P1-63.7.1
bind-utils-9.9.9P1-63.7.1
bind-libs-9.9.9P1-63.7.1
bind-debugsource-9.9.9P1-63.7.1
bind-utils-debuginfo-9.9.9P1-63.7.1
bind-libs-debuginfo-9.9.9P1-63.7.1
bind-libs-32bit-9.9.9P1-63.7.1

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: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0248-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00103.html

SuSE Linux 42.2
i586
php5-xmlreader-5.5.14-77.18.2
php5-sqlite-5.5.14-77.18.2
php5-suhosin-debuginfo-5.5.14-77.18.2
php5-ctype-debuginfo-5.5.14-77.18.2
php5-shmop-5.5.14-77.18.2
php5-sysvmsg-5.5.14-77.18.2
php5-xmlreader-debuginfo-5.5.14-77.18.2
php5-xmlrpc-5.5.14-77.18.2
php5-enchant-debuginfo-5.5.14-77.18.2
php5-mbstring-5.5.14-77.18.2
php5-ftp-5.5.14-77.18.2
apache2-mod_php5-debuginfo-5.5.14-77.18.2
php5-soap-5.5.14-77.18.2
php5-openssl-debuginfo-5.5.14-77.18.2
php5-fpm-debuginfo-5.5.14-77.18.2
php5-bz2-debuginfo-5.5.14-77.18.2
php5-tidy-5.5.14-77.18.2
php5-readline-5.5.14-77.18.2
php5-exif-5.5.14-77.18.2
php5-calendar-5.5.14-77.18.2
php5-xsl-debuginfo-5.5.14-77.18.2
php5-xsl-5.5.14-77.18.2
php5-dom-debuginfo-5.5.14-77.18.2
php5-zlib-5.5.14-77.18.2
php5-soap-debuginfo-5.5.14-77.18.2
php5-shmop-debuginfo-5.5.14-77.18.2
php5-intl-debuginfo-5.5.14-77.18.2
php5-ftp-debuginfo-5.5.14-77.18.2
php5-devel-5.5.14-77.18.2
php5-gmp-debuginfo-5.5.14-77.18.2
php5-pgsql-5.5.14-77.18.2
php5-sysvshm-debuginfo-5.5.14-77.18.2
php5-curl-debuginfo-5.5.14-77.18.2
php5-mbstring-debuginfo-5.5.14-77.18.2
php5-wddx-5.5.14-77.18.2
php5-tokenizer-5.5.14-77.18.2
php5-fastcgi-debuginfo-5.5.14-77.18.2
php5-mssql-debuginfo-5.5.14-77.18.2
php5-calendar-debuginfo-5.5.14-77.18.2
php5-posix-debuginfo-5.5.14-77.18.2
php5-json-5.5.14-77.18.2
php5-tokenizer-debuginfo-5.5.14-77.18.2
php5-intl-5.5.14-77.18.2
php5-tidy-debuginfo-5.5.14-77.18.2
php5-fileinfo-debuginfo-5.5.14-77.18.2
php5-mssql-5.5.14-77.18.2
php5-odbc-5.5.14-77.18.2
apache2-mod_php5-5.5.14-77.18.2
php5-pdo-5.5.14-77.18.2

php5-pcntl-5.5.14-77.18.2
php5-bcmath-debuginfo-5.5.14-77.18.2
php5-snmp-debuginfo-5.5.14-77.18.2
php5-opcache-5.5.14-77.18.2
php5-gd-5.5.14-77.18.2
php5-dba-debuginfo-5.5.14-77.18.2
php5-openssl-5.5.14-77.18.2
php5-xmlwriter-debuginfo-5.5.14-77.18.2
php5-suhosin-5.5.14-77.18.2
php5-readline-debuginfo-5.5.14-77.18.2
php5-curl-5.5.14-77.18.2
php5-sockets-debuginfo-5.5.14-77.18.2
php5-pcntl-debuginfo-5.5.14-77.18.2
php5-pspell-debuginfo-5.5.14-77.18.2
php5-posix-5.5.14-77.18.2
php5-pdo-debuginfo-5.5.14-77.18.2
php5-iconv-5.5.14-77.18.2
php5-debugsource-5.5.14-77.18.2
php5-imap-5.5.14-77.18.2
php5-sysvshm-5.5.14-77.18.2
php5-firebird-5.5.14-77.18.2
php5-sysvsem-debuginfo-5.5.14-77.18.2
php5-mysql-5.5.14-77.18.2
php5-pgsql-debuginfo-5.5.14-77.18.2
php5-iconv-debuginfo-5.5.14-77.18.2
php5-odbc-debuginfo-5.5.14-77.18.2
php5-zip-debuginfo-5.5.14-77.18.2
php5-zlib-debuginfo-5.5.14-77.18.2
php5-sysvmsg-debuginfo-5.5.14-77.18.2
php5-bz2-5.5.14-77.18.2
php5-mysql-debuginfo-5.5.14-77.18.2
php5-phar-debuginfo-5.5.14-77.18.2
php5-ctype-5.5.14-77.18.2
php5-pspell-5.5.14-77.18.2
php5-zip-5.5.14-77.18.2
php5-xmlwriter-5.5.14-77.18.2
php5-mcrypt-debuginfo-5.5.14-77.18.2
php5-sysvsem-5.5.14-77.18.2
php5-wddx-debuginfo-5.5.14-77.18.2
php5-fpm-5.5.14-77.18.2
php5-gd-debuginfo-5.5.14-77.18.2
php5-gettext-debuginfo-5.5.14-77.18.2
php5-json-debuginfo-5.5.14-77.18.2
php5-bcmath-5.5.14-77.18.2
php5-ldap-5.5.14-77.18.2
php5-mcrypt-5.5.14-77.18.2
php5-snmp-5.5.14-77.18.2
php5-enchant-5.5.14-77.18.2
php5-debuginfo-5.5.14-77.18.2
php5-sqlite-debuginfo-5.5.14-77.18.2
php5-sockets-5.5.14-77.18.2
php5-5.5.14-77.18.2
php5-phar-5.5.14-77.18.2
php5-dom-5.5.14-77.18.2
php5-ldap-debuginfo-5.5.14-77.18.2
php5-gettext-5.5.14-77.18.2
php5-fileinfo-5.5.14-77.18.2
php5-xmlrpc-debuginfo-5.5.14-77.18.2
php5-firebird-debuginfo-5.5.14-77.18.2
php5-fastcgi-5.5.14-77.18.2

php5-dba-5.5.14-77.18.2
php5-opcache-debuginfo-5.5.14-77.18.2
php5-gmp-5.5.14-77.18.2
php5-imap-debuginfo-5.5.14-77.18.2
php5-exif-debuginfo-5.5.14-77.18.2

noarch
php5-pear-5.5.14-77.18.2

x86_64
php5-xmlreader-5.5.14-77.18.2
php5-sqlite-5.5.14-77.18.2
php5-suhosin-debuginfo-5.5.14-77.18.2
php5-ctype-debuginfo-5.5.14-77.18.2
php5-shmop-5.5.14-77.18.2
php5-sysvmsg-5.5.14-77.18.2
php5-xmlreader-debuginfo-5.5.14-77.18.2
php5-xmlrpc-5.5.14-77.18.2
php5-enchant-debuginfo-5.5.14-77.18.2
php5-mbstring-5.5.14-77.18.2
php5-ftp-5.5.14-77.18.2
apache2-mod_php5-debuginfo-5.5.14-77.18.2
php5-soap-5.5.14-77.18.2
php5-openssl-debuginfo-5.5.14-77.18.2
php5-fpm-debuginfo-5.5.14-77.18.2
php5-bz2-debuginfo-5.5.14-77.18.2
php5-tidy-5.5.14-77.18.2
php5-readline-5.5.14-77.18.2
php5-exif-5.5.14-77.18.2
php5-calendar-5.5.14-77.18.2
php5-xsl-debuginfo-5.5.14-77.18.2
php5-xsl-5.5.14-77.18.2
php5-dom-debuginfo-5.5.14-77.18.2
php5-zlib-5.5.14-77.18.2
php5-soap-debuginfo-5.5.14-77.18.2
php5-shmop-debuginfo-5.5.14-77.18.2
php5-intl-debuginfo-5.5.14-77.18.2
php5-ftp-debuginfo-5.5.14-77.18.2
php5-devel-5.5.14-77.18.2
php5-gmp-debuginfo-5.5.14-77.18.2
php5-pgsql-5.5.14-77.18.2
php5-sysvshm-debuginfo-5.5.14-77.18.2
php5-curl-debuginfo-5.5.14-77.18.2
php5-mbstring-debuginfo-5.5.14-77.18.2
php5-wddx-5.5.14-77.18.2
php5-tokenizer-5.5.14-77.18.2
php5-fastcgi-debuginfo-5.5.14-77.18.2
php5-mssql-debuginfo-5.5.14-77.18.2
php5-calendar-debuginfo-5.5.14-77.18.2
php5-posix-debuginfo-5.5.14-77.18.2
php5-json-5.5.14-77.18.2
php5-tokenizer-debuginfo-5.5.14-77.18.2
php5-intl-5.5.14-77.18.2
php5-tidy-debuginfo-5.5.14-77.18.2
php5-fileinfo-debuginfo-5.5.14-77.18.2
php5-mssql-5.5.14-77.18.2
php5-odbc-5.5.14-77.18.2
apache2-mod_php5-5.5.14-77.18.2
php5-pdo-5.5.14-77.18.2
php5-pcntl-5.5.14-77.18.2

php5-bcmath-debuginfo-5.5.14-77.18.2
php5-snmp-debuginfo-5.5.14-77.18.2
php5-opcache-5.5.14-77.18.2
php5-gd-5.5.14-77.18.2
php5-dba-debuginfo-5.5.14-77.18.2
php5-openssl-5.5.14-77.18.2
php5-xmlwriter-debuginfo-5.5.14-77.18.2
php5-suhosin-5.5.14-77.18.2
php5-readline-debuginfo-5.5.14-77.18.2
php5-curl-5.5.14-77.18.2
php5-sockets-debuginfo-5.5.14-77.18.2
php5-pcntl-debuginfo-5.5.14-77.18.2
php5-pspell-debuginfo-5.5.14-77.18.2
php5-posix-5.5.14-77.18.2
php5-pdo-debuginfo-5.5.14-77.18.2
php5-iconv-5.5.14-77.18.2
php5-debugsource-5.5.14-77.18.2
php5-imap-5.5.14-77.18.2
php5-sysvshm-5.5.14-77.18.2
php5-firebird-5.5.14-77.18.2
php5-sysvsem-debuginfo-5.5.14-77.18.2
php5-mysql-5.5.14-77.18.2
php5-pgsql-debuginfo-5.5.14-77.18.2
php5-iconv-debuginfo-5.5.14-77.18.2
php5-odbc-debuginfo-5.5.14-77.18.2
php5-zip-debuginfo-5.5.14-77.18.2
php5-zlib-debuginfo-5.5.14-77.18.2
php5-sysvmsg-debuginfo-5.5.14-77.18.2
php5-bz2-5.5.14-77.18.2
php5-mysql-debuginfo-5.5.14-77.18.2
php5-phar-debuginfo-5.5.14-77.18.2
php5-ctype-5.5.14-77.18.2
php5-pspell-5.5.14-77.18.2
php5-zip-5.5.14-77.18.2
php5-xmlwriter-5.5.14-77.18.2
php5-mcrypt-debuginfo-5.5.14-77.18.2
php5-sysvsem-5.5.14-77.18.2
php5-wddx-debuginfo-5.5.14-77.18.2
php5-fpm-5.5.14-77.18.2
php5-gd-debuginfo-5.5.14-77.18.2
php5-gettext-debuginfo-5.5.14-77.18.2
php5-json-debuginfo-5.5.14-77.18.2
php5-bcmath-5.5.14-77.18.2
php5-ldap-5.5.14-77.18.2
php5-mcrypt-5.5.14-77.18.2
php5-snmp-5.5.14-77.18.2
php5-enchant-5.5.14-77.18.2
php5-debuginfo-5.5.14-77.18.2
php5-sqlite-debuginfo-5.5.14-77.18.2
php5-sockets-5.5.14-77.18.2
php5-5.5.14-77.18.2

SuSE Linux 42.3
i586
php5-odbc-5.5.14-91.2

146319 - SuSE SLES 11 SP4 SUSE-SU-2018:0263-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0263-1

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/003659.html

SuSE SLES 11 SP4
i586
libevent-1_4-2-1.4.5-24.24.3.1

x86_64
libevent-1_4-2-1.4.5-24.24.3.1

160354 - CentOS 7 CESA-2018-0163 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15134

Description

The scan detected that the host is missing the following update:
CESA-2018-0163

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/022719.html

CentOS 7
x86_64
389-ds-base-snmp-1.3.6.1-26.el7_4
389-ds-base-1.3.6.1-26.el7_4
389-ds-base-libs-1.3.6.1-26.el7_4
389-ds-base-devel-1.3.6.1-26.el7_4

160356 - CentOS 7 CESA-2018-0151 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8539, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-7472

Description

The scan detected that the host is missing the following update:
CESA-2018-0151

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/022730.html

CentOS 7
x86_64
kernel-3.10.0-693.17.1.el7
kernel-headers-3.10.0-693.17.1.el7
kernel-tools-3.10.0-693.17.1.el7
perf-3.10.0-693.17.1.el7
kernel-tools-libs-devel-3.10.0-693.17.1.el7
kernel-tools-libs-3.10.0-693.17.1.el7
kernel-devel-3.10.0-693.17.1.el7
kernel-debug-devel-3.10.0-693.17.1.el7
python-perf-3.10.0-693.17.1.el7
kernel-debug-3.10.0-693.17.1.el7

noarch
kernel-abi-whitelists-3.10.0-693.17.1.el7
kernel-doc-3.10.0-693.17.1.el7

163536 - Oracle Enterprise Linux ELSA-2018-4020 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5157, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
ELSA-2018-4020

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007470.html

OEL6
x86_64
kernel-uek-debug-devel-2.6.39-400.298.2.el6uek
kernel-uek-firmware-2.6.39-400.298.2.el6uek
kernel-uek-doc-2.6.39-400.298.2.el6uek
kernel-uek-2.6.39-400.298.2.el6uek
kernel-uek-devel-2.6.39-400.298.2.el6uek
kernel-uek-debug-2.6.39-400.298.2.el6uek

i386
kernel-uek-debug-devel-2.6.39-400.298.2.el6uek
kernel-uek-firmware-2.6.39-400.298.2.el6uek
kernel-uek-doc-2.6.39-400.298.2.el6uek
kernel-uek-2.6.39-400.298.2.el6uek
kernel-uek-devel-2.6.39-400.298.2.el6uek
kernel-uek-debug-2.6.39-400.298.2.el6uek

163539 - Oracle Enterprise Linux ELSA-2018-4022 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5157, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
ELSA-2018-4022

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007516.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007515.html

OEL7
x86_64
kernel-uek-debug-devel-3.8.13-118.20.2.el7uek
kernel-uek-debug-3.8.13-118.20.2.el7uek
kernel-uek-3.8.13-118.20.2.el7uek
kernel-uek-firmware-3.8.13-118.20.2.el7uek
dtrace-modules-3.8.13-118.20.2.el7uek-0.4.5-3.el7
kernel-uek-devel-3.8.13-118.20.2.el7uek
kernel-uek-doc-3.8.13-118.20.2.el7uek

OEL6
x86_64
kernel-uek-3.8.13-118.20.2.el6uek
kernel-uek-debug-3.8.13-118.20.2.el6uek
kernel-uek-firmware-3.8.13-118.20.2.el6uek
kernel-uek-doc-3.8.13-118.20.2.el6uek
dtrace-modules-3.8.13-118.20.2.el6uek-0.4.5-3.el6
kernel-uek-debug-devel-3.8.13-118.20.2.el6uek
kernel-uek-devel-3.8.13-118.20.2.el6uek

163540 - Oracle Enterprise Linux ELSA-2018-0163 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15134

Description

The scan detected that the host is missing the following update:
ELSA-2018-0163

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007485.html

OEL7
x86_64
389-ds-base-snmp-1.3.6.1-26.el7_4
389-ds-base-1.3.6.1-26.el7_4
389-ds-base-libs-1.3.6.1-26.el7_4
389-ds-base-devel-1.3.6.1-26.el7_4

163542 - Oracle Enterprise Linux ELSA-2018-0151 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8539, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7472

Description

The scan detected that the host is missing the following update:
ELSA-2018-0151

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007483.html

OEL7
x86_64
kernel-3.10.0-693.17.1.el7
kernel-debug-3.10.0-693.17.1.el7
kernel-tools-3.10.0-693.17.1.el7
perf-3.10.0-693.17.1.el7
kernel-tools-libs-devel-3.10.0-693.17.1.el7
kernel-tools-libs-3.10.0-693.17.1.el7
kernel-devel-3.10.0-693.17.1.el7
kernel-debug-devel-3.10.0-693.17.1.el7
kernel-abi-whitelists-3.10.0-693.17.1.el7
kernel-doc-3.10.0-693.17.1.el7
python-perf-3.10.0-693.17.1.el7
kernel-headers-3.10.0-693.17.1.el7

175317 - Scientific Linux Security ERRATA Important: 389-ds-base on SL7.x x86_64 (1801-8825)

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

Risk Level: High

CVE: CVE-2017-15134

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: 389-ds-base on SL7.x x86_64 (1801-8825)

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=8825

SL7
x86_64
389-ds-base-snmp-1.3.6.1-26.el7_4
389-ds-base-debuginfo-1.3.6.1-26.el7_4
389-ds-base-libs-1.3.6.1-26.el7_4
389-ds-base-devel-1.3.6.1-26.el7_4
389-ds-base-1.3.6.1-26.el7_4

175319 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1801-8366)

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

Risk Level: High

CVE: CVE-2015-8539, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7472

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1801-8366)

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=8366

SL7
x86_64
kernel-debug-debuginfo-3.10.0-693.17.1.el7
kernel-tools-debuginfo-3.10.0-693.17.1.el7
perf-debuginfo-3.10.0-693.17.1.el7
kernel-headers-3.10.0-693.17.1.el7
python-perf-3.10.0-693.17.1.el7
kernel-tools-libs-3.10.0-693.17.1.el7
kernel-3.10.0-693.17.1.el7
kernel-debuginfo-3.10.0-693.17.1.el7
kernel-debug-devel-3.10.0-693.17.1.el7
kernel-tools-libs-devel-3.10.0-693.17.1.el7
perf-3.10.0-693.17.1.el7
kernel-debug-3.10.0-693.17.1.el7
kernel-devel-3.10.0-693.17.1.el7
kernel-debuginfo-common-x86_64-3.10.0-693.17.1.el7
kernel-tools-3.10.0-693.17.1.el7
python-perf-debuginfo-3.10.0-693.17.1.el7

noarch
kernel-abi-whitelists-3.10.0-693.17.1.el7
kernel-doc-3.10.0-693.17.1.el7

178581 - Gentoo Linux GLSA-201801-19 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201801-19

Observation

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

https://security.gentoo.org/glsa/201801-19

Affected packages:
app-antivirus/clamav < 0.99.3

23010 - Cisco Nexus 3000 Series Switches GNU glibc Vulnerability (CSCuy38921)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-7547

Description

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

Observation

Cisco NX-OS is networking software.

A vulnerability is present in some versions of Cisco NX-OS. The flaw lies in the glibc component. Successful exploitation by a remote attacker could result in a denial-of-service or arbitrary remote code execution.

23024 - Cisco NX-OS Software Management Interface Denial of Service Vulnerability (cisco-sa-20180117-nxos)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0090

Description

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

Observation

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

A denial-of-service vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to a bad code fix in the 7.3.2 code. Successful exploitation could allow an attacker to cause a denial-of-service condition.

23025 - Oracle Database Server Critical Patch Update January 2018

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

Risk Level: Medium

CVE: CVE-2017-10282, CVE-2017-12617, CVE-2018-2575, CVE-2018-2680

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, retrieve sensitive data or allow a malicious user to takeover the JVM or the Core RDBMS components.

23026 - Oracle Database Server Critical Patch Update January 2018

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10282, CVE-2017-12617, CVE-2018-2575, CVE-2018-2680

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, retrieve sensitive data or allow a malicious user to takeover the JVM or the Core RDBMS components.

23031 - Oracle JDeveloper Critical Patch Update January 2018

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

Risk Level: Medium

CVE: CVE-2017-10273, CVE-2018-2711

Description

Multiple vulnerabilities are present in some versions of Oracle JDeveloper.

Observation

Oracle JDeveloper is a popular development framework for Java applications.

Multiple vulnerabilities are present in some versions of Oracle JDeveloper. The flaws lie in Security Framework and Deployment subcomponents. Successful exploitation could allow a remote attacker to affect confidentiality, integrity, and availability.

23040 - (HT208473) Apple iCloud Vulnerabilities Prior To 7.3

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

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of Apple iCloud.

Observation

Apple iCloud is a manager for the Apple's cloud-based storage service.

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

131005 - Debian Linux 8.0, 9.0 DSA-4100-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11335, CVE-2017-12944, CVE-2017-13726, CVE-2017-13727, CVE-2017-18013, CVE-2017-9935

Description

The scan detected that the host is missing the following update:
DSA-4100-1

Observation

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

http://www.debian.org/security/2018/dsa-4100

Debian 8.0
all
libtiff-doc_4.0.3-12.3+deb8u5
libtiff5_4.0.3-12.3+deb8u5
libtiff-tools_4.0.3-12.3+deb8u5
libtiff-opengl_4.0.3-12.3+deb8u5
libtiff5-dev_4.0.3-12.3+deb8u5
libtiffxx5_4.0.3-12.3+deb8u5

Debian 9.0
all
libtiff-doc_4.0.8-2+deb9u2
libtiff5_4.0.8-2+deb9u2
libtiff-opengl_4.0.8-2+deb9u2
libtiff5-dev_4.0.8-2+deb9u2
libtiff-tools_4.0.8-2+deb9u2
libtiffxx5_4.0.8-2+deb9u2

131007 - Debian Linux 9.0 DSA-4095-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5345

Description

The scan detected that the host is missing the following update:
DSA-4095-1

Observation

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

http://www.debian.org/security/2018/dsa-4095

Debian 9.0
all
gcab_0.7-2+deb9u1

146287 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0229-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14500

Description

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

openSUSE-SU-2018:0229-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00100.html

SuSE Linux 42.2
x86_64
newsbeuter-debugsource-2.9-2.6.1
newsbeuter-2.9-2.6.1
newsbeuter-debuginfo-2.9-2.6.1

noarch
newsbeuter-lang-2.9-2.6.1

SuSE Linux 42.3
x86_64
newsbeuter-debugsource-2.9-8.1
newsbeuter-debuginfo-2.9-8.1
newsbeuter-2.9-8.1

noarch
newsbeuter-lang-2.9-8.1

146289 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0218-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11750, CVE-2017-12641, CVE-2017-12673, CVE-2017-12676, CVE-2017-12935, CVE-2017-13142, CVE-2017-13147, CVE-2017-14103, CVE-2017-15218, CVE-2017-9261, CVE-2017-9262

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0218-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00090.html

SuSE Linux 42.2
x86_64
perl-GraphicsMagick-debuginfo-1.3.25-11.63.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.63.1
libGraphicsMagickWand-Q16-2-1.3.25-11.63.1
perl-GraphicsMagick-1.3.25-11.63.1
GraphicsMagick-1.3.25-11.63.1
libGraphicsMagick-Q16-3-1.3.25-11.63.1
GraphicsMagick-debugsource-1.3.25-11.63.1
libGraphicsMagick++-devel-1.3.25-11.63.1
GraphicsMagick-devel-1.3.25-11.63.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.63.1
GraphicsMagick-debuginfo-1.3.25-11.63.1
libGraphicsMagick3-config-1.3.25-11.63.1

libGraphicsMagick++-Q16-12-1.3.25-11.63.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.63.1

i586
perl-GraphicsMagick-debuginfo-1.3.25-11.63.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.63.1
libGraphicsMagickWand-Q16-2-1.3.25-11.63.1
perl-GraphicsMagick-1.3.25-11.63.1
GraphicsMagick-1.3.25-11.63.1
libGraphicsMagick-Q16-3-1.3.25-11.63.1
GraphicsMagick-debugsource-1.3.25-11.63.1
libGraphicsMagick++-devel-1.3.25-11.63.1
GraphicsMagick-devel-1.3.25-11.63.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.63.1
GraphicsMagick-debuginfo-1.3.25-11.63.1
libGraphicsMagick3-config-1.3.25-11.63.1
libGraphicsMagick++-Q16-12-1.3.25-11.63.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.63.1

SuSE Linux 42.3
x86_64
GraphicsMagick-devel-1.3.25-60.1
libGraphicsMagick++-devel-1.3.25-60.1
GraphicsMagick-debugsource-1.3.25-60.1
perl-GraphicsMagick-debuginfo-1.3.25-60.1
libGraphicsMagick++-Q16-12-1.3.25-60.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-60.1
libGraphicsMagickWand-Q16-2-1.3.25-60.1
perl-GraphicsMagick-1.3.25-60.1
GraphicsMagick-1.3.25-60.1
libGraphicsMagick3-config-1.3.25-60.1
GraphicsMagick-debuginfo-1.3.25-60.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-60.1
libGraphicsMagick-Q16-3-1.3.25-60.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-60.1

i586
GraphicsMagick-devel-1.3.25-60.1
libGraphicsMagick++-devel-1.3.25-60.1
GraphicsMagick-debugsource-1.3.25-60.1
perl-GraphicsMagick-debuginfo-1.3.25-60.1
libGraphicsMagick++-Q16-12-1.3.25-60.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-60.1
libGraphicsMagickWand-Q16-2-1.3.25-60.1
perl-GraphicsMagick-1.3.25-60.1
GraphicsMagick-1.3.25-60.1
libGraphicsMagick3-config-1.3.25-60.1
GraphicsMagick-debuginfo-1.3.25-60.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-60.1
libGraphicsMagick-Q16-3-1.3.25-60.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-60.1

146294 - SuSE SLES 11 SP4 SUSE-SU-2018:0254-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11423, 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:
SUSE-SU-2018:0254-1

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/003654.html

SuSE SLES 11 SP4
i586
clamav-0.99.3-0.20.3.2

x86_64
clamav-0.99.3-0.20.3.2

146299 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0211-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6328, CVE-2017-7544

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0211-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00089.html

SuSE Linux 42.2
x86_64
libexif-debugsource-0.6.21-12.3.1
libexif-devel-0.6.21-12.3.1
libexif12-debuginfo-0.6.21-12.3.1
libexif12-debuginfo-32bit-0.6.21-12.3.1
libexif12-0.6.21-12.3.1
libexif12-32bit-0.6.21-12.3.1

i586
libexif12-debuginfo-0.6.21-12.3.1
libexif12-0.6.21-12.3.1
libexif-debugsource-0.6.21-12.3.1
libexif-devel-0.6.21-12.3.1

SuSE Linux 42.3
x86_64
libexif12-32bit-0.6.21-15.1
libexif12-0.6.21-15.1
libexif12-debuginfo-0.6.21-15.1
libexif-devel-0.6.21-15.1
libexif-debugsource-0.6.21-15.1
libexif12-debuginfo-32bit-0.6.21-15.1

i586
libexif12-0.6.21-15.1
libexif12-debuginfo-0.6.21-15.1
libexif-devel-0.6.21-15.1
libexif-debugsource-0.6.21-15.1

146305 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0255-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11423, 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:
SUSE-SU-2018:0255-1

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/003655.html

SuSE SLES 12 SP2
x86_64
clamav-debugsource-0.99.3-33.5.1
clamav-debuginfo-0.99.3-33.5.1
clamav-0.99.3-33.5.1

SuSE SLED 12 SP3
x86_64
clamav-debugsource-0.99.3-33.5.1
clamav-debuginfo-0.99.3-33.5.1
clamav-0.99.3-33.5.1

SuSE SLED 12 SP2
x86_64
clamav-debugsource-0.99.3-33.5.1
clamav-debuginfo-0.99.3-33.5.1
clamav-0.99.3-33.5.1

SuSE SLES 12 SP3
x86_64
clamav-debugsource-0.99.3-33.5.1
clamav-debuginfo-0.99.3-33.5.1
clamav-0.99.3-33.5.1

146308 - SuSE Linux 42.3 openSUSE-SU-2018:0258-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11423, 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:

openSUSE-SU-2018:0258-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00106.html

SuSE Linux 42.3
x86_64
clamav-debuginfo-0.99.3-20.1
clamav-debugsource-0.99.3-20.1
clamav-0.99.3-20.1

146309 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0227-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15369, CVE-2017-15587, CVE-2017-17858, CVE-2017-17866, CVE-2018-5686

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0227-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00098.html

SuSE Linux 42.2
x86_64
mupdf-1.12.0-13.10.1
mupdf-devel-static-1.12.0-13.10.1

i586
mupdf-1.12.0-13.10.1
mupdf-devel-static-1.12.0-13.10.1

SuSE Linux 42.3
x86_64
mupdf-devel-static-1.12.0-23.1
mupdf-1.12.0-23.1

i586
mupdf-devel-static-1.12.0-23.1
mupdf-1.12.0-23.1

146312 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0193-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6328, CVE-2017-7544

Description

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

SUSE-SU-2018:0193-1

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/003625.html

SuSE SLES 12 SP2
x86_64
libexif12-debuginfo-32bit-0.6.21-8.3.1
libexif-debugsource-0.6.21-8.3.1
libexif12-0.6.21-8.3.1
libexif12-32bit-0.6.21-8.3.1
libexif12-debuginfo-0.6.21-8.3.1

SuSE SLED 12 SP3
x86_64
libexif12-debuginfo-32bit-0.6.21-8.3.1
libexif-debugsource-0.6.21-8.3.1
libexif12-0.6.21-8.3.1
libexif12-32bit-0.6.21-8.3.1
libexif12-debuginfo-0.6.21-8.3.1

SuSE SLED 12 SP2
x86_64
libexif12-debuginfo-32bit-0.6.21-8.3.1
libexif-debugsource-0.6.21-8.3.1
libexif12-0.6.21-8.3.1
libexif12-32bit-0.6.21-8.3.1
libexif12-debuginfo-0.6.21-8.3.1

SuSE SLES 12 SP3
x86_64
libexif12-debuginfo-32bit-0.6.21-8.3.1
libexif-debugsource-0.6.21-8.3.1
libexif12-0.6.21-8.3.1
libexif12-32bit-0.6.21-8.3.1
libexif12-debuginfo-0.6.21-8.3.1

146315 - SuSE SLES 11 SP4 SUSE-SU-2018:0195-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7544

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0195-1

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/003626.html

SuSE SLES 11 SP4

i586
libexif-0.6.17-2.14.3.1

x86_64
libexif-32bit-0.6.17-2.14.3.1
libexif-0.6.17-2.14.3.1

182584 - FreeBSD gcab Stack Overflow (2cceb80e-c482-4cfd-81b3-2088d2c0ad53)

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

Risk Level: Medium

CVE: CVE-2018-5345

Description

The scan detected that the host is missing the following update:
gcab -- stack overflow (2cceb80e-c482-4cfd-81b3-2088d2c0ad53)

Observation

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

http://www.vuxml.org/freebsd/2cceb80e-c482-4cfd-81b3-2088d2c0ad53.html

Affected packages:
gcab < 0.8

186068 - Ubuntu Linux 16.04, 17.10 USN-3551-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu 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:
USN-3551-1

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/004255.html

Ubuntu 17.10

libjavascriptcoregtk-4.0-18_2.18.6-0ubuntu0.17.10.1
libwebkit2gtk-4.0-37_2.18.6-0ubuntu0.17.10.1

Ubuntu 16.04

libwebkit2gtk-4.0-37_2.18.6-0ubuntu0.16.04.1
libjavascriptcoregtk-4.0-18_2.18.6-0ubuntu0.16.04.1

186074 - Ubuntu Linux 16.04, 17.10 USN-3546-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5345

Description

The scan detected that the host is missing the following update:
USN-3546-1

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/004246.html

Ubuntu 17.10

gcab_0.7-4ubuntu0.1
libgcab-1.0-0_0.7-4ubuntu0.1

Ubuntu 16.04

gcab_0.7-1ubuntu0.1
libgcab-1.0-0_0.7-1ubuntu0.1

193215 - Fedora Linux 27 FEDORA-2018-cb339851e7 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-cb339851e7

Observation

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

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

Fedora Core 27

clamav-0.99.3-1.fc27

193220 - Fedora Linux 27 FEDORA-2018-87971e3c98 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5345

Description

The scan detected that the host is missing the following update:
FEDORA-2018-87971e3c98

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

gcab-1.0-1.fc27

193222 - Fedora Linux 27 FEDORA-2018-3199135a7e 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-2018-3199135a7e

Observation

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

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

Fedora Core 27

webkitgtk4-2.18.6-1.fc27

193224 - Fedora Linux 26 FEDORA-2017-774e7863a4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15535

Description

The scan detected that the host is missing the following update:
FEDORA-2017-774e7863a4

Observation

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

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

Fedora Core 26

mongodb-3.4.10-1.fc26

193231 - Fedora Linux 27 FEDORA-2017-913288e9a9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15535

Description

The scan detected that the host is missing the following update:
FEDORA-2017-913288e9a9

Observation

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

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

Fedora Core 27

mongodb-3.4.10-1.fc27

23005 - (K20682450) F5 BIG-IP BIG-IP AFM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6142

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in IP Intelligence (IPI) policy enforcement. Successful exploitation could allow an attacker to launch man-in-the-middle attacks.

23027 - IBM AIX Spectre and Meltdown Vulnerabilities (spectre_meltdown_advisory)

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

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of IBM AIX.

Observation

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

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lies in modern processors. Successful exploitation could allow an attacker to obtain sensitive information.

23028 - (K34514540) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6138

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.

131004 - Debian Linux 8.0, 9.0 DSA-4097-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000456, CVE-2017-14929

Description

The scan detected that the host is missing the following update:
DSA-4097-1

Observation

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

http://www.debian.org/security/2018/dsa-4097

Debian 8.0
all
libpoppler-glib-doc_0.26.5-2+deb8u3
libpoppler-private-dev_0.26.5-2+deb8u3
libpoppler-qt4-dev_0.26.5-2+deb8u3
libpoppler-qt5-dev_0.26.5-2+deb8u3
libpoppler-qt5-1_0.26.5-2+deb8u3
libpoppler-glib8_0.26.5-2+deb8u3
poppler-dbg_0.26.5-2+deb8u3
libpoppler-glib-dev_0.26.5-2+deb8u3
poppler-utils_0.26.5-2+deb8u3
libpoppler-cpp0_0.26.5-2+deb8u3
libpoppler-dev_0.26.5-2+deb8u3
libpoppler-qt4-4_0.26.5-2+deb8u3
libpoppler46_0.26.5-2+deb8u3
gir1.2-poppler-0.18_0.26.5-2+deb8u3
libpoppler-cpp-dev_0.26.5-2+deb8u3

Debian 9.0
all
gir1.2-poppler-0.18_0.48.0-2+deb9u2
libpoppler-qt4-4_0.48.0-2+deb9u2
libpoppler-private-dev_0.48.0-2+deb9u2
libpoppler-qt5-dev_0.48.0-2+deb9u2
poppler-dbg_0.48.0-2+deb9u2
libpoppler-qt4-dev_0.48.0-2+deb9u2
poppler-utils_0.48.0-2+deb9u2
libpoppler-glib-doc_0.48.0-2+deb9u2
libpoppler-qt5-1_0.48.0-2+deb9u2
libpoppler64_0.48.0-2+deb9u2
libpoppler-cpp-dev_0.48.0-2+deb9u2
libpoppler-cpp0v5_0.48.0-2+deb9u2

libpoppler-glib-dev_0.48.0-2+deb9u2
libpoppler-dev_0.48.0-2+deb9u2
libpoppler-glib8_0.48.0-2+deb9u2

141863 - Red Hat Enterprise Linux RHSA-2018-0158 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3144

Description

The scan detected that the host is missing the following update:
RHSA-2018-0158

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/msg00082.html

RHEL7D
x86_64
dhcp-debuginfo-4.2.5-58.el7_4.1
dhcp-devel-4.2.5-58.el7_4.1
dhcp-libs-4.2.5-58.el7_4.1
dhclient-4.2.5-58.el7_4.1
dhcp-common-4.2.5-58.el7_4.1
dhcp-4.2.5-58.el7_4.1

RHEL7S
x86_64
dhcp-debuginfo-4.2.5-58.el7_4.1
dhcp-devel-4.2.5-58.el7_4.1
dhcp-libs-4.2.5-58.el7_4.1
dhclient-4.2.5-58.el7_4.1
dhcp-common-4.2.5-58.el7_4.1
dhcp-4.2.5-58.el7_4.1

RHEL7WS
x86_64
dhcp-debuginfo-4.2.5-58.el7_4.1
dhcp-devel-4.2.5-58.el7_4.1
dhcp-libs-4.2.5-58.el7_4.1
dhclient-4.2.5-58.el7_4.1
dhcp-common-4.2.5-58.el7_4.1
dhcp-4.2.5-58.el7_4.1

146283 - SuSE SLES 11 SP4 SUSE-SU-2018:0232-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16899

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0232-1

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/003636.html

SuSE SLES 11 SP4
i586
transfig-3.2.5-160.3.2

x86_64
transfig-3.2.5-160.3.2

146291 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0191-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17935, CVE-2018-5334, CVE-2018-5335, CVE-2018-5336

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0191-1

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/003624.html

SuSE SLES 12 SP2
x86_64
libwscodecs1-2.2.12-48.18.1
wireshark-debuginfo-2.2.12-48.18.1
libwireshark8-2.2.12-48.18.1
libwsutil7-2.2.12-48.18.1
libwireshark8-debuginfo-2.2.12-48.18.1
wireshark-gtk-2.2.12-48.18.1
wireshark-2.2.12-48.18.1
libwiretap6-debuginfo-2.2.12-48.18.1
wireshark-debugsource-2.2.12-48.18.1
libwsutil7-debuginfo-2.2.12-48.18.1
libwscodecs1-debuginfo-2.2.12-48.18.1
wireshark-gtk-debuginfo-2.2.12-48.18.1
libwiretap6-2.2.12-48.18.1

SuSE SLED 12 SP3
x86_64
libwscodecs1-2.2.12-48.18.1
wireshark-debuginfo-2.2.12-48.18.1
libwireshark8-2.2.12-48.18.1
libwsutil7-2.2.12-48.18.1
libwireshark8-debuginfo-2.2.12-48.18.1
wireshark-gtk-2.2.12-48.18.1
wireshark-2.2.12-48.18.1
libwiretap6-debuginfo-2.2.12-48.18.1
wireshark-debugsource-2.2.12-48.18.1
libwsutil7-debuginfo-2.2.12-48.18.1

libwscodecs1-debuginfo-2.2.12-48.18.1
wireshark-gtk-debuginfo-2.2.12-48.18.1
libwiretap6-2.2.12-48.18.1

SuSE SLED 12 SP2
x86_64
libwscodecs1-2.2.12-48.18.1
wireshark-debuginfo-2.2.12-48.18.1
libwireshark8-2.2.12-48.18.1
libwsutil7-2.2.12-48.18.1
libwireshark8-debuginfo-2.2.12-48.18.1
wireshark-gtk-2.2.12-48.18.1
wireshark-2.2.12-48.18.1
libwiretap6-debuginfo-2.2.12-48.18.1
wireshark-debugsource-2.2.12-48.18.1
libwsutil7-debuginfo-2.2.12-48.18.1
libwscodecs1-debuginfo-2.2.12-48.18.1
wireshark-gtk-debuginfo-2.2.12-48.18.1
libwiretap6-2.2.12-48.18.1

SuSE SLES 12 SP3
x86_64
libwscodecs1-2.2.12-48.18.1
wireshark-debuginfo-2.2.12-48.18.1
libwireshark8-2.2.12-48.18.1
libwsutil7-2.2.12-48.18.1
libwireshark8-debuginfo-2.2.12-48.18.1
wireshark-gtk-2.2.12-48.18.1
wireshark-2.2.12-48.18.1
libwiretap6-debuginfo-2.2.12-48.18.1
wireshark-debugsource-2.2.12-48.18.1
libwsutil7-debuginfo-2.2.12-48.18.1
libwscodecs1-debuginfo-2.2.12-48.18.1
wireshark-gtk-debuginfo-2.2.12-48.18.1
libwiretap6-2.2.12-48.18.1

146293 - SuSE SLES 11 SP4 SUSE-SU-2018:0230-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7141, CVE-2018-1000007

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0230-1

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/003634.html

SuSE SLES 11 SP4
i586
libcurl4-7.19.7-1.70.13.1
curl-7.19.7-1.70.13.1

x86_64

libcurl4-32bit-7.19.7-1.70.13.1
libcurl4-7.19.7-1.70.13.1
curl-7.19.7-1.70.13.1

146300 - SuSE Linux 42.3 openSUSE-SU-2018:0291-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7659, CVE-2017-9789

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0291-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00108.html

SuSE Linux 42.3
i586
apache2-devel-2.4.23-19.1
apache2-worker-debuginfo-2.4.23-19.1
apache2-worker-2.4.23-19.1
apache2-2.4.23-19.1
apache2-event-debuginfo-2.4.23-19.1
apache2-debugsource-2.4.23-19.1
apache2-utils-debuginfo-2.4.23-19.1
apache2-prefork-2.4.23-19.1
apache2-prefork-debuginfo-2.4.23-19.1
apache2-example-pages-2.4.23-19.1
apache2-debuginfo-2.4.23-19.1
apache2-utils-2.4.23-19.1
apache2-event-2.4.23-19.1

noarch
apache2-doc-2.4.23-19.1

x86_64
apache2-devel-2.4.23-19.1
apache2-worker-debuginfo-2.4.23-19.1
apache2-worker-2.4.23-19.1
apache2-2.4.23-19.1
apache2-event-debuginfo-2.4.23-19.1
apache2-debugsource-2.4.23-19.1
apache2-utils-debuginfo-2.4.23-19.1
apache2-prefork-2.4.23-19.1
apache2-prefork-debuginfo-2.4.23-19.1
apache2-example-pages-2.4.23-19.1
apache2-debuginfo-2.4.23-19.1
apache2-utils-2.4.23-19.1
apache2-event-2.4.23-19.1

146302 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2018:0261-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7659, CVE-2017-9789

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0261-1

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/003657.html

SuSE SLES 12 SP3
noarch
apache2-doc-2.4.23-29.13.1

x86_64
apache2-utils-2.4.23-29.13.1
apache2-example-pages-2.4.23-29.13.1
apache2-prefork-2.4.23-29.13.1
apache2-prefork-debuginfo-2.4.23-29.13.1
apache2-2.4.23-29.13.1
apache2-debugsource-2.4.23-29.13.1
apache2-worker-2.4.23-29.13.1
apache2-utils-debuginfo-2.4.23-29.13.1
apache2-debuginfo-2.4.23-29.13.1
apache2-worker-debuginfo-2.4.23-29.13.1

SuSE SLES 12 SP2
noarch
apache2-doc-2.4.23-29.13.1

x86_64
apache2-utils-2.4.23-29.13.1
apache2-example-pages-2.4.23-29.13.1
apache2-prefork-2.4.23-29.13.1
apache2-prefork-debuginfo-2.4.23-29.13.1
apache2-2.4.23-29.13.1
apache2-debugsource-2.4.23-29.13.1
apache2-worker-2.4.23-29.13.1
apache2-utils-debuginfo-2.4.23-29.13.1
apache2-debuginfo-2.4.23-29.13.1
apache2-worker-debuginfo-2.4.23-29.13.1

146313 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0299-1 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:
SUSE-SU-2018:0299-1

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/003686.html

SuSE SLES 12 SP2
noarch
systemd-bash-completion-228-150.29.1

x86_64
udev-228-150.29.1
systemd-228-150.29.1
udev-debuginfo-228-150.29.1
systemd-debugsource-228-150.29.1
systemd-32bit-228-150.29.1
libsystemd0-32bit-228-150.29.1
libudev1-228-150.29.1
libsystemd0-debuginfo-32bit-228-150.29.1
systemd-debuginfo-228-150.29.1
libsystemd0-228-150.29.1
systemd-sysvinit-228-150.29.1
systemd-debuginfo-32bit-228-150.29.1
libudev1-debuginfo-32bit-228-150.29.1
libudev1-32bit-228-150.29.1
libudev1-debuginfo-228-150.29.1
libsystemd0-debuginfo-228-150.29.1

SuSE SLED 12 SP3
x86_64
systemd-228-150.29.1
systemd-debugsource-228-150.29.1
udev-228-150.29.1
libsystemd0-debuginfo-32bit-228-150.29.1
systemd-32bit-228-150.29.1
libudev1-32bit-228-150.29.1
systemd-sysvinit-228-150.29.1
systemd-debuginfo-228-150.29.1
libsystemd0-228-150.29.1
libudev1-228-150.29.1
systemd-debuginfo-32bit-228-150.29.1
libudev1-debuginfo-32bit-228-150.29.1
udev-debuginfo-228-150.29.1
libudev1-debuginfo-228-150.29.1
libsystemd0-32bit-228-150.29.1
libsystemd0-debuginfo-228-150.29.1

noarch
systemd-bash-completion-228-150.29.1

SuSE SLED 12 SP2
x86_64
systemd-228-150.29.1
systemd-debugsource-228-150.29.1
udev-228-150.29.1
libsystemd0-debuginfo-32bit-228-150.29.1
systemd-32bit-228-150.29.1
libudev1-32bit-228-150.29.1
systemd-sysvinit-228-150.29.1
systemd-debuginfo-228-150.29.1
libsystemd0-228-150.29.1
libudev1-228-150.29.1

systemd-debuginfo-32bit-228-150.29.1
libudev1-debuginfo-32bit-228-150.29.1
udev-debuginfo-228-150.29.1
libudev1-debuginfo-228-150.29.1
libsystemd0-32bit-228-150.29.1
libsystemd0-debuginfo-228-150.29.1

noarch
systemd-bash-completion-228-150.29.1

SuSE SLES 12 SP3
noarch
systemd-bash-completion-228-150.29.1

x86_64
udev-228-150.29.1
systemd-228-150.29.1
udev-debuginfo-228-150.29.1
systemd-debugsource-228-150.29.1
systemd-32bit-228-150.29.1
libsystemd0-32bit-228-150.29.1
libudev1-228-150.29.1
libsystemd0-debuginfo-32bit-228-150.29.1
systemd-debuginfo-228-150.29.1
libsystemd0-228-150.29.1
systemd-sysvinit-228-150.29.1
systemd-debuginfo-32bit-228-150.29.1
libudev1-debuginfo-32bit-228-150.29.1
libudev1-32bit-228-150.29.1
libudev1-debuginfo-228-150.29.1
libsystemd0-debuginfo-228-150.29.1

146316 - SuSE SLES 11 SP4 SUSE-SU-2018:0246-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13720, CVE-2017-13722, CVE-2017-16612

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0246-1

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/003648.html

SuSE SLES 11 SP4
i586
xorg-x11-libs-7.4-8.26.50.5.3

x86_64
xorg-x11-libs-7.4-8.26.50.5.3
xorg-x11-libs-32bit-7.4-8.26.50.5.3

146320 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0231-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16899

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0231-1

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/003635.html

SuSE SLES 12 SP2
x86_64
transfig-debuginfo-3.2.5e-2.3.2
transfig-debugsource-3.2.5e-2.3.2
transfig-3.2.5e-2.3.2

SuSE SLED 12 SP3
x86_64
transfig-debuginfo-3.2.5e-2.3.2
transfig-debugsource-3.2.5e-2.3.2
transfig-3.2.5e-2.3.2

SuSE SLED 12 SP2
x86_64
transfig-debuginfo-3.2.5e-2.3.2
transfig-debugsource-3.2.5e-2.3.2
transfig-3.2.5e-2.3.2

SuSE SLES 12 SP3
x86_64
transfig-debuginfo-3.2.5e-2.3.2
transfig-debugsource-3.2.5e-2.3.2
transfig-3.2.5e-2.3.2

160355 - CentOS 7 CESA-2018-0158 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3144

Description

The scan detected that the host is missing the following update:
CESA-2018-0158

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/022725.html

CentOS 7
x86_64

dhcp-libs-4.2.5-58.el7.centos.1
dhclient-4.2.5-58.el7.centos.1
dhcp-4.2.5-58.el7.centos.1
dhcp-devel-4.2.5-58.el7.centos.1
dhcp-common-4.2.5-58.el7.centos.1

i686
dhcp-devel-4.2.5-58.el7.centos.1
dhcp-libs-4.2.5-58.el7.centos.1

163537 - Oracle Enterprise Linux ELSA-2018-0158 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3144

Description

The scan detected that the host is missing the following update:
ELSA-2018-0158

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007484.html

OEL7
x86_64
dhclient-4.2.5-58.0.1.el7_4.1
dhcp-4.2.5-58.0.1.el7_4.1
dhcp-libs-4.2.5-58.0.1.el7_4.1
dhcp-common-4.2.5-58.0.1.el7_4.1
dhcp-devel-4.2.5-58.0.1.el7_4.1

175318 - Scientific Linux Security ERRATA Moderate: dhcp on SL7.x x86_64 (1801-9173)

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

Risk Level: Medium

CVE: CVE-2017-3144

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: dhcp on SL7.x x86_64 (1801-9173)

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=9173

SL7
x86_64
dhcp-debuginfo-4.2.5-58.el7_4.1
dhcp-devel-4.2.5-58.el7_4.1
dhcp-libs-4.2.5-58.el7_4.1
dhclient-4.2.5-58.el7_4.1

dhcp-common-4.2.5-58.el7_4.1
dhcp-4.2.5-58.el7_4.1

178582 - Gentoo Linux GLSA-201801-20 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201801-20

Observation

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

https://security.gentoo.org/glsa/201801-20

Affected packages:
dev-vcs/fossil < 2.4

193216 - Fedora Linux 27 FEDORA-2018-8c3a01cc65 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17935

Description

The scan detected that the host is missing the following update:
FEDORA-2018-8c3a01cc65

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

wireshark-2.4.4-1.fc27

23033 - Oracle WebCenter Sites Critical Patch Update January 2018

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

Risk Level: Medium

CVE: CVE-2018-2584

Description

A vulnerability is present in some versions of Oracle WebCenter Sites.

Observation

Oracle WebCenter Sites is a business-oriented product used to create web pages.

A vulnerability is present in some versions of Oracle WebCenter Sites. The flaw lies in Advanced UI sub component. Successful exploitation could allow an attacker to retrieve sensitive data.

131003 - Debian Linux 8.0, 9.0 DSA-4101-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
DSA-4101-1

Observation

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

http://www.debian.org/security/2018/dsa-4101

Debian 8.0
all
wireshark_1.12.1+g01b65bf-4+deb8u13

Debian 9.0
all
wireshark_2.2.6+g32dac6a-2+deb9u2

131009 - Debian Linux 9.0 DSA-4099-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17081

Description

The scan detected that the host is missing the following update:
DSA-4099-1

Observation

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

http://www.debian.org/security/2018/dsa-4099

Debian 9.0
all
ffmpeg_7:3.2.10-1~deb9u1

141856 - Red Hat Enterprise Linux RHSA-2018-0223 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14604

Description

The scan detected that the host is missing the following update:
RHSA-2018-0223

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/msg00087.html

RHEL7D
x86_64
nautilus-devel-3.22.3-4.el7_4
nautilus-debuginfo-3.22.3-4.el7_4
nautilus-extensions-3.22.3-4.el7_4
nautilus-3.22.3-4.el7_4

RHEL7S
x86_64
nautilus-devel-3.22.3-4.el7_4
nautilus-debuginfo-3.22.3-4.el7_4
nautilus-extensions-3.22.3-4.el7_4
nautilus-3.22.3-4.el7_4

RHEL7WS
x86_64
nautilus-devel-3.22.3-4.el7_4
nautilus-debuginfo-3.22.3-4.el7_4
nautilus-extensions-3.22.3-4.el7_4
nautilus-3.22.3-4.el7_4

141857 - Red Hat Enterprise Linux RHSA-2018-0182 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0182

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/msg00086.html

RHEL7_3S
noarch
kernel-abi-whitelists-3.10.0-514.41.1.el7
kernel-doc-3.10.0-514.41.1.el7

x86_64
perf-debuginfo-3.10.0-514.41.1.el7
kernel-debuginfo-3.10.0-514.41.1.el7
kernel-debug-debuginfo-3.10.0-514.41.1.el7
kernel-tools-3.10.0-514.41.1.el7

kernel-debuginfo-common-x86_64-3.10.0-514.41.1.el7
kernel-3.10.0-514.41.1.el7
kernel-tools-libs-3.10.0-514.41.1.el7
perf-3.10.0-514.41.1.el7
kernel-debug-3.10.0-514.41.1.el7
kernel-tools-libs-devel-3.10.0-514.41.1.el7
python-perf-debuginfo-3.10.0-514.41.1.el7
python-perf-3.10.0-514.41.1.el7
kernel-debug-devel-3.10.0-514.41.1.el7
kernel-headers-3.10.0-514.41.1.el7
kernel-tools-debuginfo-3.10.0-514.41.1.el7
kernel-devel-3.10.0-514.41.1.el7

146318 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0284-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0284-1

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/003678.html

SuSE SLES 12 SP2
x86_64
libncurses6-32bit-5.9-58.1
ncurses-utils-debuginfo-5.9-58.1
tack-5.9-58.1
ncurses-debugsource-5.9-58.1
ncurses-devel-debuginfo-32bit-5.9-58.1
libncurses6-5.9-58.1
terminfo-5.9-58.1
libncurses6-debuginfo-5.9-58.1
libncurses6-debuginfo-32bit-5.9-58.1
ncurses-devel-5.9-58.1
libncurses5-debuginfo-5.9-58.1
libncurses5-32bit-5.9-58.1
tack-debuginfo-5.9-58.1
ncurses-devel-32bit-5.9-58.1
terminfo-base-5.9-58.1
libncurses5-5.9-58.1
ncurses-devel-debuginfo-5.9-58.1
libncurses5-debuginfo-32bit-5.9-58.1
ncurses-utils-5.9-58.1

SuSE SLED 12 SP3
x86_64
ncurses-utils-debuginfo-5.9-58.1
tack-5.9-58.1
libncurses6-32bit-5.9-58.1
libncurses6-5.9-58.1

tack-debuginfo-5.9-58.1
terminfo-5.9-58.1
libncurses6-debuginfo-5.9-58.1
libncurses6-debuginfo-32bit-5.9-58.1
ncurses-devel-5.9-58.1
libncurses5-debuginfo-5.9-58.1
libncurses5-32bit-5.9-58.1
ncurses-utils-5.9-58.1
terminfo-base-5.9-58.1
ncurses-devel-debuginfo-5.9-58.1
libncurses5-5.9-58.1
ncurses-debugsource-5.9-58.1
libncurses5-debuginfo-32bit-5.9-58.1

SuSE SLED 12 SP2
x86_64
ncurses-utils-debuginfo-5.9-58.1
tack-5.9-58.1
libncurses6-32bit-5.9-58.1
libncurses6-5.9-58.1
tack-debuginfo-5.9-58.1
terminfo-5.9-58.1
libncurses6-debuginfo-5.9-58.1
libncurses6-debuginfo-32bit-5.9-58.1
ncurses-devel-5.9-58.1
libncurses5-debuginfo-5.9-58.1
libncurses5-32bit-5.9-58.1
ncurses-utils-5.9-58.1
terminfo-base-5.9-58.1
ncurses-devel-debuginfo-5.9-58.1
libncurses5-5.9-58.1
ncurses-debugsource-5.9-58.1
libncurses5-debuginfo-32bit-5.9-58.1

SuSE SLES 12 SP3
x86_64
libncurses6-32bit-5.9-58.1
ncurses-utils-debuginfo-5.9-58.1
tack-5.9-58.1
ncurses-debugsource-5.9-58.1
ncurses-devel-debuginfo-32bit-5.9-58.1
libncurses6-5.9-58.1
terminfo-5.9-58.1
libncurses6-debuginfo-5.9-58.1
libncurses6-debuginfo-32bit-5.9-58.1
ncurses-devel-5.9-58.1
libncurses5-debuginfo-5.9-58.1
libncurses5-32bit-5.9-58.1
tack-debuginfo-5.9-58.1
ncurses-devel-32bit-5.9-58.1
terminfo-base-5.9-58.1
libncurses5-5.9-58.1
ncurses-devel-debuginfo-5.9-58.1
libncurses5-debuginfo-32bit-5.9-58.1
ncurses-utils-5.9-58.1

160353 - CentOS 7 CESA-2018-0223 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14604

Description

The scan detected that the host is missing the following update:
CESA-2018-0223

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/022734.html

CentOS 7
x86_64
nautilus-3.22.3-4.el7_4
nautilus-extensions-3.22.3-4.el7_4
nautilus-devel-3.22.3-4.el7_4

i686
nautilus-3.22.3-4.el7_4
nautilus-extensions-3.22.3-4.el7_4
nautilus-devel-3.22.3-4.el7_4

163541 - Oracle Enterprise Linux ELSA-2018-0223 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14604

Description

The scan detected that the host is missing the following update:
ELSA-2018-0223

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007486.html

OEL7
x86_64
nautilus-3.22.3-4.el7_4
nautilus-extensions-3.22.3-4.el7_4
nautilus-devel-3.22.3-4.el7_4

175322 - Scientific Linux Security ERRATA Moderate: nautilus on SL7.x x86_64 (1801-9492)

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

Risk Level: Medium

CVE: CVE-2017-14604

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: nautilus on SL7.x x86_64 (1801-9492)

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=9492

SL7
x86_64
nautilus-devel-3.22.3-4.el7_4
nautilus-debuginfo-3.22.3-4.el7_4
nautilus-extensions-3.22.3-4.el7_4
nautilus-3.22.3-4.el7_4

186072 - Ubuntu Linux 16.04 USN-3549-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
USN-3549-1

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/004252.html

Ubuntu 16.04

linux-image-4.4.0-1017-kvm_4.4.0-1017.22
linux-image-kvm_4.4.0.1017.16

193217 - Fedora Linux 27 FEDORA-2018-2a1f469c85 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6418, CVE-2017-6420

Description

The scan detected that the host is missing the following update:
FEDORA-2018-2a1f469c85

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=3

Fedora Core 27

clamav-0.99.2-18.fc27

193235 - Fedora Linux 26 FEDORA-2018-a86bad9689 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6418, CVE-2017-6420

Description

The scan detected that the host is missing the following update:
FEDORA-2018-a86bad9689

Observation

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

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

Fedora Core 26

clamav-0.99.2-18.fc26

88911 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-024-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000005, CVE-2018-1000007

Description

The scan detected that the host is missing the following update:
SSA:2018-024-01

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.430089

Slackware 14.0
x86_64
curl-7.58.0-x86_64-1

Slackware 14.2
x86_64
curl-7.58.0-x86_64-1

i586
curl-7.58.0-i586-1

Slackware 14.1
x86_64
curl-7.58.0-x86_64-1

88912 - Slackware Linux 14.2 SSA:2018-025-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2018-025-01

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.357609

Slackware 14.2
x86_64
mozilla-thunderbird-52.6.0-x86_64-1

i586
mozilla-thunderbird-52.6.0-i586-1

131006 - Debian Linux 8.0, 9.0 DSA-4098-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000005, CVE-2018-1000007

Description

The scan detected that the host is missing the following update:
DSA-4098-1

Observation

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

http://www.debian.org/security/2018/dsa-4098

Debian 8.0
all
curl_7.38.0-4+deb8u9

Debian 9.0
all
curl_7.52.1-5+deb9u4

131008 - Debian Linux 9.0 DSA-4102-1 Update Is Not Installed

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

Risk Level: Low

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:
DSA-4102-1

Observation

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

For more information see:

http://www.debian.org/security/2018/dsa-4102

Debian 9.0
all
thunderbird_1:52.6.0-1~deb9u1

131010 - Debian Linux 8.0, 9.0 DSA-4096-1 Update Is Not Installed

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

Risk Level: Low

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:
DSA-4096-1

Observation

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

http://www.debian.org/security/2018/dsa-4096

Debian 8.0
all
firefox-esr_52.6.0esr-1~deb8u1

Debian 9.0
all
firefox-esr_52.6.0esr-1~deb9u1

141862 - Red Hat Enterprise Linux RHSA-2018-0239 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2018-0239

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/msg00088.html

RHEL6_2S
x86_64
redhat-release-server-6Server-6.2.0.8.el6_2.2

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

Description

The scan detected that the host is missing the following update:
firefox -- Arbitrary code execution through unsanitized browser UI (103bf96a-6211-45ab-b567-1555ebb3a86a)

Observation

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

http://www.vuxml.org/freebsd/103bf96a-6211-45ab-b567-1555ebb3a86a.html

Affected packages:
firefox < 58.0.1,1

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

Description

The scan detected that the host is missing the following update:
dovecot -- abort of SASL authentication results in a memory leak (92b8b284-a3a2-41b1-956c-f9cf8b74f500)

Observation

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

http://www.vuxml.org/freebsd/92b8b284-a3a2-41b1-956c-f9cf8b74f500.html

Affected packages:
2.0 < dovecot <= 2.2.33.2_2
2.3 <= dovecot <= 2.3.0

182586 - FreeBSD clamav Multiple Vulnerabilities (b464f61b-84c7-4e1c-8ad4-6cf9efffd025)

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
clamav -- multiple vulnerabilities (b464f61b-84c7-4e1c-8ad4-6cf9efffd025)

Observation

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

http://www.vuxml.org/freebsd/b464f61b-84c7-4e1c-8ad4-6cf9efffd025.html

Affected packages:
clamav < 0.99.3

182587 - FreeBSD cURL Multiple Vulnerabilities (0cbf0fa6-dcb7-469c-b87a-f94cffd94583)

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

Risk Level: Low

CVE: CVE-2018-1000007

Description

The scan detected that the host is missing the following update:
cURL -- Multiple vulnerabilities (0cbf0fa6-dcb7-469c-b87a-f94cffd94583)

Observation

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

http://www.vuxml.org/freebsd/0cbf0fa6-dcb7-469c-b87a-f94cffd94583.html

Affected packages:
curl < 7.58.0

186070 - Ubuntu Linux 16.04 USN-3548-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3548-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004251.html

Ubuntu 16.04

linux-image-generic-hwe-16.04_4.13.0.32.52
linux-image-4.13.0-1019-oem_4.13.0-1019.20
linux-image-4.13.0-1007-azure_4.13.0-1007.9
linux-image-lowlatency-hwe-16.04_4.13.0.32.52
linux-image-4.13.0-32-lowlatency_4.13.0-32.35~16.04.1
linux-image-oem_4.13.0.1019.23
linux-image-azure_4.13.0.1007.8
linux-image-gcp_4.13.0.1008.10
linux-image-4.13.0-1008-gcp_4.13.0-1008.11
linux-image-4.13.0-32-generic_4.13.0-32.35~16.04.1
linux-image-gke_4.13.0.1008.10

186071 - Ubuntu Linux 17.10 USN-3548-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3548-1

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/004250.html

Ubuntu 17.10

linux-image-generic_4.13.0.32.34
linux-image-4.13.0-32-lowlatency_4.13.0-32.35
linux-image-4.13.0-32-generic_4.13.0-32.35
linux-image-lowlatency_4.13.0.32.34

186073 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3529-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7829, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848, CVE-2018-5013, 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:
USN-3529-1

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/004253.html

Ubuntu 16.04

thunderbird_52.6.0+build1-0ubuntu0.16.04.1

Ubuntu 14.04

thunderbird_52.6.0+build1-0ubuntu0.14.04.1

Ubuntu 17.10

thunderbird_52.6.0+build1-0ubuntu0.17.10.1

186076 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3550-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
USN-3550-1

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/004254.html

Ubuntu 16.04

clamav_0.99.3+addedllvm-0ubuntu0.16.04.1

Ubuntu 14.04

clamav_0.99.3+addedllvm-0ubuntu0.14.04.1

Ubuntu 17.10

clamav_0.99.3+addedllvm-0ubuntu0.17.10.1

186077 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3544-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5089, CVE-2018-5090, CVE-2018-5091, CVE-2018-5092, CVE-2018-5093, CVE-2018-5094, CVE-2018-5095, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5100, CVE-2018-5101, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5105, CVE-2018-5106, CVE-2018-5107, CVE-2018-5108, CVE-2018-5109, CVE-2018-5111, CVE-2018-5112, CVE-2018-5113, CVE-2018-5114, CVE-2018-5115, CVE-2018-5116, CVE-2018-5117, CVE-2018-5118, CVE-2018-5119, CVE-2018-5122

Description

The scan detected that the host is missing the following update:
USN-3544-1

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/004247.html

Ubuntu 16.04

firefox_58.0+build6-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_58.0+build6-0ubuntu0.14.04.1

Ubuntu 17.10

firefox_58.0+build6-0ubuntu0.17.10.1

193211 - Fedora Linux 27 FEDORA-2018-fbe4017846 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-fbe4017846

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

dnsmasq-2.78-2.fc27

193212 - Fedora Linux 27 FEDORA-2018-241a5a2409 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000005, CVE-2018-1000007

Description

The scan detected that the host is missing the following update:
FEDORA-2018-241a5a2409

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

curl-7.55.1-9.fc27

193213 - Fedora Linux 26 FEDORA-2018-0ce24a50c3 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-2018-0ce24a50c3

Observation

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

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

Fedora Core 26

firefox-58.0-4.fc26

193214 - Fedora Linux 27 FEDORA-2018-ef9e28d9e4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000472

Description

The scan detected that the host is missing the following update:
FEDORA-2018-ef9e28d9e4

Observation

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

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

Fedora Core 27

poco-1.7.8p3-3.fc27

193218 - Fedora Linux 27 FEDORA-2018-69316c5b7a 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-2018-69316c5b7a

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

unbound-1.6.8-1.fc27

193219 - Fedora Linux 26 FEDORA-2018-6550550774 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3145

Description

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

FEDORA-2018-6550550774

Observation

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

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

Fedora Core 26

dnsperf-2.1.0.0-8.fc26
bind-9.11.2-1.P1.fc26
bind-dyndb-ldap-11.1-6.fc26

193223 - Fedora Linux 26 FEDORA-2018-85655b12b6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000005, CVE-2018-1000007

Description

The scan detected that the host is missing the following update:
FEDORA-2018-85655b12b6

Observation

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

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

Fedora Core 26

curl-7.53.1-14.fc26

193225 - Fedora Linux 26 FEDORA-2018-d50769efa0 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-d50769efa0

Observation

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

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

Fedora Core 26

java-1.8.0-openjdk-1.8.0.161-0.b14.fc26

193227 - Fedora Linux 27 FEDORA-2018-48da15ea59 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-2018-48da15ea59

Observation

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

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

Fedora Core 27

wordpress-4.9.2-1.fc27

193228 - Fedora Linux 27 FEDORA-2018-781b88f72d 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-2018-781b88f72d

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=3

Fedora Core 27

firefox-58.0-3.fc27

193229 - Fedora Linux 27 FEDORA-2018-6cdffa56a2 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-2018-6cdffa56a2

Observation

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

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

Fedora Core 27

firefox-58.0-4.fc27

193230 - Fedora Linux 26 FEDORA-2018-7349a7723e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000472

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7349a7723e

Observation

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

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

Fedora Core 26

poco-1.7.8p3-3.fc26

193232 - Fedora Linux 27 FEDORA-2018-a82015aa02 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-a82015aa02

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

java-1.8.0-openjdk-1.8.0.161-0.b14.fc27

193233 - Fedora Linux 27 FEDORA-2018-499a02cc9d 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-2018-499a02cc9d

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

transmission-2.92-12.fc27

193234 - Fedora Linux 27 FEDORA-2018-f8c54aeec4 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-f8c54aeec4

Observation

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

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

Fedora Core 27

mingw-libtasn1-4.13-1.fc27

193236 - Fedora Linux 26 FEDORA-2018-306856c244 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-2018-306856c244

Observation

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

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

Fedora Core 26

rubygem-rack-protection-1.5.3-5.fc26

193237 - Fedora Linux 26 FEDORA-2018-19c693fd9a 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-2018-19c693fd9a

Observation

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

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

Fedora Core 26

wordpress-4.9.2-1.fc26

193238 - Fedora Linux 27 FEDORA-2018-e2e52fb0bf 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-e2e52fb0bf

Observation

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

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

Fedora Core 27

java-9-openjdk-9.0.4.11-3.fc27

146298 - SuSE SLES 11 SP4 SUSE-SU-2018:0307-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12618

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0307-1

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/003689.html

SuSE SLES 11 SP4

i586
libapr-util1-dbd-sqlite3-1.3.4-12.22.23.3.2
libapr-util1-1.3.4-12.22.23.3.2

x86_64
libapr-util1-dbd-sqlite3-1.3.4-12.22.23.3.2
libapr-util1-1.3.4-12.22.23.3.2

193226 - Fedora Linux 27 FEDORA-2018-669520d2ba Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-18018

Description

The scan detected that the host is missing the following update:
FEDORA-2018-669520d2ba

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

coreutils-8.27-19.fc27

ENHANCED CHECKS

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

22939 - (MSPT-Jan2018) Microsoft Products Speculative Execution Side-Channel Vulnerabilities (CVE-2017-5753)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5753

Update Details

FASLScript is updated

22940 - (MSPT-Jan2018) Microsoft Products Speculative Execution Side-Channel Vulnerabilities (CVE-2017-5715)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5715

Update Details

FASLScript is updated

22941 - (MSPT-Jan2018) Microsoft Products Speculative Execution Side-Channel Vulnerabilities (CVE-2017-5754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5754

Update Details

FASLScript is updated

22587 - (MSPT-Oct2017) Microsoft Office Memory Corruption Vulnerability (CVE-2017-11826)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-11826

Update Details

FASLScript is updated

130124 - Debian Linux 7.0 DSA-3202-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2318, CVE-2015-2319, CVE-2015-2320

Update Details

Risk is updated

135194 - Oracle Solaris 11.1.12.5.0 Update Is Not Installed (CVE-2018-2710)

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

Risk Level: High

CVE: CVE-2018-2710

Update Details

Risk is updated

193191 - Fedora Linux 26 FEDORA-2018-8dc60a4feb Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5332, CVE-2018-5333, CVE-2018-5344

Update Details

Risk is updated

193210 - Fedora Linux 27 FEDORA-2018-262eb7c289 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5332, CVE-2018-5333, CVE-2018-5344

Update Details

Risk is updated

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

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

Risk Level: Medium

CVE: CVE-2017-4948

Update Details

Risk is updated

135193 - Oracle Solaris 11.3.27.4.0 Update Is Not Installed (CVE-2018-2578)

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

Risk Level: Medium

CVE: CVE-2018-2578

Update Details

Risk is updated

21589 - Microsoft Office File Parsing Security Bypass

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-0204

Update Details

Name is updated

22646 - Oracle iPlanet Web Server Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2017-10055

Update Details

FASLScript is updated

22647 - Oracle iPlanet Web Server Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2017-10055

Update Details

FASLScript is updated

23013 - Oracle WebCenter Content Critical Patch Update January 2018

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

Risk Level: Medium

CVE: CVE-2018-2564, CVE-2018-2596

Update Details

Risk is updated

182570 - FreeBSD Flash Player Information Disclosure (9c016563-f582-11e7-b33c-6451062f0f7a)

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

Risk Level: Medium

CVE: CVE-2018-4871

Update Details

Risk is updated

22995 - Wireshark Multiple Vulnerabilities Prior To 2.4.4

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

Risk Level: Medium

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

Update Details

Risk is updated

135195 - Oracle Solaris 11.1.12.5.0 Update Is Not Installed (CVE-2018-2717)

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

Risk Level: Low

CVE: CVE-2018-2717

Update Details

Risk is updated

182480 - FreeBSD nss Use-after-free In TLS 1.2 Generating Handshake Hashes (e71fd9d3-af47-11e7-a633-009c02a2ab30)

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

Risk Level: Low

CVE: CVE-2017-7805

Update Details

FASLScript is updated

182582 - FreeBSD mozilla Multiple Vulnerabilities (a891c5b4-3d7a-4de9-9c71-eef3fd698c77)

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

Risk Level: Low

CVE: CVE-2018-5089, CVE-2018-5090, CVE-2018-5091, CVE-2018-5092, CVE-2018-5093, CVE-2018-5094, CVE-2018-5095, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5100, CVE-2018-5101, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5105, CVE-2018-5106, CVE-2018-5107, CVE-2018-5108, CVE-2018-5109, CVE-2018-5110, CVE-2018-5111, CVE-2018-5112, CVE-2018-5113, CVE-2018-5114, CVE-2018-5115, CVE-2018-5116, CVE-2018-5117, CVE-2018-5118, CVE-2018-5119, CVE-2018-5121, CVE-2018-5122

Update Details

FASLScript is updated

93519 - Mandriva Linux MBS2 MDVSA-2015-077 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1858, CVE-2014-1859

Update Details

Risk is updated

135192 - Oracle Solaris 11.3.27.4.0 Update Is Not Installed (CVE-2018-2577)

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

Risk Level: Low

CVE: CVE-2018-2577

Update Details

Risk is updated

170281 - Amazon Linux AMI ALAS-2014-302 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1858, CVE-2014-1859

Update Details

Risk is updated

187633 - Fedora Linux 20 FEDORA-2014-2289 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1858, CVE-2014-1859

Update Details

Risk is updated

187657 - Fedora Linux 19 FEDORA-2014-2387 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1858, CVE-2014-1859

Update Details

Risk is updated

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70086 - oracle.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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