2017-DEC-14
FSL version 7.5.981

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

132417 - Oracle VM OVMSA-2017-0173 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10044, CVE-2016-10200, CVE-2016-7097, CVE-2016-9604, CVE-2016-9685, CVE-2017-1000111, CVE-2017-1000251, CVE-2017-1000363, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-10661, CVE-2017-11176, CVE-2017-11473, CVE-2017-12134, CVE-2017-12190, CVE-2017-14489, CVE-2017-2671, CVE-2017-7542, CVE-2017-7645, CVE-2017-7889, CVE-2017-8831, CVE-2017-9075, CVE-2017-9077, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0173

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-December/000804.html

OVM3.3
x86_64
kernel-uek-firmware-3.8.13-118.20.1.el6uek
kernel-uek-3.8.13-118.20.1.el6uek

146139 - SuSE SLES 11 SP4 SUSE-SU-2017:3265-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000112, CVE-2017-10661, CVE-2017-12762, CVE-2017-13080, CVE-2017-14051, CVE-2017-14140, CVE-2017-14340, CVE-2017-14489, CVE-2017-15102, CVE-2017-15265, CVE-2017-15274, CVE-2017-16525, CVE-2017-16527, CVE-2017-16529, CVE-2017-16531, CVE-2017-16535, CVE-2017-16536, CVE-2017-16537, CVE-2017-16649, CVE-2017-8831

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3265-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003488.html

SuSE SLES 11 SP4
i586

kernel-default-base-3.0.101-108.18.1
kernel-pae-base-3.0.101-108.18.1
kernel-xen-3.0.101-108.18.1
kernel-syms-3.0.101-108.18.1
kernel-ec2-devel-3.0.101-108.18.1
kernel-ec2-base-3.0.101-108.18.1
kernel-ec2-3.0.101-108.18.1
kernel-xen-devel-3.0.101-108.18.1
kernel-trace-devel-3.0.101-108.18.1
kernel-source-3.0.101-108.18.1
kernel-default-devel-3.0.101-108.18.1
kernel-pae-3.0.101-108.18.1
kernel-trace-3.0.101-108.18.1
kernel-xen-base-3.0.101-108.18.1
kernel-default-3.0.101-108.18.1
kernel-trace-base-3.0.101-108.18.1
kernel-pae-devel-3.0.101-108.18.1

x86_64
kernel-default-base-3.0.101-108.18.1
kernel-xen-3.0.101-108.18.1
kernel-syms-3.0.101-108.18.1
kernel-ec2-devel-3.0.101-108.18.1
kernel-ec2-base-3.0.101-108.18.1
kernel-ec2-3.0.101-108.18.1
kernel-xen-devel-3.0.101-108.18.1
kernel-trace-devel-3.0.101-108.18.1
kernel-source-3.0.101-108.18.1
kernel-default-devel-3.0.101-108.18.1
kernel-trace-3.0.101-108.18.1
kernel-xen-base-3.0.101-108.18.1
kernel-default-3.0.101-108.18.1
kernel-trace-base-3.0.101-108.18.1

146143 - SuSE SLES 11 SP4 SUSE-SU-2017:3231-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16844

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3231-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003477.html

SuSE SLES 11 SP4
i586
procmail-3.22-240.8.3.1

x86_64
procmail-3.22-240.8.3.1

163509 - Oracle Enterprise Linux ELSA-2017-3657 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10044, CVE-2016-10200, CVE-2016-7097, CVE-2016-9604, CVE-2016-9685, CVE-2017-1000111, CVE-2017-1000251, CVE-2017-1000363, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-10661, CVE-2017-11176, CVE-2017-11473, CVE-2017-12134, CVE-2017-12190, CVE-2017-14489, CVE-2017-2671, CVE-2017-7542, CVE-2017-7645, CVE-2017-7889, CVE-2017-8831, CVE-2017-9075, CVE-2017-9077, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
ELSA-2017-3657

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-December/007407.html
http://oss.oracle.com/pipermail/el-errata/2017-December/007408.html

OEL7
x86_64
kernel-uek-debug-devel-3.8.13-118.20.1.el7uek
dtrace-modules-3.8.13-118.20.1.el7uek-0.4.5-3.el7
kernel-uek-doc-3.8.13-118.20.1.el7uek
kernel-uek-debug-3.8.13-118.20.1.el7uek
kernel-uek-3.8.13-118.20.1.el7uek
kernel-uek-devel-3.8.13-118.20.1.el7uek
kernel-uek-firmware-3.8.13-118.20.1.el7uek

OEL6
x86_64
kernel-uek-3.8.13-118.20.1.el6uek
kernel-uek-debug-3.8.13-118.20.1.el6uek
kernel-uek-devel-3.8.13-118.20.1.el6uek
kernel-uek-firmware-3.8.13-118.20.1.el6uek
kernel-uek-debug-devel-3.8.13-118.20.1.el6uek
dtrace-modules-3.8.13-118.20.1.el6uek-0.4.5-3.el6
kernel-uek-doc-3.8.13-118.20.1.el6uek

163513 - Oracle Enterprise Linux ELSA-2017-3658 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9710, CVE-2015-1465, CVE-2015-2686, CVE-2015-4167, CVE-2016-10044, CVE-2016-10200, CVE-2016-9604, CVE-2016-9685, CVE-2017-1000111, CVE-2017-1000251, CVE-2017-1000253, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-10661, CVE-2017-11176, CVE-2017-11473, CVE-2017-12134, CVE-2017-12190, CVE-2017-14489, CVE-2017-2671, CVE-2017-7273, CVE-2017-7308, CVE-2017-7542, CVE-2017-7645, CVE-2017-7889, CVE-2017-8831, CVE-2017-9074, CVE-2017-9075, CVE-2017-9077, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
ELSA-2017-3658

Observation

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

For more information see:

http://oss.oracle.com/pipermail/el-errata/2017-December/007409.html

OEL6
x86_64
kernel-uek-doc-2.6.39-400.298.1.el6uek
kernel-uek-debug-2.6.39-400.298.1.el6uek
kernel-uek-debug-devel-2.6.39-400.298.1.el6uek
kernel-uek-firmware-2.6.39-400.298.1.el6uek
kernel-uek-2.6.39-400.298.1.el6uek
kernel-uek-devel-2.6.39-400.298.1.el6uek

i386
kernel-uek-doc-2.6.39-400.298.1.el6uek
kernel-uek-debug-2.6.39-400.298.1.el6uek
kernel-uek-debug-devel-2.6.39-400.298.1.el6uek
kernel-uek-firmware-2.6.39-400.298.1.el6uek
kernel-uek-2.6.39-400.298.1.el6uek
kernel-uek-devel-2.6.39-400.298.1.el6uek

193032 - Fedora Linux 27 FEDORA-2017-355ac8a91a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0801, CVE-2017-0561, CVE-2017-9417

Description

The scan detected that the host is missing the following update:
FEDORA-2017-355ac8a91a

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/2017/12/?count=200&page=3

Fedora Core 27

linux-firmware-20171126-80.git17e62881.fc27

193039 - Fedora Linux 26 FEDORA-2017-d0a336a2a3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12635, CVE-2017-12636

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d0a336a2a3

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/2017/12/?count=200&page=5

Fedora Core 26

couchdb-1.7.1-3.fc26
erlang-jiffy-0.14.13-1.fc26

193051 - Fedora Linux 27 FEDORA-2017-a20d92573b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12635, CVE-2017-12636

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a20d92573b

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/2017/12/?count=200&page=4

Fedora Core 27

couchdb-1.7.1-3.fc27
erlang-jiffy-0.14.13-1.fc27

193061 - Fedora Linux 25 FEDORA-2017-d7ab32cc23 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16820

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d7ab32cc23

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/2017/12/?count=200&page=5

Fedora Core 25

collectd-5.8.0-2.fc25

193069 - Fedora Linux 27 FEDORA-2017-f47206eae4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16820

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f47206eae4

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/2017/12/?count=200&page=3

Fedora Core 27

collectd-5.8.0-2.fc27

193078 - Fedora Linux 26 FEDORA-2017-a253644369 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0801, CVE-2017-0561, CVE-2017-9417

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a253644369

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/2017/12/?count=200&page=4

Fedora Core 26

linux-firmware-20171126-80.git17e62881.fc26

193080 - Fedora Linux 26 FEDORA-2017-f9cfcef9d6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16820

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f9cfcef9d6

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/2017/12/?count=200&page=4

Fedora Core 26

collectd-5.8.0-2.fc26

22856 - (HT208331) Apple macOS Multiple Vulnerabilities Prior To 10.13.2

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

Risk Level: High

CVE: CVE-2017-1000254, CVE-2017-13826, CVE-2017-13833, CVE-2017-13844, CVE-2017-13847, CVE-2017-13848, CVE-2017-13855, CVE-2017-13858, CVE-2017-13860, CVE-2017-13862, CVE-2017-13865, CVE-2017-13867, CVE-2017-13868, CVE-2017-13869, CVE-2017-13871, CVE-2017-13872, CVE-2017-13875, CVE-2017-13876, CVE-2017-13878, CVE-2017-13883, CVE-2017-3735, CVE-2017-9798

Description

Multiple vulnerabilities are present in some versions of Apple macOS.

Observation

Apple macOS is the operating system developed by Apple.

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

141800 - Red Hat Enterprise Linux RHSA-2017-3401 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427

Description

The scan detected that the host is missing the following update:
RHSA-2017-3401

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00010.html

RHEL6D
x86_64
chromium-browser-63.0.3239.84-1.el6_9
chromium-browser-debuginfo-63.0.3239.84-1.el6_9

i386
chromium-browser-63.0.3239.84-1.el6_9
chromium-browser-debuginfo-63.0.3239.84-1.el6_9

RHEL6S
x86_64
chromium-browser-63.0.3239.84-1.el6_9
chromium-browser-debuginfo-63.0.3239.84-1.el6_9

i386
chromium-browser-63.0.3239.84-1.el6_9
chromium-browser-debuginfo-63.0.3239.84-1.el6_9

RHEL6WS
x86_64
chromium-browser-63.0.3239.84-1.el6_9
chromium-browser-debuginfo-63.0.3239.84-1.el6_9

i386
chromium-browser-63.0.3239.84-1.el6_9
chromium-browser-debuginfo-63.0.3239.84-1.el6_9

146148 - SuSE SLES 11 SP4 SUSE-SU-2017:3242-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13672, CVE-2017-15289, CVE-2017-15592, CVE-2017-15595, CVE-2017-15597

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3242-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003485.html

SuSE SLES 11 SP4
x86_64
xen-doc-html-4.4.4_26-61.17.1
xen-kmp-default-4.4.4_26_3.0.101_108.13-61.17.1
xen-libs-4.4.4_26-61.17.1
xen-tools-domU-4.4.4_26-61.17.1
xen-tools-4.4.4_26-61.17.1
xen-4.4.4_26-61.17.1
xen-libs-32bit-4.4.4_26-61.17.1

i586
xen-libs-4.4.4_26-61.17.1
xen-kmp-pae-4.4.4_26_3.0.101_108.13-61.17.1
xen-kmp-default-4.4.4_26_3.0.101_108.13-61.17.1
xen-tools-domU-4.4.4_26-61.17.1

22801 - WordPress Multiple Vulnerabilities Prior To 4.9.1

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 by an attacker could result in undetermined result.

22826 - (CTX230138) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-15592, CVE-2017-17044, CVE-2017-17045, CVE-2017-7980

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in multiple components. Successful exploitation could allow a malicious administrator of a guest VM to compromise the host.

22829 - Cisco NX-OS Software CLI Command Injection Vulnerability (cisco-sa-20171129-nxos3)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-12334

Description

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

Observation

Cisco NX-OS is a network operating system.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the command line interface (CLI). Successful exploitation could allow a local attacker to perform a command injection attack.

22851 - IBM AIX Java Multiple Vulnerabilities (java_oct2017_advisory)

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10309, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

Multiple vulnerabilities are present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lie in Java SDK component. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

132416 - Oracle VM OVMSA-2017-0172 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9191, CVE-2017-1000405, CVE-2017-12190, CVE-2017-12192, CVE-2017-15649, CVE-2017-16527, CVE-2017-16650, CVE-2017-2618

Description

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

OVMSA-2017-0172

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-December/000803.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-103.10.1.el6uek
kernel-uek-4.1.12-103.10.1.el6uek

141798 - Red Hat Enterprise Linux RHSA-2017-3405 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15097

Description

The scan detected that the host is missing the following update:
RHSA-2017-3405

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00014.html

RHEL7S
x86_64
rh-postgresql96-postgresql-devel-9.6.5-2.el7
rh-postgresql96-postgresql-server-9.6.5-2.el7
rh-postgresql96-postgresql-plpython-9.6.5-2.el7
rh-postgresql96-postgresql-docs-9.6.5-2.el7
rh-postgresql96-postgresql-syspaths-9.6.5-2.el7
rh-postgresql96-postgresql-contrib-syspaths-9.6.5-2.el7
rh-postgresql96-postgresql-debuginfo-9.6.5-2.el7
rh-postgresql96-postgresql-9.6.5-2.el7
rh-postgresql96-postgresql-contrib-9.6.5-2.el7
rh-postgresql96-postgresql-pltcl-9.6.5-2.el7
rh-postgresql96-postgresql-libs-9.6.5-2.el7
rh-postgresql96-postgresql-test-9.6.5-2.el7
rh-postgresql96-postgresql-static-9.6.5-2.el7
rh-postgresql96-postgresql-server-syspaths-9.6.5-2.el7
rh-postgresql96-postgresql-plperl-9.6.5-2.el7

RHEL6S
x86_64
rh-postgresql96-postgresql-server-9.6.5-2.el6
rh-postgresql96-postgresql-plpython-9.6.5-2.el6
rh-postgresql96-postgresql-9.6.5-2.el6
rh-postgresql96-postgresql-docs-9.6.5-2.el6
rh-postgresql96-postgresql-contrib-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-plperl-9.6.5-2.el6
rh-postgresql96-postgresql-devel-9.6.5-2.el6

rh-postgresql96-postgresql-test-9.6.5-2.el6
rh-postgresql96-postgresql-contrib-9.6.5-2.el6
rh-postgresql96-postgresql-pltcl-9.6.5-2.el6
rh-postgresql96-postgresql-libs-9.6.5-2.el6
rh-postgresql96-postgresql-debuginfo-9.6.5-2.el6
rh-postgresql96-postgresql-server-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-static-9.6.5-2.el6

RHEL6WS
x86_64
rh-postgresql96-postgresql-server-9.6.5-2.el6
rh-postgresql96-postgresql-plpython-9.6.5-2.el6
rh-postgresql96-postgresql-9.6.5-2.el6
rh-postgresql96-postgresql-docs-9.6.5-2.el6
rh-postgresql96-postgresql-contrib-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-plperl-9.6.5-2.el6
rh-postgresql96-postgresql-devel-9.6.5-2.el6
rh-postgresql96-postgresql-test-9.6.5-2.el6
rh-postgresql96-postgresql-contrib-9.6.5-2.el6
rh-postgresql96-postgresql-pltcl-9.6.5-2.el6
rh-postgresql96-postgresql-libs-9.6.5-2.el6
rh-postgresql96-postgresql-debuginfo-9.6.5-2.el6
rh-postgresql96-postgresql-server-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-static-9.6.5-2.el6

RHEL6_7S
x86_64
rh-postgresql96-postgresql-server-9.6.5-2.el6
rh-postgresql96-postgresql-plpython-9.6.5-2.el6
rh-postgresql96-postgresql-9.6.5-2.el6
rh-postgresql96-postgresql-docs-9.6.5-2.el6
rh-postgresql96-postgresql-contrib-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-plperl-9.6.5-2.el6
rh-postgresql96-postgresql-devel-9.6.5-2.el6
rh-postgresql96-postgresql-test-9.6.5-2.el6
rh-postgresql96-postgresql-contrib-9.6.5-2.el6
rh-postgresql96-postgresql-pltcl-9.6.5-2.el6
rh-postgresql96-postgresql-libs-9.6.5-2.el6
rh-postgresql96-postgresql-debuginfo-9.6.5-2.el6
rh-postgresql96-postgresql-server-syspaths-9.6.5-2.el6
rh-postgresql96-postgresql-static-9.6.5-2.el6

RHEL7_3S
x86_64
rh-postgresql96-postgresql-devel-9.6.5-2.el7
rh-postgresql96-postgresql-server-9.6.5-2.el7
rh-postgresql96-postgresql-plpython-9.6.5-2.el7
rh-postgresql96-postgresql-docs-9.6.5-2.el7
rh-postgresql96-postgresql-syspaths-9.6.5-2.el7
rh-postgresql96-postgresql-contrib-syspaths-9.6.5-2.el7
rh-postgresql96-postgresql-debuginfo-9.6.5-2.el7
rh-postgresql96-postgresql-9.6.5-2.el7
rh-postgresql96-postgresql-contrib-9.6.5-2.el7
rh-postgresql96-postgresql-pltcl-9.6.5-2.el7
rh-postgresql96-postgresql-libs-9.6.5-2.el7
rh-postgresql96-postgresql-test-9.6.5-2.el7
rh-postgresql96-postgresql-static-9.6.5-2.el7
rh-postgresql96-postgresql-server-syspaths-9.6.5-2.el7

rh-postgresql96-postgresql-plperl-9.6.5-2.el7

RHEL7WS
x86_64
rh-postgresql96-postgresql-devel-9.6.5-2.el7
rh-postgresql96-postgresql-server-9.6.5-2.el7
rh-postgresql96-postgresql-plpython-9.6.5-2.el7
rh-postgresql96-postgresql-docs-9.6.5-2.el7
rh-postgresql96-postgresql-syspaths-9.6.5-2.el7
rh-postgresql96-postgresql-contrib-syspaths-9.6.5-2.el7
rh-postgresql96-postgresql-debuginfo-9.6.5-2.el7
rh-postgresql96-postgresql-9.6.5-2.el7
rh-postgresql96-postgresql-contrib-9.6.5-2.el7
rh-postgresql96-postgresql-pltcl-9.6.5-2.el7
rh-postgresql96-postgresql-libs-9.6.5-2.el7
rh-postgresql96-postgresql-test-9.6.5-2.el7
rh-postgresql96-postgresql-static-9.6.5-2.el7
rh-postgresql96-postgresql-server-syspaths-9.6.5-2.el7
rh-postgresql96-postgresql-plperl-9.6.5-2.el7

141799 - Red Hat Enterprise Linux RHSA-2017-3452 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12629

Description

The scan detected that the host is missing the following update:
RHSA-2017-3452

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00018.html

RHEL7S
noarch
rh-java-common-lucene5-queries-5.4.1-2.4.el7
rh-java-common-lucene5-highlighter-5.4.1-2.4.el7
rh-java-common-lucene5-javadoc-5.4.1-2.4.el7
rh-java-common-lucene5-facet-5.4.1-2.4.el7
rh-java-common-lucene5-grouping-5.4.1-2.4.el7
rh-java-common-lucene5-5.4.1-2.4.el7
rh-java-common-lucene5-solr-grandparent-5.4.1-2.4.el7
rh-java-common-lucene5-analysis-5.4.1-2.4.el7
rh-java-common-lucene5-analyzers-smartcn-5.4.1-2.4.el7
rh-java-common-lucene5-parent-5.4.1-2.4.el7
rh-java-common-lucene5-replicator-5.4.1-2.4.el7
rh-java-common-lucene5-codecs-5.4.1-2.4.el7
rh-java-common-lucene5-join-5.4.1-2.4.el7
rh-java-common-lucene5-misc-5.4.1-2.4.el7
rh-java-common-lucene5-sandbox-5.4.1-2.4.el7
rh-java-common-lucene5-backward-codecs-5.4.1-2.4.el7
rh-java-common-lucene5-classification-5.4.1-2.4.el7
rh-java-common-lucene5-memory-5.4.1-2.4.el7
rh-java-common-lucene5-suggest-5.4.1-2.4.el7
rh-java-common-lucene5-queryparser-5.4.1-2.4.el7

RHEL6S
noarch
rh-java-common-lucene5-highlighter-5.4.1-2.4.el6
rh-java-common-lucene5-parent-5.4.1-2.4.el6
rh-java-common-lucene5-sandbox-5.4.1-2.4.el6
rh-java-common-lucene5-codecs-5.4.1-2.4.el6
rh-java-common-lucene5-suggest-5.4.1-2.4.el6
rh-java-common-lucene5-grouping-5.4.1-2.4.el6
rh-java-common-lucene5-analysis-5.4.1-2.4.el6
rh-java-common-lucene5-solr-grandparent-5.4.1-2.4.el6
rh-java-common-lucene5-backward-codecs-5.4.1-2.4.el6
rh-java-common-lucene5-5.4.1-2.4.el6
rh-java-common-lucene5-replicator-5.4.1-2.4.el6
rh-java-common-lucene5-javadoc-5.4.1-2.4.el6
rh-java-common-lucene5-facet-5.4.1-2.4.el6
rh-java-common-lucene5-misc-5.4.1-2.4.el6
rh-java-common-lucene5-join-5.4.1-2.4.el6
rh-java-common-lucene5-queries-5.4.1-2.4.el6
rh-java-common-lucene5-analyzers-smartcn-5.4.1-2.4.el6
rh-java-common-lucene5-classification-5.4.1-2.4.el6
rh-java-common-lucene5-memory-5.4.1-2.4.el6
rh-java-common-lucene5-queryparser-5.4.1-2.4.el6

RHEL6WS
noarch
rh-java-common-lucene5-highlighter-5.4.1-2.4.el6
rh-java-common-lucene5-parent-5.4.1-2.4.el6
rh-java-common-lucene5-sandbox-5.4.1-2.4.el6
rh-java-common-lucene5-codecs-5.4.1-2.4.el6
rh-java-common-lucene5-suggest-5.4.1-2.4.el6
rh-java-common-lucene5-grouping-5.4.1-2.4.el6
rh-java-common-lucene5-analysis-5.4.1-2.4.el6
rh-java-common-lucene5-solr-grandparent-5.4.1-2.4.el6
rh-java-common-lucene5-backward-codecs-5.4.1-2.4.el6
rh-java-common-lucene5-5.4.1-2.4.el6
rh-java-common-lucene5-replicator-5.4.1-2.4.el6
rh-java-common-lucene5-javadoc-5.4.1-2.4.el6
rh-java-common-lucene5-facet-5.4.1-2.4.el6
rh-java-common-lucene5-misc-5.4.1-2.4.el6
rh-java-common-lucene5-join-5.4.1-2.4.el6
rh-java-common-lucene5-queries-5.4.1-2.4.el6
rh-java-common-lucene5-analyzers-smartcn-5.4.1-2.4.el6
rh-java-common-lucene5-classification-5.4.1-2.4.el6
rh-java-common-lucene5-memory-5.4.1-2.4.el6
rh-java-common-lucene5-queryparser-5.4.1-2.4.el6

RHEL6_7S
noarch
rh-java-common-lucene5-highlighter-5.4.1-2.4.el6
rh-java-common-lucene5-parent-5.4.1-2.4.el6
rh-java-common-lucene5-sandbox-5.4.1-2.4.el6
rh-java-common-lucene5-codecs-5.4.1-2.4.el6
rh-java-common-lucene5-suggest-5.4.1-2.4.el6
rh-java-common-lucene5-grouping-5.4.1-2.4.el6
rh-java-common-lucene5-analysis-5.4.1-2.4.el6
rh-java-common-lucene5-solr-grandparent-5.4.1-2.4.el6
rh-java-common-lucene5-backward-codecs-5.4.1-2.4.el6
rh-java-common-lucene5-5.4.1-2.4.el6
rh-java-common-lucene5-replicator-5.4.1-2.4.el6

rh-java-common-lucene5-javadoc-5.4.1-2.4.el6
rh-java-common-lucene5-facet-5.4.1-2.4.el6
rh-java-common-lucene5-misc-5.4.1-2.4.el6
rh-java-common-lucene5-join-5.4.1-2.4.el6
rh-java-common-lucene5-queries-5.4.1-2.4.el6
rh-java-common-lucene5-analyzers-smartcn-5.4.1-2.4.el6
rh-java-common-lucene5-classification-5.4.1-2.4.el6
rh-java-common-lucene5-memory-5.4.1-2.4.el6
rh-java-common-lucene5-queryparser-5.4.1-2.4.el6

RHEL7_3S
noarch
rh-java-common-lucene5-queries-5.4.1-2.4.el7
rh-java-common-lucene5-highlighter-5.4.1-2.4.el7
rh-java-common-lucene5-javadoc-5.4.1-2.4.el7
rh-java-common-lucene5-facet-5.4.1-2.4.el7
rh-java-common-lucene5-grouping-5.4.1-2.4.el7
rh-java-common-lucene5-5.4.1-2.4.el7
rh-java-common-lucene5-solr-grandparent-5.4.1-2.4.el7
rh-java-common-lucene5-analysis-5.4.1-2.4.el7
rh-java-common-lucene5-analyzers-smartcn-5.4.1-2.4.el7
rh-java-common-lucene5-parent-5.4.1-2.4.el7
rh-java-common-lucene5-replicator-5.4.1-2.4.el7
rh-java-common-lucene5-codecs-5.4.1-2.4.el7
rh-java-common-lucene5-join-5.4.1-2.4.el7
rh-java-common-lucene5-misc-5.4.1-2.4.el7
rh-java-common-lucene5-sandbox-5.4.1-2.4.el7
rh-java-common-lucene5-backward-codecs-5.4.1-2.4.el7
rh-java-common-lucene5-classification-5.4.1-2.4.el7
rh-java-common-lucene5-memory-5.4.1-2.4.el7
rh-java-common-lucene5-suggest-5.4.1-2.4.el7
rh-java-common-lucene5-queryparser-5.4.1-2.4.el7

RHEL7WS
noarch
rh-java-common-lucene5-queries-5.4.1-2.4.el7
rh-java-common-lucene5-highlighter-5.4.1-2.4.el7
rh-java-common-lucene5-javadoc-5.4.1-2.4.el7
rh-java-common-lucene5-facet-5.4.1-2.4.el7
rh-java-common-lucene5-grouping-5.4.1-2.4.el7
rh-java-common-lucene5-5.4.1-2.4.el7
rh-java-common-lucene5-solr-grandparent-5.4.1-2.4.el7
rh-java-common-lucene5-analysis-5.4.1-2.4.el7
rh-java-common-lucene5-analyzers-smartcn-5.4.1-2.4.el7
rh-java-common-lucene5-parent-5.4.1-2.4.el7
rh-java-common-lucene5-replicator-5.4.1-2.4.el7
rh-java-common-lucene5-codecs-5.4.1-2.4.el7
rh-java-common-lucene5-join-5.4.1-2.4.el7
rh-java-common-lucene5-misc-5.4.1-2.4.el7
rh-java-common-lucene5-sandbox-5.4.1-2.4.el7
rh-java-common-lucene5-backward-codecs-5.4.1-2.4.el7
rh-java-common-lucene5-classification-5.4.1-2.4.el7
rh-java-common-lucene5-memory-5.4.1-2.4.el7
rh-java-common-lucene5-suggest-5.4.1-2.4.el7
rh-java-common-lucene5-queryparser-5.4.1-2.4.el7

141801 - Red Hat Enterprise Linux RHSA-2017-3451 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12629

Description

The scan detected that the host is missing the following update:
RHSA-2017-3451

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00017.html

RHEL7S
noarch
rh-java-common-lucene-codecs-4.8.0-6.9.el7
rh-java-common-lucene-parent-4.8.0-6.9.el7
rh-java-common-lucene-sandbox-4.8.0-6.9.el7
rh-java-common-lucene-solr-grandparent-4.8.0-6.9.el7
rh-java-common-lucene-queries-4.8.0-6.9.el7
rh-java-common-lucene-grouping-4.8.0-6.9.el7
rh-java-common-lucene-suggest-4.8.0-6.9.el7
rh-java-common-lucene-classification-4.8.0-6.9.el7
rh-java-common-lucene-replicator-4.8.0-6.9.el7
rh-java-common-lucene-javadoc-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-phonetic-4.8.0-6.9.el7
rh-java-common-lucene-misc-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-smartcn-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-stempel-4.8.0-6.9.el7
rh-java-common-lucene-memory-4.8.0-6.9.el7
rh-java-common-lucene-join-4.8.0-6.9.el7
rh-java-common-lucene-queryparser-4.8.0-6.9.el7
rh-java-common-lucene-facet-4.8.0-6.9.el7
rh-java-common-lucene-highlighter-4.8.0-6.9.el7
rh-java-common-lucene-analysis-4.8.0-6.9.el7
rh-java-common-lucene-4.8.0-6.9.el7

RHEL6S
noarch
rh-java-common-lucene-codecs-4.8.0-6.9.el6
rh-java-common-lucene-parent-4.8.0-6.9.el6
rh-java-common-lucene-solr-grandparent-4.8.0-6.9.el6
rh-java-common-lucene-classification-4.8.0-6.9.el6
rh-java-common-lucene-queries-4.8.0-6.9.el6
rh-java-common-lucene-queryparser-4.8.0-6.9.el6
rh-java-common-lucene-suggest-4.8.0-6.9.el6
rh-java-common-lucene-misc-4.8.0-6.9.el6
rh-java-common-lucene-join-4.8.0-6.9.el6
rh-java-common-lucene-sandbox-4.8.0-6.9.el6
rh-java-common-lucene-memory-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-smartcn-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-stempel-4.8.0-6.9.el6
rh-java-common-lucene-replicator-4.8.0-6.9.el6
rh-java-common-lucene-grouping-4.8.0-6.9.el6
rh-java-common-lucene-javadoc-4.8.0-6.9.el6
rh-java-common-lucene-highlighter-4.8.0-6.9.el6
rh-java-common-lucene-facet-4.8.0-6.9.el6
rh-java-common-lucene-analysis-4.8.0-6.9.el6
rh-java-common-lucene-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-phonetic-4.8.0-6.9.el6

RHEL6WS
noarch
rh-java-common-lucene-codecs-4.8.0-6.9.el6
rh-java-common-lucene-parent-4.8.0-6.9.el6
rh-java-common-lucene-solr-grandparent-4.8.0-6.9.el6
rh-java-common-lucene-classification-4.8.0-6.9.el6
rh-java-common-lucene-queries-4.8.0-6.9.el6
rh-java-common-lucene-queryparser-4.8.0-6.9.el6
rh-java-common-lucene-suggest-4.8.0-6.9.el6
rh-java-common-lucene-misc-4.8.0-6.9.el6
rh-java-common-lucene-join-4.8.0-6.9.el6
rh-java-common-lucene-sandbox-4.8.0-6.9.el6
rh-java-common-lucene-memory-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-smartcn-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-stempel-4.8.0-6.9.el6
rh-java-common-lucene-replicator-4.8.0-6.9.el6
rh-java-common-lucene-grouping-4.8.0-6.9.el6
rh-java-common-lucene-javadoc-4.8.0-6.9.el6
rh-java-common-lucene-highlighter-4.8.0-6.9.el6
rh-java-common-lucene-facet-4.8.0-6.9.el6
rh-java-common-lucene-analysis-4.8.0-6.9.el6
rh-java-common-lucene-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-phonetic-4.8.0-6.9.el6

RHEL6_7S
noarch
rh-java-common-lucene-codecs-4.8.0-6.9.el6
rh-java-common-lucene-parent-4.8.0-6.9.el6
rh-java-common-lucene-solr-grandparent-4.8.0-6.9.el6
rh-java-common-lucene-classification-4.8.0-6.9.el6
rh-java-common-lucene-queries-4.8.0-6.9.el6
rh-java-common-lucene-queryparser-4.8.0-6.9.el6
rh-java-common-lucene-suggest-4.8.0-6.9.el6
rh-java-common-lucene-misc-4.8.0-6.9.el6
rh-java-common-lucene-join-4.8.0-6.9.el6
rh-java-common-lucene-sandbox-4.8.0-6.9.el6
rh-java-common-lucene-memory-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-smartcn-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-stempel-4.8.0-6.9.el6
rh-java-common-lucene-replicator-4.8.0-6.9.el6
rh-java-common-lucene-grouping-4.8.0-6.9.el6
rh-java-common-lucene-javadoc-4.8.0-6.9.el6
rh-java-common-lucene-highlighter-4.8.0-6.9.el6
rh-java-common-lucene-facet-4.8.0-6.9.el6
rh-java-common-lucene-analysis-4.8.0-6.9.el6
rh-java-common-lucene-4.8.0-6.9.el6
rh-java-common-lucene-analyzers-phonetic-4.8.0-6.9.el6

RHEL7_3S
noarch
rh-java-common-lucene-codecs-4.8.0-6.9.el7
rh-java-common-lucene-parent-4.8.0-6.9.el7
rh-java-common-lucene-sandbox-4.8.0-6.9.el7
rh-java-common-lucene-solr-grandparent-4.8.0-6.9.el7
rh-java-common-lucene-queries-4.8.0-6.9.el7
rh-java-common-lucene-grouping-4.8.0-6.9.el7
rh-java-common-lucene-suggest-4.8.0-6.9.el7
rh-java-common-lucene-classification-4.8.0-6.9.el7
rh-java-common-lucene-replicator-4.8.0-6.9.el7

rh-java-common-lucene-javadoc-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-phonetic-4.8.0-6.9.el7
rh-java-common-lucene-misc-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-smartcn-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-stempel-4.8.0-6.9.el7
rh-java-common-lucene-memory-4.8.0-6.9.el7
rh-java-common-lucene-join-4.8.0-6.9.el7
rh-java-common-lucene-queryparser-4.8.0-6.9.el7
rh-java-common-lucene-facet-4.8.0-6.9.el7
rh-java-common-lucene-highlighter-4.8.0-6.9.el7
rh-java-common-lucene-analysis-4.8.0-6.9.el7
rh-java-common-lucene-4.8.0-6.9.el7

RHEL7WS
noarch
rh-java-common-lucene-codecs-4.8.0-6.9.el7
rh-java-common-lucene-parent-4.8.0-6.9.el7
rh-java-common-lucene-sandbox-4.8.0-6.9.el7
rh-java-common-lucene-solr-grandparent-4.8.0-6.9.el7
rh-java-common-lucene-queries-4.8.0-6.9.el7
rh-java-common-lucene-grouping-4.8.0-6.9.el7
rh-java-common-lucene-suggest-4.8.0-6.9.el7
rh-java-common-lucene-classification-4.8.0-6.9.el7
rh-java-common-lucene-replicator-4.8.0-6.9.el7
rh-java-common-lucene-javadoc-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-phonetic-4.8.0-6.9.el7
rh-java-common-lucene-misc-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-smartcn-4.8.0-6.9.el7
rh-java-common-lucene-analyzers-stempel-4.8.0-6.9.el7
rh-java-common-lucene-memory-4.8.0-6.9.el7
rh-java-common-lucene-join-4.8.0-6.9.el7
rh-java-common-lucene-queryparser-4.8.0-6.9.el7
rh-java-common-lucene-facet-4.8.0-6.9.el7
rh-java-common-lucene-highlighter-4.8.0-6.9.el7
rh-java-common-lucene-analysis-4.8.0-6.9.el7
rh-java-common-lucene-4.8.0-6.9.el7

141802 - Red Hat Enterprise Linux RHSA-2017-3404 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15097

Description

The scan detected that the host is missing the following update:
RHSA-2017-3404

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00013.html

RHEL7S
x86_64
rh-postgresql95-postgresql-contrib-9.5.9-4.el7
rh-postgresql95-postgresql-plperl-9.5.9-4.el7
rh-postgresql95-postgresql-plpython-9.5.9-4.el7

rh-postgresql95-postgresql-pltcl-9.5.9-4.el7
rh-postgresql95-postgresql-devel-9.5.9-4.el7
rh-postgresql95-postgresql-docs-9.5.9-4.el7
rh-postgresql95-postgresql-libs-9.5.9-4.el7
rh-postgresql95-postgresql-test-9.5.9-4.el7
rh-postgresql95-postgresql-debuginfo-9.5.9-4.el7
rh-postgresql95-postgresql-static-9.5.9-4.el7
rh-postgresql95-postgresql-9.5.9-4.el7
rh-postgresql95-postgresql-server-9.5.9-4.el7

RHEL6S
x86_64
rh-postgresql95-postgresql-plperl-9.5.9-4.el6
rh-postgresql95-postgresql-static-9.5.9-4.el6
rh-postgresql95-postgresql-devel-9.5.9-4.el6
rh-postgresql95-postgresql-contrib-9.5.9-4.el6
rh-postgresql95-postgresql-plpython-9.5.9-4.el6
rh-postgresql95-postgresql-debuginfo-9.5.9-4.el6
rh-postgresql95-postgresql-docs-9.5.9-4.el6
rh-postgresql95-postgresql-9.5.9-4.el6
rh-postgresql95-postgresql-libs-9.5.9-4.el6
rh-postgresql95-postgresql-server-9.5.9-4.el6
rh-postgresql95-postgresql-pltcl-9.5.9-4.el6
rh-postgresql95-postgresql-test-9.5.9-4.el6

RHEL6WS
x86_64
rh-postgresql95-postgresql-plperl-9.5.9-4.el6
rh-postgresql95-postgresql-static-9.5.9-4.el6
rh-postgresql95-postgresql-devel-9.5.9-4.el6
rh-postgresql95-postgresql-contrib-9.5.9-4.el6
rh-postgresql95-postgresql-plpython-9.5.9-4.el6
rh-postgresql95-postgresql-debuginfo-9.5.9-4.el6
rh-postgresql95-postgresql-docs-9.5.9-4.el6
rh-postgresql95-postgresql-9.5.9-4.el6
rh-postgresql95-postgresql-libs-9.5.9-4.el6
rh-postgresql95-postgresql-server-9.5.9-4.el6
rh-postgresql95-postgresql-pltcl-9.5.9-4.el6
rh-postgresql95-postgresql-test-9.5.9-4.el6

RHEL6_7S
x86_64
rh-postgresql95-postgresql-plperl-9.5.9-4.el6
rh-postgresql95-postgresql-static-9.5.9-4.el6
rh-postgresql95-postgresql-devel-9.5.9-4.el6
rh-postgresql95-postgresql-contrib-9.5.9-4.el6
rh-postgresql95-postgresql-plpython-9.5.9-4.el6
rh-postgresql95-postgresql-debuginfo-9.5.9-4.el6
rh-postgresql95-postgresql-docs-9.5.9-4.el6
rh-postgresql95-postgresql-9.5.9-4.el6
rh-postgresql95-postgresql-libs-9.5.9-4.el6
rh-postgresql95-postgresql-server-9.5.9-4.el6
rh-postgresql95-postgresql-pltcl-9.5.9-4.el6
rh-postgresql95-postgresql-test-9.5.9-4.el6

RHEL7_3S
x86_64
rh-postgresql95-postgresql-contrib-9.5.9-4.el7
rh-postgresql95-postgresql-plperl-9.5.9-4.el7
rh-postgresql95-postgresql-plpython-9.5.9-4.el7

rh-postgresql95-postgresql-pltcl-9.5.9-4.el7
rh-postgresql95-postgresql-devel-9.5.9-4.el7
rh-postgresql95-postgresql-docs-9.5.9-4.el7
rh-postgresql95-postgresql-libs-9.5.9-4.el7
rh-postgresql95-postgresql-test-9.5.9-4.el7
rh-postgresql95-postgresql-debuginfo-9.5.9-4.el7
rh-postgresql95-postgresql-static-9.5.9-4.el7
rh-postgresql95-postgresql-9.5.9-4.el7
rh-postgresql95-postgresql-server-9.5.9-4.el7

RHEL7WS
x86_64
rh-postgresql95-postgresql-contrib-9.5.9-4.el7
rh-postgresql95-postgresql-plperl-9.5.9-4.el7
rh-postgresql95-postgresql-plpython-9.5.9-4.el7
rh-postgresql95-postgresql-pltcl-9.5.9-4.el7
rh-postgresql95-postgresql-devel-9.5.9-4.el7
rh-postgresql95-postgresql-docs-9.5.9-4.el7
rh-postgresql95-postgresql-libs-9.5.9-4.el7
rh-postgresql95-postgresql-test-9.5.9-4.el7
rh-postgresql95-postgresql-debuginfo-9.5.9-4.el7
rh-postgresql95-postgresql-static-9.5.9-4.el7
rh-postgresql95-postgresql-9.5.9-4.el7
rh-postgresql95-postgresql-server-9.5.9-4.el7

141803 - Red Hat Enterprise Linux RHSA-2017-3403 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15097

Description

The scan detected that the host is missing the following update:
RHSA-2017-3403

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00012.html

RHEL7S
x86_64
rh-postgresql94-postgresql-docs-9.4.14-2.el7
rh-postgresql94-postgresql-plpython-9.4.14-2.el7
rh-postgresql94-postgresql-devel-9.4.14-2.el7
rh-postgresql94-postgresql-libs-9.4.14-2.el7
rh-postgresql94-postgresql-pltcl-9.4.14-2.el7
rh-postgresql94-postgresql-static-9.4.14-2.el7
rh-postgresql94-postgresql-contrib-9.4.14-2.el7
rh-postgresql94-postgresql-9.4.14-2.el7
rh-postgresql94-postgresql-test-9.4.14-2.el7
rh-postgresql94-postgresql-debuginfo-9.4.14-2.el7
rh-postgresql94-postgresql-upgrade-9.4.14-2.el7
rh-postgresql94-postgresql-server-9.4.14-2.el7
rh-postgresql94-postgresql-plperl-9.4.14-2.el7

RHEL6S

x86_64
rh-postgresql94-postgresql-docs-9.4.14-2.el6
rh-postgresql94-postgresql-plpython-9.4.14-2.el6
rh-postgresql94-postgresql-libs-9.4.14-2.el6
rh-postgresql94-postgresql-contrib-9.4.14-2.el6
rh-postgresql94-postgresql-static-9.4.14-2.el6
rh-postgresql94-postgresql-plperl-9.4.14-2.el6
rh-postgresql94-postgresql-pltcl-9.4.14-2.el6
rh-postgresql94-postgresql-debuginfo-9.4.14-2.el6
rh-postgresql94-postgresql-server-9.4.14-2.el6
rh-postgresql94-postgresql-upgrade-9.4.14-2.el6
rh-postgresql94-postgresql-devel-9.4.14-2.el6
rh-postgresql94-postgresql-test-9.4.14-2.el6
rh-postgresql94-postgresql-9.4.14-2.el6

RHEL6WS
x86_64
rh-postgresql94-postgresql-docs-9.4.14-2.el6
rh-postgresql94-postgresql-plpython-9.4.14-2.el6
rh-postgresql94-postgresql-libs-9.4.14-2.el6
rh-postgresql94-postgresql-contrib-9.4.14-2.el6
rh-postgresql94-postgresql-static-9.4.14-2.el6
rh-postgresql94-postgresql-plperl-9.4.14-2.el6
rh-postgresql94-postgresql-pltcl-9.4.14-2.el6
rh-postgresql94-postgresql-debuginfo-9.4.14-2.el6
rh-postgresql94-postgresql-server-9.4.14-2.el6
rh-postgresql94-postgresql-upgrade-9.4.14-2.el6
rh-postgresql94-postgresql-devel-9.4.14-2.el6
rh-postgresql94-postgresql-test-9.4.14-2.el6
rh-postgresql94-postgresql-9.4.14-2.el6

RHEL6_7S
x86_64
rh-postgresql94-postgresql-docs-9.4.14-2.el6
rh-postgresql94-postgresql-plpython-9.4.14-2.el6
rh-postgresql94-postgresql-libs-9.4.14-2.el6
rh-postgresql94-postgresql-contrib-9.4.14-2.el6
rh-postgresql94-postgresql-static-9.4.14-2.el6
rh-postgresql94-postgresql-plperl-9.4.14-2.el6
rh-postgresql94-postgresql-pltcl-9.4.14-2.el6
rh-postgresql94-postgresql-debuginfo-9.4.14-2.el6
rh-postgresql94-postgresql-server-9.4.14-2.el6
rh-postgresql94-postgresql-upgrade-9.4.14-2.el6
rh-postgresql94-postgresql-devel-9.4.14-2.el6
rh-postgresql94-postgresql-test-9.4.14-2.el6
rh-postgresql94-postgresql-9.4.14-2.el6

RHEL7_3S
x86_64
rh-postgresql94-postgresql-docs-9.4.14-2.el7
rh-postgresql94-postgresql-plpython-9.4.14-2.el7
rh-postgresql94-postgresql-devel-9.4.14-2.el7
rh-postgresql94-postgresql-libs-9.4.14-2.el7
rh-postgresql94-postgresql-pltcl-9.4.14-2.el7
rh-postgresql94-postgresql-static-9.4.14-2.el7
rh-postgresql94-postgresql-contrib-9.4.14-2.el7
rh-postgresql94-postgresql-9.4.14-2.el7
rh-postgresql94-postgresql-test-9.4.14-2.el7
rh-postgresql94-postgresql-debuginfo-9.4.14-2.el7
rh-postgresql94-postgresql-upgrade-9.4.14-2.el7

rh-postgresql94-postgresql-server-9.4.14-2.el7
rh-postgresql94-postgresql-plperl-9.4.14-2.el7

RHEL7WS
x86_64
rh-postgresql94-postgresql-docs-9.4.14-2.el7
rh-postgresql94-postgresql-plpython-9.4.14-2.el7
rh-postgresql94-postgresql-devel-9.4.14-2.el7
rh-postgresql94-postgresql-libs-9.4.14-2.el7
rh-postgresql94-postgresql-pltcl-9.4.14-2.el7
rh-postgresql94-postgresql-static-9.4.14-2.el7
rh-postgresql94-postgresql-contrib-9.4.14-2.el7
rh-postgresql94-postgresql-9.4.14-2.el7
rh-postgresql94-postgresql-test-9.4.14-2.el7
rh-postgresql94-postgresql-debuginfo-9.4.14-2.el7
rh-postgresql94-postgresql-upgrade-9.4.14-2.el7
rh-postgresql94-postgresql-server-9.4.14-2.el7
rh-postgresql94-postgresql-plperl-9.4.14-2.el7

141805 - Red Hat Enterprise Linux RHSA-2017-3402 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15097

Description

The scan detected that the host is missing the following update:
RHSA-2017-3402

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00011.html

RHEL7D
x86_64
postgresql-test-9.2.23-3.el7_4
postgresql-docs-9.2.23-3.el7_4
postgresql-upgrade-9.2.23-3.el7_4
postgresql-plpython-9.2.23-3.el7_4
postgresql-libs-9.2.23-3.el7_4
postgresql-static-9.2.23-3.el7_4
postgresql-9.2.23-3.el7_4
postgresql-contrib-9.2.23-3.el7_4
postgresql-devel-9.2.23-3.el7_4
postgresql-plperl-9.2.23-3.el7_4
postgresql-server-9.2.23-3.el7_4
postgresql-pltcl-9.2.23-3.el7_4
postgresql-debuginfo-9.2.23-3.el7_4

RHEL7S
x86_64
postgresql-test-9.2.23-3.el7_4
postgresql-docs-9.2.23-3.el7_4
postgresql-upgrade-9.2.23-3.el7_4
postgresql-plpython-9.2.23-3.el7_4
postgresql-libs-9.2.23-3.el7_4

postgresql-static-9.2.23-3.el7_4
postgresql-9.2.23-3.el7_4
postgresql-contrib-9.2.23-3.el7_4
postgresql-devel-9.2.23-3.el7_4
postgresql-plperl-9.2.23-3.el7_4
postgresql-server-9.2.23-3.el7_4
postgresql-pltcl-9.2.23-3.el7_4
postgresql-debuginfo-9.2.23-3.el7_4

RHEL7WS
x86_64
postgresql-test-9.2.23-3.el7_4
postgresql-docs-9.2.23-3.el7_4
postgresql-upgrade-9.2.23-3.el7_4
postgresql-plpython-9.2.23-3.el7_4
postgresql-libs-9.2.23-3.el7_4
postgresql-static-9.2.23-3.el7_4
postgresql-9.2.23-3.el7_4
postgresql-contrib-9.2.23-3.el7_4
postgresql-devel-9.2.23-3.el7_4
postgresql-plperl-9.2.23-3.el7_4
postgresql-server-9.2.23-3.el7_4
postgresql-pltcl-9.2.23-3.el7_4
postgresql-debuginfo-9.2.23-3.el7_4

146138 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3270-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10799, CVE-2017-12140, CVE-2017-12644, CVE-2017-12662, CVE-2017-14733, CVE-2017-14994

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3270-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00045.html

SuSE Linux 42.2
x86_64
libGraphicsMagick3-config-1.3.25-11.48.1
libGraphicsMagick++-Q16-12-1.3.25-11.48.1
GraphicsMagick-debugsource-1.3.25-11.48.1
GraphicsMagick-debuginfo-1.3.25-11.48.1
libGraphicsMagick++-devel-1.3.25-11.48.1
libGraphicsMagickWand-Q16-2-1.3.25-11.48.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.48.1
perl-GraphicsMagick-1.3.25-11.48.1
GraphicsMagick-devel-1.3.25-11.48.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.48.1
perl-GraphicsMagick-debuginfo-1.3.25-11.48.1
GraphicsMagick-1.3.25-11.48.1
libGraphicsMagick-Q16-3-1.3.25-11.48.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.48.1

i586
libGraphicsMagick3-config-1.3.25-11.48.1
libGraphicsMagick++-Q16-12-1.3.25-11.48.1
GraphicsMagick-debugsource-1.3.25-11.48.1
GraphicsMagick-debuginfo-1.3.25-11.48.1
libGraphicsMagick++-devel-1.3.25-11.48.1
libGraphicsMagickWand-Q16-2-1.3.25-11.48.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.48.1
perl-GraphicsMagick-1.3.25-11.48.1
GraphicsMagick-devel-1.3.25-11.48.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.48.1
perl-GraphicsMagick-debuginfo-1.3.25-11.48.1
GraphicsMagick-1.3.25-11.48.1
libGraphicsMagick-Q16-3-1.3.25-11.48.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.48.1

SuSE Linux 42.3
x86_64
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-47.1
perl-GraphicsMagick-debuginfo-1.3.25-47.1
libGraphicsMagick3-config-1.3.25-47.1
GraphicsMagick-debugsource-1.3.25-47.1
libGraphicsMagick-Q16-3-1.3.25-47.1
GraphicsMagick-devel-1.3.25-47.1
libGraphicsMagick++-devel-1.3.25-47.1
libGraphicsMagick++-Q16-12-1.3.25-47.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-47.1
GraphicsMagick-1.3.25-47.1
GraphicsMagick-debuginfo-1.3.25-47.1
libGraphicsMagickWand-Q16-2-1.3.25-47.1
perl-GraphicsMagick-1.3.25-47.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-47.1

i586
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-47.1
perl-GraphicsMagick-debuginfo-1.3.25-47.1
libGraphicsMagick3-config-1.3.25-47.1
GraphicsMagick-debugsource-1.3.25-47.1
libGraphicsMagick-Q16-3-1.3.25-47.1
GraphicsMagick-devel-1.3.25-47.1
libGraphicsMagick++-devel-1.3.25-47.1
libGraphicsMagick++-Q16-12-1.3.25-47.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-47.1
GraphicsMagick-1.3.25-47.1
GraphicsMagick-debuginfo-1.3.25-47.1
libGraphicsMagickWand-Q16-2-1.3.25-47.1
perl-GraphicsMagick-1.3.25-47.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-47.1

146146 - SuSE SLES 11 SP4 SUSE-SU-2017:3233-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3233-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003479.html

SuSE SLES 11 SP4
i586
MozillaFirefox-52.5.0esr-72.17.1
MozillaFirefox-translations-52.5.0esr-72.17.1

x86_64
MozillaFirefox-52.5.0esr-72.17.1
MozillaFirefox-translations-52.5.0esr-72.17.1

146149 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3244-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3244-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00033.html

SuSE Linux 42.2
x86_64
chromium-debugsource-63.0.3239.84-104.41.1
chromium-63.0.3239.84-104.41.1
chromedriver-debuginfo-63.0.3239.84-104.41.1
chromedriver-63.0.3239.84-104.41.1
chromium-debuginfo-63.0.3239.84-104.41.1

SuSE Linux 42.3
x86_64
chromedriver-63.0.3239.84-127.1
chromium-debugsource-63.0.3239.84-127.1
chromium-63.0.3239.84-127.1
chromedriver-debuginfo-63.0.3239.84-127.1
chromium-debuginfo-63.0.3239.84-127.1

146150 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3268-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17439

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3268-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00043.html

SuSE Linux 42.2
x86_64
libheimdal-debugsource-7.4.0-2.6.1
libheimdal-devel-7.4.0-2.6.1
libheimdal-7.4.0-2.6.1
libheimdal-debuginfo-7.4.0-2.6.1

i586
libheimdal-debugsource-7.4.0-2.6.1
libheimdal-devel-7.4.0-2.6.1
libheimdal-7.4.0-2.6.1
libheimdal-debuginfo-7.4.0-2.6.1

SuSE Linux 42.3
x86_64
libheimdal-devel-7.4.0-6.1
libheimdal-debugsource-7.4.0-6.1
libheimdal-7.4.0-6.1
libheimdal-debuginfo-7.4.0-6.1

i586
libheimdal-devel-7.4.0-6.1
libheimdal-debugsource-7.4.0-6.1
libheimdal-7.4.0-6.1
libheimdal-debuginfo-7.4.0-6.1

146153 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:3225-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3225-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003474.html

SuSE SLED 12 SP3
x86_64
kernel-default-debuginfo-4.4.92-6.30.1
kernel-default-extra-debuginfo-4.4.92-6.30.1
kernel-syms-4.4.92-6.30.1

kernel-default-debugsource-4.4.92-6.30.1
kernel-default-4.4.92-6.30.1
kernel-default-extra-4.4.92-6.30.1
kernel-default-devel-4.4.92-6.30.1

noarch
kernel-source-4.4.92-6.30.1
kernel-macros-4.4.92-6.30.1
kernel-devel-4.4.92-6.30.1

SuSE SLES 12 SP3
noarch
kernel-source-4.4.92-6.30.1
kernel-macros-4.4.92-6.30.1
kernel-devel-4.4.92-6.30.1

x86_64
kernel-default-debuginfo-4.4.92-6.30.1
kernel-syms-4.4.92-6.30.1
kernel-default-debugsource-4.4.92-6.30.1
kernel-default-base-4.4.92-6.30.1
kernel-default-base-debuginfo-4.4.92-6.30.1
kernel-default-4.4.92-6.30.1
kernel-default-devel-4.4.92-6.30.1

146154 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:3226-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3226-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003475.html

SuSE SLED 12 SP2
x86_64
kernel-default-4.4.90-92.50.1
kernel-default-devel-4.4.90-92.50.1
kernel-default-debuginfo-4.4.90-92.50.1
kernel-default-extra-4.4.90-92.50.1
kernel-default-extra-debuginfo-4.4.90-92.50.1
kernel-default-debugsource-4.4.90-92.50.1
kernel-syms-4.4.90-92.50.1

noarch
kernel-devel-4.4.90-92.50.1
kernel-source-4.4.90-92.50.1
kernel-macros-4.4.90-92.50.1

SuSE SLES 12 SP2
noarch

kernel-devel-4.4.90-92.50.1
kernel-source-4.4.90-92.50.1
kernel-macros-4.4.90-92.50.1

x86_64
kernel-default-4.4.90-92.50.1
kernel-default-devel-4.4.90-92.50.1
kernel-default-debuginfo-4.4.90-92.50.1
kernel-default-base-4.4.90-92.50.1
kernel-default-debugsource-4.4.90-92.50.1
kernel-default-base-debuginfo-4.4.90-92.50.1
kernel-syms-4.4.90-92.50.1

146156 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3240-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16642, CVE-2017-9228, CVE-2017-9229

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3240-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00030.html

SuSE Linux 42.2
i586
apache2-mod_php7-debuginfo-7.0.7-14.15.1
php7-pspell-7.0.7-14.15.1
php7-bcmath-7.0.7-14.15.1
php7-pcntl-debuginfo-7.0.7-14.15.1
php7-exif-debuginfo-7.0.7-14.15.1
php7-mbstring-7.0.7-14.15.1
php7-ctype-7.0.7-14.15.1
php7-xmlreader-debuginfo-7.0.7-14.15.1
php7-opcache-debuginfo-7.0.7-14.15.1
php7-xsl-7.0.7-14.15.1
php7-fastcgi-7.0.7-14.15.1
php7-gettext-7.0.7-14.15.1
php7-json-7.0.7-14.15.1
php7-sysvmsg-7.0.7-14.15.1
php7-fileinfo-debuginfo-7.0.7-14.15.1
php7-pgsql-debuginfo-7.0.7-14.15.1
php7-sqlite-7.0.7-14.15.1
php7-sysvshm-debuginfo-7.0.7-14.15.1
php7-zip-debuginfo-7.0.7-14.15.1
php7-dba-debuginfo-7.0.7-14.15.1
php7-pdo-7.0.7-14.15.1
php7-pgsql-7.0.7-14.15.1
php7-phar-debuginfo-7.0.7-14.15.1
php7-dba-7.0.7-14.15.1
php7-pdo-debuginfo-7.0.7-14.15.1
php7-shmop-debuginfo-7.0.7-14.15.1
php7-openssl-debuginfo-7.0.7-14.15.1

php7-tokenizer-7.0.7-14.15.1
php7-curl-7.0.7-14.15.1
php7-phar-7.0.7-14.15.1
php7-fpm-7.0.7-14.15.1
php7-odbc-debuginfo-7.0.7-14.15.1
php7-snmp-debuginfo-7.0.7-14.15.1
php7-tidy-7.0.7-14.15.1
php7-xmlrpc-7.0.7-14.15.1
php7-opcache-7.0.7-14.15.1
php7-firebird-debuginfo-7.0.7-14.15.1
php7-sysvsem-debuginfo-7.0.7-14.15.1
php7-zip-7.0.7-14.15.1
php7-7.0.7-14.15.1
php7-posix-7.0.7-14.15.1
php7-mysql-7.0.7-14.15.1
php7-zlib-debuginfo-7.0.7-14.15.1
php7-imap-debuginfo-7.0.7-14.15.1
php7-tidy-debuginfo-7.0.7-14.15.1
php7-debuginfo-7.0.7-14.15.1
php7-sqlite-debuginfo-7.0.7-14.15.1
php7-ftp-debuginfo-7.0.7-14.15.1
php7-dom-debuginfo-7.0.7-14.15.1
php7-sysvsem-7.0.7-14.15.1
php7-exif-7.0.7-14.15.1
php7-odbc-7.0.7-14.15.1
php7-ldap-7.0.7-14.15.1
php7-wddx-7.0.7-14.15.1
php7-ldap-debuginfo-7.0.7-14.15.1
php7-dom-7.0.7-14.15.1
php7-gmp-debuginfo-7.0.7-14.15.1
php7-tokenizer-debuginfo-7.0.7-14.15.1
php7-gd-7.0.7-14.15.1
php7-mcrypt-debuginfo-7.0.7-14.15.1
apache2-mod_php7-7.0.7-14.15.1
php7-curl-debuginfo-7.0.7-14.15.1
php7-snmp-7.0.7-14.15.1
php7-json-debuginfo-7.0.7-14.15.1
php7-enchant-7.0.7-14.15.1
php7-bcmath-debuginfo-7.0.7-14.15.1
php7-iconv-7.0.7-14.15.1
php7-fastcgi-debuginfo-7.0.7-14.15.1
php7-posix-debuginfo-7.0.7-14.15.1
php7-xmlreader-7.0.7-14.15.1
php7-firebird-7.0.7-14.15.1
php7-pcntl-7.0.7-14.15.1
php7-intl-debuginfo-7.0.7-14.15.1
php7-intl-7.0.7-14.15.1
php7-sockets-7.0.7-14.15.1
php7-mbstring-debuginfo-7.0.7-14.15.1
php7-ftp-7.0.7-14.15.1
php7-pspell-debuginfo-7.0.7-14.15.1
php7-xmlwriter-7.0.7-14.15.1
php7-iconv-debuginfo-7.0.7-14.15.1
php7-shmop-7.0.7-14.15.1
php7-mysql-debuginfo-7.0.7-14.15.1
php7-readline-7.0.7-14.15.1
php7-zlib-7.0.7-14.15.1
php7-fileinfo-7.0.7-14.15.1
php7-readline-debuginfo-7.0.7-14.15.1
php7-soap-7.0.7-14.15.1

php7-gettext-debuginfo-7.0.7-14.15.1
php7-soap-debuginfo-7.0.7-14.15.1
php7-sockets-debuginfo-7.0.7-14.15.1
php7-ctype-debuginfo-7.0.7-14.15.1
php7-imap-7.0.7-14.15.1
php7-gmp-7.0.7-14.15.1
php7-sysvmsg-debuginfo-7.0.7-14.15.1
php7-debugsource-7.0.7-14.15.1
php7-fpm-debuginfo-7.0.7-14.15.1
php7-calendar-debuginfo-7.0.7-14.15.1
php7-gd-debuginfo-7.0.7-14.15.1
php7-calendar-7.0.7-14.15.1
php7-xsl-debuginfo-7.0.7-14.15.1
php7-xmlwriter-debuginfo-7.0.7-14.15.1
php7-enchant-debuginfo-7.0.7-14.15.1
php7-devel-7.0.7-14.15.1
php7-wddx-debuginfo-7.0.7-14.15.1
php7-openssl-7.0.7-14.15.1
php7-mcrypt-7.0.7-14.15.1
php7-sysvshm-7.0.7-14.15.1
php7-bz2-7.0.7-14.15.1
php7-bz2-debuginfo-7.0.7-14.15.1
php7-xmlrpc-debuginfo-7.0.7-14.15.1

noarch
php7-pear-7.0.7-14.15.1
php7-pear-Archive_Tar-7.0.7-14.15.1

x86_64
apache2-mod_php7-debuginfo-7.0.7-14.15.1
php7-pspell-7.0.7-14.15.1
php7-bcmath-7.0.7-14.15.1
php7-pcntl-debuginfo-7.0.7-14.15.1
php7-exif-debuginfo-7.0.7-14.15.1
php7-mbstring-7.0.7-14.15.1
php7-ctype-7.0.7-14.15.1
php7-xmlreader-debuginfo-7.0.7-14.15.1
php7-opcache-debuginfo-7.0.7-14.15.1
php7-xsl-7.0.7-14.15.1
php7-fastcgi-7.0.7-14.15.1
php7-gettext-7.0.7-14.15.1
php7-json-7.0.7-14.15.1
php7-sysvmsg-7.0.7-14.15.1
php7-fileinfo-debuginfo-7.0.7-14.15.1
php7-pgsql-debuginfo-7.0.7-14.15.1
php7-sqlite-7.0.7-14.15.1
php7-sysvshm-debuginfo-7.0.7-14.15.1
php7-zip-debuginfo-7.0.7-14.15.1
php7-dba-debuginfo-7.0.7-14.15.1
php7-pdo-7.0.7-14.15.1
php7-pgsql-7.0.7-14.15.1
php7-phar-debuginfo-7.0.7-14.15.1
php7-dba-7.0.7-14.15.1
php7-pdo-debuginfo-7.0.7-14.15.1
php7-shmop-debuginfo-7.0.7-14.15.1
php7-openssl-debuginfo-7.0.7-14.15.1
php7-tokenizer-7.0.7-14.15.1
php7-curl-7.0.7-14.15.1
php7-phar-7.0.7-14.15.1
php7-fpm-7.0.7-14.15.1

php7-odbc-debuginfo-7.0.7-14.15.1
php7-snmp-debuginfo-7.0.7-14.15.1
php7-tidy-7.0.7-14.15.1
php7-xmlrpc-7.0.7-14.15.1
php7-opcache-7.0.7-14.15.1
php7-firebird-debuginfo-7.0.7-14.15.1
php7-sysvsem-debuginfo-7.0.7-14.15.1
php7-zip-7.0.7-14.15.1
php7-7.0.7-14.15.1
php7-posix-7.0.7-14.15.1
php7-mysql-7.0.7-14.15.1
php7-zlib-debuginfo-7.0.7-14.15.1
php7-imap-debuginfo-7.0.7-14.15.1
php7-tidy-debuginfo-7.0.7-14.15.1
php7-debuginfo-7.0.7-14.15.1
php7-sqlite-debuginfo-7.0.7-14.15.1
php7-ftp-debuginfo-7.0.7-14.15.1
php7-dom-debuginfo-7.0.7-14.15.1
php7-sysvsem-7.0.7-14.15.1
php7-exif-7.0.7-14.15.1
php7-odbc-7.0.7-14.15.1
php7-ldap-7.0.7-14.15.1
php7-wddx-7.0.7-14.15.1
php7-ldap-debuginfo-7.0.7-14.15.1
php7-dom-7.0.7-14.15.1
php7-gmp-debuginfo-7.0.7-14.15.1
php7-tokenizer-debuginfo-7.0.7-14.15.1
php7-gd-7.0.7-14.15.1
php7-mcrypt-debuginfo-7.0.7-14.15.1
apache2-mod_php7-7.0.7-14.15.1
php7-curl-debuginfo-7.0.7-14.15.1
php7-snmp-7.0.7-14.15.1
php7-json-debuginfo-7.0.7-14.15.1
php7-enchant-7.0.7-14.15.1
php7-bcmath-debuginfo-7.0.7-14.15.1
php7-iconv-7.0.7-14.15.1
php7-fastcgi-debuginfo-7.0.7-14.15.1
php7-posix-debuginfo-7.0.7-14.15.1
php7-xmlreader-7.0.7-14.15.1
php7-firebird-7.0.7-14.15.1
php7-pcntl-7.0.7-14.15.1
php7-intl-debuginfo-7.0.7-14.15.1
php7-intl-7.0.7-14.15.1
php7-sockets-7.0.7-14.15.1
php7-mbstring-debuginfo-7.0.7-14.15.1
php7-ftp-7.0.7-14.15.1
php7-pspell-debuginfo-7.0.7-14.15.1
php7-xmlwriter-7.0.7-14.15.1
php7-iconv-debuginfo-7.0.7-14.15.1
php7-shmop-7.0.7-14.15.1
php7-mysql-debuginfo-7.0.7-14.15.1
php7-readline-7.0.7-14.15.1
php7-zlib-7.0.7-14.15.1
php7-fileinfo-7.0.7-14.15.1
php7-readline-debuginfo-7.0.7-14.15.1
php7-soap-7.0.7-14.15.1
php7-gettext-debuginfo-7.0.7-14.15.1
php7-soap-debuginfo-7.0.7-14.15.1
php7-sockets-debuginfo-7.0.7-14.15.1
php7-ctype-debuginfo-7.0.7-14.15.1

php7-imap-7.0.7-14.15.1
php7-gmp-7.0.7-14.15.1
php7-sysvmsg-debuginfo-7.0.7-14.15.1
php7-debugsource-7.0.7-14.15.1
php7-fpm-debuginfo-7.0.7-14.15.1
php7-calendar-debuginfo-7.0.7-14.15.1
php7-gd-debuginfo-7.0.7-14.15.1
php7-calendar-7.0.7-14.15.1
php7-xsl-debuginfo-7.0.7-14.15.1
php7-xmlwriter-debuginfo-7.0.7-14.15.1
php7-enchant-debuginfo-7.0.7-14.15.1
php7-devel-7.0.7-14.15.1
php7-wddx-debuginfo-7.0.7-14.15.1
php7-openssl-7.0.7-14.15.1
php7-mcrypt-7.0.7-14.15.1
php7-sysvshm-7.0.7-14.15.1
php7-bz2-7.0.7-14.15.1
php7-bz2-debuginfo-7.0.7-14.15.1
php7-xmlrpc-debuginfo-7.0.7-14.15.1

SuSE Linux 42.3
i586
php7-dba-7.0.7-25.1

146157 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3257-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10253, CVE-2017-1000385

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3257-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00038.html

SuSE Linux 42.2
x86_64
erlang-jinterface-18.3.4.7-2.7.1
erlang-reltool-18.3.4.7-2.7.1
erlang-wx-src-18.3.4.7-2.7.1
erlang-debuginfo-18.3.4.7-2.7.1
erlang-wx-18.3.4.7-2.7.1
erlang-diameter-18.3.4.7-2.7.1
erlang-dialyzer-src-18.3.4.7-2.7.1
erlang-gs-18.3.4.7-2.7.1
erlang-epmd-18.3.4.7-2.7.1
erlang-doc-18.3.4.7-2.7.1
erlang-dialyzer-debuginfo-18.3.4.7-2.7.1
erlang-et-src-18.3.4.7-2.7.1
erlang-src-18.3.4.7-2.7.1
erlang-18.3.4.7-2.7.1
erlang-observer-18.3.4.7-2.7.1
erlang-diameter-src-18.3.4.7-2.7.1

erlang-epmd-debuginfo-18.3.4.7-2.7.1
erlang-observer-src-18.3.4.7-2.7.1
erlang-debugsource-18.3.4.7-2.7.1
erlang-dialyzer-18.3.4.7-2.7.1
erlang-debugger-src-18.3.4.7-2.7.1
erlang-reltool-src-18.3.4.7-2.7.1
erlang-et-18.3.4.7-2.7.1
erlang-wx-debuginfo-18.3.4.7-2.7.1
erlang-gs-src-18.3.4.7-2.7.1
erlang-debugger-18.3.4.7-2.7.1
erlang-jinterface-src-18.3.4.7-2.7.1

i586
erlang-jinterface-18.3.4.7-2.7.1
erlang-reltool-18.3.4.7-2.7.1
erlang-wx-src-18.3.4.7-2.7.1
erlang-debuginfo-18.3.4.7-2.7.1
erlang-wx-18.3.4.7-2.7.1
erlang-diameter-18.3.4.7-2.7.1
erlang-dialyzer-src-18.3.4.7-2.7.1
erlang-gs-18.3.4.7-2.7.1
erlang-epmd-18.3.4.7-2.7.1
erlang-doc-18.3.4.7-2.7.1
erlang-dialyzer-debuginfo-18.3.4.7-2.7.1
erlang-et-src-18.3.4.7-2.7.1
erlang-src-18.3.4.7-2.7.1
erlang-18.3.4.7-2.7.1
erlang-observer-18.3.4.7-2.7.1
erlang-diameter-src-18.3.4.7-2.7.1
erlang-epmd-debuginfo-18.3.4.7-2.7.1
erlang-observer-src-18.3.4.7-2.7.1
erlang-debugsource-18.3.4.7-2.7.1
erlang-dialyzer-18.3.4.7-2.7.1
erlang-debugger-src-18.3.4.7-2.7.1
erlang-reltool-src-18.3.4.7-2.7.1
erlang-et-18.3.4.7-2.7.1
erlang-wx-debuginfo-18.3.4.7-2.7.1
erlang-gs-src-18.3.4.7-2.7.1
erlang-debugger-18.3.4.7-2.7.1
erlang-jinterface-src-18.3.4.7-2.7.1

SuSE Linux 42.3
x86_64
erlang-epmd-18.3.4.7-6.1
erlang-18.3.4.7-6.1
erlang-diameter-18.3.4.7-6.1
erlang-et-18.3.4.7-6.1
erlang-wx-src-18.3.4.7-6.1
erlang-reltool-18.3.4.7-6.1
erlang-observer-src-18.3.4.7-6.1
erlang-et-src-18.3.4.7-6.1
erlang-debugsource-18.3.4.7-6.1
erlang-src-18.3.4.7-6.1
erlang-jinterface-18.3.4.7-6.1
erlang-gs-18.3.4.7-6.1
erlang-doc-18.3.4.7-6.1
erlang-jinterface-src-18.3.4.7-6.1
erlang-gs-src-18.3.4.7-6.1
erlang-observer-18.3.4.7-6.1
erlang-epmd-debuginfo-18.3.4.7-6.1

erlang-debuginfo-18.3.4.7-6.1
erlang-dialyzer-debuginfo-18.3.4.7-6.1
erlang-debugger-18.3.4.7-6.1
erlang-diameter-src-18.3.4.7-6.1
erlang-wx-debuginfo-18.3.4.7-6.1
erlang-dialyzer-18.3.4.7-6.1
erlang-dialyzer-src-18.3.4.7-6.1
erlang-wx-18.3.4.7-6.1
erlang-reltool-src-18.3.4.7-6.1
erlang-debugger-src-18.3.4.7-6.1

146158 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3271-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17459

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3271-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00046.html

SuSE Linux 42.2
x86_64
fossil-debuginfo-2.4-5.6.1
fossil-debugsource-2.4-5.6.1
fossil-2.4-5.6.1

i586
fossil-debuginfo-2.4-5.6.1
fossil-debugsource-2.4-5.6.1
fossil-2.4-5.6.1

SuSE Linux 42.3
x86_64
fossil-debuginfo-2.4-6.1
fossil-debugsource-2.4-6.1
fossil-2.4-6.1

i586
fossil-debuginfo-2.4-6.1
fossil-debugsource-2.4-6.1
fossil-2.4-6.1

146159 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3272-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7843

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3272-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00047.html

SuSE Linux 42.2
x86_64
MozillaFirefox-debugsource-52.5.2-57.24.1
MozillaFirefox-buildsymbols-52.5.2-57.24.1
MozillaFirefox-52.5.2-57.24.1
MozillaFirefox-debuginfo-52.5.2-57.24.1
MozillaFirefox-devel-52.5.2-57.24.1
MozillaFirefox-translations-other-52.5.2-57.24.1
MozillaFirefox-translations-common-52.5.2-57.24.1
MozillaFirefox-branding-upstream-52.5.2-57.24.1

SuSE Linux 42.3
x86_64
MozillaFirefox-devel-52.5.2-69.1
MozillaFirefox-branding-upstream-52.5.2-69.1
MozillaFirefox-buildsymbols-52.5.2-69.1
MozillaFirefox-translations-other-52.5.2-69.1
MozillaFirefox-translations-common-52.5.2-69.1
MozillaFirefox-debugsource-52.5.2-69.1
MozillaFirefox-52.5.2-69.1
MozillaFirefox-debuginfo-52.5.2-69.1

160330 - CentOS 7 CESA-2017-3402 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15097

Description

The scan detected that the host is missing the following update:
CESA-2017-3402

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-December/022690.html

CentOS 7
x86_64
postgresql-docs-9.2.23-3.el7_4
postgresql-static-9.2.23-3.el7_4
postgresql-upgrade-9.2.23-3.el7_4
postgresql-9.2.23-3.el7_4
postgresql-plpython-9.2.23-3.el7_4
postgresql-plperl-9.2.23-3.el7_4
postgresql-test-9.2.23-3.el7_4
postgresql-devel-9.2.23-3.el7_4

postgresql-libs-9.2.23-3.el7_4
postgresql-server-9.2.23-3.el7_4
postgresql-pltcl-9.2.23-3.el7_4
postgresql-contrib-9.2.23-3.el7_4

i686
postgresql-static-9.2.23-3.el7_4
postgresql-devel-9.2.23-3.el7_4
postgresql-libs-9.2.23-3.el7_4
postgresql-9.2.23-3.el7_4

160331 - CentOS 7 CESA-2017-3368 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14167, CVE-2017-15289

Description

The scan detected that the host is missing the following update:
CESA-2017-3368

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-December/022679.html

CentOS 7
x86_64
qemu-img-1.5.3-141.el7_4.4
qemu-kvm-tools-1.5.3-141.el7_4.4
qemu-kvm-1.5.3-141.el7_4.4
qemu-kvm-common-1.5.3-141.el7_4.4

160335 - CentOS 6, 7 CESA-2017-3372 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
CESA-2017-3372

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-December/022681.html
http://lists.centos.org/pipermail/centos-announce/2017-December/022686.html

CentOS 7
x86_64
thunderbird-52.5.0-1.el7.centos

CentOS 6

x86_64
thunderbird-52.5.0-1.el6.centos

i686
thunderbird-52.5.0-1.el6.centos

160337 - CentOS 6, 7 CESA-2017-3382 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7843

Description

The scan detected that the host is missing the following update:
CESA-2017-3382

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-December/022687.html
http://lists.centos.org/pipermail/centos-announce/2017-December/022683.html

CentOS 7
x86_64
firefox-52.5.1-1.el7.centos

i686
firefox-52.5.1-1.el7.centos

CentOS 6
x86_64
firefox-52.5.1-1.el6.centos

i686
firefox-52.5.1-1.el6.centos

163510 - Oracle Enterprise Linux ELSA-2017-3402 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15097

Description

The scan detected that the host is missing the following update:
ELSA-2017-3402

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-December/007404.html

OEL7
x86_64
postgresql-docs-9.2.23-3.el7_4

postgresql-static-9.2.23-3.el7_4
postgresql-upgrade-9.2.23-3.el7_4
postgresql-9.2.23-3.el7_4
postgresql-plpython-9.2.23-3.el7_4
postgresql-plperl-9.2.23-3.el7_4
postgresql-test-9.2.23-3.el7_4
postgresql-devel-9.2.23-3.el7_4
postgresql-libs-9.2.23-3.el7_4
postgresql-server-9.2.23-3.el7_4
postgresql-pltcl-9.2.23-3.el7_4
postgresql-contrib-9.2.23-3.el7_4

163511 - Oracle Enterprise Linux ELSA-2017-3651 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9191, CVE-2017-1000405, CVE-2017-12190, CVE-2017-12192, CVE-2017-15649, CVE-2017-16527, CVE-2017-16650, CVE-2017-2618

Description

The scan detected that the host is missing the following update:
ELSA-2017-3651

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-December/007406.html
http://oss.oracle.com/pipermail/el-errata/2017-December/007405.html

OEL7
x86_64
kernel-uek-firmware-4.1.12-103.10.1.el7uek
kernel-uek-doc-4.1.12-103.10.1.el7uek
kernel-uek-debug-4.1.12-103.10.1.el7uek
kernel-uek-4.1.12-103.10.1.el7uek
kernel-uek-devel-4.1.12-103.10.1.el7uek
kernel-uek-debug-devel-4.1.12-103.10.1.el7uek

OEL6
x86_64
kernel-uek-firmware-4.1.12-103.10.1.el6uek
kernel-uek-doc-4.1.12-103.10.1.el6uek
kernel-uek-debug-devel-4.1.12-103.10.1.el6uek
kernel-uek-devel-4.1.12-103.10.1.el6uek
kernel-uek-4.1.12-103.10.1.el6uek
kernel-uek-debug-4.1.12-103.10.1.el6uek

170907 - Amazon Linux AMI ALAS-2017-931 Update Is Not Installed

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

Risk Level: High

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

Description

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

ALAS-2017-931

Observation

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

https://alas.aws.amazon.com/ALAS-2017-931.html

Amazon Linux AMI
x86_64
postgresql92-9.2.24-1.65.amzn1
postgresql94-plpython27-9.4.15-1.73.amzn1
postgresql92-devel-9.2.24-1.65.amzn1
postgresql94-devel-9.4.15-1.73.amzn1
postgresql92-plperl-9.2.24-1.65.amzn1
postgresql93-debuginfo-9.3.20-1.69.amzn1
postgresql94-libs-9.4.15-1.73.amzn1
postgresql94-9.4.15-1.73.amzn1
postgresql93-9.3.20-1.69.amzn1
postgresql92-server-compat-9.2.24-1.65.amzn1
postgresql94-contrib-9.4.15-1.73.amzn1
postgresql94-plperl-9.4.15-1.73.amzn1
postgresql94-server-9.4.15-1.73.amzn1
postgresql93-libs-9.3.20-1.69.amzn1
postgresql94-test-9.4.15-1.73.amzn1
postgresql92-plpython26-9.2.24-1.65.amzn1
postgresql94-docs-9.4.15-1.73.amzn1
postgresql93-plpython26-9.3.20-1.69.amzn1
postgresql92-plpython27-9.2.24-1.65.amzn1
postgresql92-libs-9.2.24-1.65.amzn1
postgresql93-pltcl-9.3.20-1.69.amzn1
postgresql92-server-9.2.24-1.65.amzn1
postgresql93-plperl-9.3.20-1.69.amzn1
postgresql93-server-9.3.20-1.69.amzn1
postgresql94-debuginfo-9.4.15-1.73.amzn1
postgresql94-plpython26-9.4.15-1.73.amzn1
postgresql93-test-9.3.20-1.69.amzn1
postgresql92-test-9.2.24-1.65.amzn1
postgresql93-devel-9.3.20-1.69.amzn1
postgresql93-plpython27-9.3.20-1.69.amzn1
postgresql92-pltcl-9.2.24-1.65.amzn1
postgresql92-contrib-9.2.24-1.65.amzn1
postgresql92-debuginfo-9.2.24-1.65.amzn1
postgresql93-docs-9.3.20-1.69.amzn1
postgresql92-docs-9.2.24-1.65.amzn1
postgresql93-contrib-9.3.20-1.69.amzn1

i686
postgresql92-9.2.24-1.65.amzn1
postgresql94-plpython26-9.4.15-1.73.amzn1
postgresql92-devel-9.2.24-1.65.amzn1
postgresql94-devel-9.4.15-1.73.amzn1
postgresql92-plperl-9.2.24-1.65.amzn1
postgresql93-debuginfo-9.3.20-1.69.amzn1
postgresql94-libs-9.4.15-1.73.amzn1
postgresql94-9.4.15-1.73.amzn1
postgresql93-9.3.20-1.69.amzn1
postgresql92-server-compat-9.2.24-1.65.amzn1
postgresql94-contrib-9.4.15-1.73.amzn1
postgresql94-plperl-9.4.15-1.73.amzn1

postgresql94-server-9.4.15-1.73.amzn1
postgresql93-libs-9.3.20-1.69.amzn1
postgresql94-test-9.4.15-1.73.amzn1
postgresql92-plpython26-9.2.24-1.65.amzn1
postgresql93-plpython26-9.3.20-1.69.amzn1
postgresql94-docs-9.4.15-1.73.amzn1
postgresql94-plpython27-9.4.15-1.73.amzn1
postgresql92-plpython27-9.2.24-1.65.amzn1
postgresql92-libs-9.2.24-1.65.amzn1
postgresql93-pltcl-9.3.20-1.69.amzn1
postgresql92-server-9.2.24-1.65.amzn1
postgresql93-plperl-9.3.20-1.69.amzn1
postgresql93-server-9.3.20-1.69.amzn1
postgresql94-debuginfo-9.4.15-1.73.amzn1
postgresql93-plpython27-9.3.20-1.69.amzn1
postgresql93-test-9.3.20-1.69.amzn1
postgresql92-test-9.2.24-1.65.amzn1
postgresql93-devel-9.3.20-1.69.amzn1
postgresql93-docs-9.3.20-1.69.amzn1
postgresql92-pltcl-9.2.24-1.65.amzn1
postgresql92-contrib-9.2.24-1.65.amzn1
postgresql92-debuginfo-9.2.24-1.65.amzn1
postgresql92-docs-9.2.24-1.65.amzn1
postgresql93-contrib-9.3.20-1.69.amzn1

170908 - Amazon Linux AMI ALAS-2017-930 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15098, CVE-2017-15099

Description

The scan detected that the host is missing the following update:
ALAS-2017-930

Observation

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

https://alas.aws.amazon.com/ALAS-2017-930.html

Amazon Linux AMI
x86_64
postgresql96-plperl-9.6.6-1.79.amzn1
postgresql96-docs-9.6.6-1.79.amzn1
postgresql96-static-9.6.6-1.79.amzn1
postgresql95-plpython26-9.5.10-1.77.amzn1
postgresql96-plpython26-9.6.6-1.79.amzn1
postgresql96-plpython27-9.6.6-1.79.amzn1
postgresql95-plperl-9.5.10-1.77.amzn1
postgresql95-test-9.5.10-1.77.amzn1
postgresql96-server-9.6.6-1.79.amzn1
postgresql96-test-9.6.6-1.79.amzn1
postgresql95-devel-9.5.10-1.77.amzn1
postgresql96-devel-9.6.6-1.79.amzn1
postgresql96-libs-9.6.6-1.79.amzn1
postgresql95-debuginfo-9.5.10-1.77.amzn1
postgresql95-static-9.5.10-1.77.amzn1

postgresql95-9.5.10-1.77.amzn1
postgresql95-libs-9.5.10-1.77.amzn1
postgresql96-debuginfo-9.6.6-1.79.amzn1
postgresql96-9.6.6-1.79.amzn1
postgresql96-contrib-9.6.6-1.79.amzn1
postgresql95-contrib-9.5.10-1.77.amzn1
postgresql95-docs-9.5.10-1.77.amzn1
postgresql95-server-9.5.10-1.77.amzn1
postgresql95-plpython27-9.5.10-1.77.amzn1

i686
postgresql96-plperl-9.6.6-1.79.amzn1
postgresql96-devel-9.6.6-1.79.amzn1
postgresql96-contrib-9.6.6-1.79.amzn1
postgresql95-plpython26-9.5.10-1.77.amzn1
postgresql96-plpython26-9.6.6-1.79.amzn1
postgresql96-static-9.6.6-1.79.amzn1
postgresql96-plpython27-9.6.6-1.79.amzn1
postgresql95-plperl-9.5.10-1.77.amzn1
postgresql95-test-9.5.10-1.77.amzn1
postgresql96-test-9.6.6-1.79.amzn1
postgresql95-devel-9.5.10-1.77.amzn1
postgresql96-docs-9.6.6-1.79.amzn1
postgresql96-libs-9.6.6-1.79.amzn1
postgresql95-debuginfo-9.5.10-1.77.amzn1
postgresql95-static-9.5.10-1.77.amzn1
postgresql95-9.5.10-1.77.amzn1
postgresql95-libs-9.5.10-1.77.amzn1
postgresql96-debuginfo-9.6.6-1.79.amzn1
postgresql96-9.6.6-1.79.amzn1
postgresql96-server-9.6.6-1.79.amzn1
postgresql95-contrib-9.5.10-1.77.amzn1
postgresql95-docs-9.5.10-1.77.amzn1
postgresql95-server-9.5.10-1.77.amzn1
postgresql95-plpython27-9.5.10-1.77.amzn1

175299 - Scientific Linux Security ERRATA Important: Openafs Security Update on SL6.x, SL7.x i386/x86_64 (1712-6984)

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: Openafs Security Update on SL6.x, SL7.x i386/x86_64 (1712-6984)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=6984

SL7
x86_64
openafs-1.6-sl-kernel-source-1.6.22-278.sl7
openafs-1.6-sl-1.6.22-278.sl7
openafs-1.6-sl-devel-1.6.22-278.sl7

openafs-1.6-sl-client-1.6.22-278.sl7
openafs-1.6-sl-krb5-1.6.22-278.sl7
openafs-1.6-sl-plumbing-tools-1.6.22-278.sl7
openafs-1.6-sl-module-tools-1.6.22-278.sl7
openafs-1.6-sl-authlibs-devel-1.6.22-278.sl7
openafs-1.6-sl-authlibs-1.6.22-278.sl7
kmod-openafs-1.6-sl-693-1.6.22-278.sl7.693.11.1
openafs-1.6-sl-kpasswd-1.6.22-278.sl7
openafs-1.6-sl-server-1.6.22-278.sl7
openafs-1.6-sl-compat-1.6.22-278.sl7

SL6
x86_64
openafs-kernel-source-1.6.20-257.sl6
openafs-kpasswd-1.6.20-257.sl6
openafs-client-1.6.20-257.sl6
openafs-authlibs-1.6.20-257.sl6
openafs-module-tools-1.6.20-257.sl6
openafs-1.6.20-257.sl6
openafs-devel-1.6.20-257.sl6
openafs-authlibs-devel-1.6.20-257.sl6
kmod-openafs-696-1.6.20-257.sl6.696
openafs-krb5-1.6.20-257.sl6
openafs-compat-1.6.20-257.sl6
openafs-server-1.6.20-257.sl6
openafs-plumbing-tools-1.6.20-257.sl6

i386
openafs-kernel-source-1.6.20-257.sl6
openafs-kpasswd-1.6.20-257.sl6
openafs-client-1.6.20-257.sl6
openafs-authlibs-1.6.20-257.sl6
openafs-module-tools-1.6.20-257.sl6
openafs-1.6.20-257.sl6
openafs-devel-1.6.20-257.sl6
openafs-authlibs-devel-1.6.20-257.sl6
kmod-openafs-696-1.6.20-257.sl6.696
openafs-krb5-1.6.20-257.sl6
openafs-compat-1.6.20-257.sl6
openafs-server-1.6.20-257.sl6
openafs-plumbing-tools-1.6.20-257.sl6

186007 - Ubuntu Linux 16.04 USN-3511-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3511-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004190.html

Ubuntu 16.04

linux-image-4.11.0-1016-azure_4.11.0-1016.16
linux-image-azure_4.11.0.1016.16

186008 - Ubuntu Linux 16.04 USN-3507-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12193, CVE-2017-15299, CVE-2017-15306, CVE-2017-15951, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3507-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004192.html

Ubuntu 16.04

linux-image-4.13.0-1002-gcp_4.13.0-1002.5
linux-image-gcp_4.13.0.1002.4
linux-image-gke_4.13.0.1002.4

186009 - Ubuntu Linux 12.04 USN-3510-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3510-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004189.html

Ubuntu 12.04

linux-image-3.13.0-137-generic-lpae_3.13.0-137.186~precise1
linux-image-3.13.0-137-generic_3.13.0-137.186~precise1
linux-image-generic-lpae-lts-trusty_3.13.0.137.127
linux-image-generic-lts-trusty_3.13.0.137.127

186012 - Ubuntu Linux 14.04 USN-3510-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3510-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004186.html

Ubuntu 14.04

linux-image-3.13.0-137-generic-lpae_3.13.0-137.186
linux-image-3.13.0-137-lowlatency_3.13.0-137.186
linux-image-powerpc64-smp_3.13.0.137.146
linux-image-lowlatency_3.13.0.137.146
linux-image-3.13.0-137-powerpc-e500_3.13.0-137.186
linux-image-powerpc-smp_3.13.0.137.146
linux-image-3.13.0-137-powerpc-e500mc_3.13.0-137.186
linux-image-powerpc-e500_3.13.0.137.146
linux-image-generic_3.13.0.137.146
linux-image-3.13.0-137-generic_3.13.0-137.186
linux-image-powerpc-e500mc_3.13.0.137.146
linux-image-powerpc64-emb_3.13.0.137.146
linux-image-3.13.0-137-powerpc64-smp_3.13.0-137.186
linux-image-3.13.0-137-powerpc64-emb_3.13.0-137.186
linux-image-generic-lpae_3.13.0.137.146
linux-image-3.13.0-137-powerpc-smp_3.13.0-137.186

186013 - Ubuntu Linux 16.04 USN-3508-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12146, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3508-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004187.html

Ubuntu 16.04

linux-image-4.10.0-42-generic_4.10.0-42.46~16.04.1
linux-image-lowlatency-hwe-16.04_4.10.0.42.44
linux-image-generic-hwe-16.04_4.10.0.42.44
linux-image-4.10.0-42-generic-lpae_4.10.0-42.46~16.04.1
linux-image-4.10.0-42-lowlatency_4.10.0-42.46~16.04.1
linux-image-generic-lpae-hwe-16.04_4.10.0.42.44

186014 - Ubuntu Linux 16.04 USN-3509-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12193, CVE-2017-16643, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3509-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004185.html

Ubuntu 16.04

linux-image-aws_4.4.0.1043.45
linux-image-4.4.0-1081-snapdragon_4.4.0-1081.86
linux-image-powerpc-e500mc_4.4.0.103.108
linux-image-snapdragon_4.4.0.1081.73
linux-image-4.4.0-1079-raspi2_4.4.0-1079.87
linux-image-generic_4.4.0.103.108
linux-image-kvm_4.4.0.1012.12
linux-image-powerpc64-smp_4.4.0.103.108
linux-image-4.4.0-103-powerpc64-smp_4.4.0-103.126
linux-image-generic-lpae_4.4.0.103.108
linux-image-4.4.0-103-powerpc-e500mc_4.4.0-103.126
linux-image-4.4.0-103-lowlatency_4.4.0-103.126
linux-image-raspi2_4.4.0.1079.79
linux-image-4.4.0-1012-kvm_4.4.0-1012.17
linux-image-lowlatency_4.4.0.103.108
linux-image-powerpc-smp_4.4.0.103.108
linux-image-4.4.0-103-powerpc64-emb_4.4.0-103.126
linux-image-4.4.0-103-generic-lpae_4.4.0-103.126
linux-image-4.4.0-103-powerpc-smp_4.4.0-103.126
linux-image-powerpc64-emb_4.4.0.103.108
linux-image-4.4.0-103-generic_4.4.0-103.126
linux-image-4.4.0-1043-aws_4.4.0-1043.52

186015 - Ubuntu Linux 17.10 USN-3507-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12193, CVE-2017-15299, CVE-2017-15306, CVE-2017-15951, CVE-2017-16535, CVE-2017-16643, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3507-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004183.html

Ubuntu 17.10

linux-image-4.13.0-19-generic_4.13.0-19.22
linux-image-raspi2_4.13.0.1008.6
linux-image-4.13.0-19-generic-lpae_4.13.0-19.22
linux-image-generic_4.13.0.19.20
linux-image-lowlatency_4.13.0.19.20
linux-image-4.13.0-19-lowlatency_4.13.0-19.22
linux-image-4.13.0-1008-raspi2_4.13.0-1008.8
linux-image-generic-lpae_4.13.0.19.20

186017 - Ubuntu Linux 14.04 USN-3509-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12193, CVE-2017-16643, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3509-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004188.html

Ubuntu 14.04

linux-image-4.4.0-1005-aws_4.4.0-1005.5
linux-image-aws_4.4.0.1005.5
linux-image-generic-lts-xenial_4.4.0.103.86
linux-image-powerpc-smp-lts-xenial_4.4.0.103.86
linux-image-4.4.0-103-powerpc-e500mc_4.4.0-103.126~14.04.1
linux-image-generic-lpae-lts-xenial_4.4.0.103.86
linux-image-lowlatency-lts-xenial_4.4.0.103.86
linux-image-4.4.0-103-lowlatency_4.4.0-103.126~14.04.1
linux-image-4.4.0-103-powerpc64-smp_4.4.0-103.126~14.04.1
linux-image-powerpc64-emb-lts-xenial_4.4.0.103.86
linux-image-powerpc64-smp-lts-xenial_4.4.0.103.86
linux-image-4.4.0-103-powerpc64-emb_4.4.0-103.126~14.04.1
linux-image-4.4.0-103-generic_4.4.0-103.126~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.103.86
linux-image-4.4.0-103-generic-lpae_4.4.0-103.126~14.04.1
linux-image-4.4.0-103-powerpc-smp_4.4.0-103.126~14.04.1

186018 - Ubuntu Linux 17.04 USN-3508-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12146, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3508-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004184.html

Ubuntu 17.04

linux-image-generic_4.10.0.42.42
linux-image-4.10.0-42-generic_4.10.0-42.46
linux-image-lowlatency_4.10.0.42.42
linux-image-4.10.0-42-generic-lpae_4.10.0-42.46
linux-image-4.10.0-1023-raspi2_4.10.0-1023.26
linux-image-4.10.0-42-lowlatency_4.10.0-42.46
linux-image-raspi2_4.10.0.1023.24
linux-image-generic-lpae_4.10.0.42.42

193029 - Fedora Linux 26 FEDORA-2017-0032baa7d7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16943, CVE-2017-16944

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0032baa7d7

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/2017/12/?count=200&page=1

Fedora Core 26

exim-4.89-7.fc26

193031 - Fedora Linux 25 FEDORA-2017-1fb805bfc2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16927

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1fb805bfc2

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/2017/12/?count=200&page=5

Fedora Core 25

xrdp-0.9.4-2.fc25

193046 - Fedora Linux 27 FEDORA-2017-b891f919c5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16927

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b891f919c5

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/2017/12/?count=200&page=3

Fedora Core 27

xrdp-0.9.4-2.fc27

193050 - Fedora Linux 27 FEDORA-2017-0053bb9719 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16943, CVE-2017-16944

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0053bb9719

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/2017/12/?count=200&page=2

Fedora Core 27

exim-4.89-7.fc27

193053 - Fedora Linux 27 FEDORA-2017-9fd430dba0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13764, CVE-2017-13765, CVE-2017-13766, CVE-2017-13767, CVE-2017-15189, CVE-2017-15190, CVE-2017-15191, CVE-2017-15192, CVE-2017-15193

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9fd430dba0

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/2017/12/?count=200&page=4

Fedora Core 27

wireshark-2.4.2-1.fc27

193064 - Fedora Linux 26 FEDORA-2017-f67f3ffb5d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16927

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f67f3ffb5d

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/2017/12/?count=200&page=4

Fedora Core 26

xrdp-0.9.4-2.fc26

193077 - Fedora Linux 25 FEDORA-2017-f2577f2108 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15592, CVE-2017-15595

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f2577f2108

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/2017/12/?count=200&page=1

Fedora Core 25

xen-4.7.4-1.fc25

22854 - (SB10218) McAfee ePolicy Orchestrator Tomcat Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-12615, CVE-2017-12617

Description

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator.

Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator. The flaws lie in the Tomcat component. Successful exploitation could allow an attacker to upload JSP files to the server and execute them using specific requests.

130969 - Debian Linux 8.0, 9.0 DSA-4058-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000229, CVE-2017-16938

Description

The scan detected that the host is missing the following update:
DSA-4058-1

Observation

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

http://www.debian.org/security/2017/dsa-4058

Debian 8.0
all
optipng_0.7.5-1+deb8u2

Debian 9.0
all
optipng_0.7.6-1+deb9u1

141806 - Red Hat Enterprise Linux RHSA-2017-3392 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10193, CVE-2017-10198, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
RHSA-2017-3392

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00006.html

RHEL7S
noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el7_4

x86_64
java-1.7.0-openjdk-accessibility-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-headless-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el7_4

RHEL6S
i386
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el6_9

x86_64
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el6_9

RHEL6WS
x86_64
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el6_9

i386
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el6_9

RHEL7D
x86_64
java-1.7.0-openjdk-accessibility-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-headless-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el7_4

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el7_4

RHEL6D
i386
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el6_9

x86_64
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el6_9

RHEL7WS
x86_64
java-1.7.0-openjdk-accessibility-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-headless-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el7_4

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el7_4

146140 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3243-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2008-1483, CVE-2017-15906

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3243-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00032.html

SuSE Linux 42.2
x86_64
openssh-helpers-debuginfo-7.2p2-11.6.1
openssh-cavs-7.2p2-11.6.1
openssh-askpass-gnome-debuginfo-7.2p2-11.6.1
openssh-helpers-7.2p2-11.6.1
openssh-askpass-gnome-7.2p2-11.6.1
openssh-7.2p2-11.6.1
openssh-debugsource-7.2p2-11.6.1
openssh-cavs-debuginfo-7.2p2-11.6.1
openssh-fips-7.2p2-11.6.1
openssh-debuginfo-7.2p2-11.6.1

i586
openssh-helpers-debuginfo-7.2p2-11.6.1
openssh-cavs-7.2p2-11.6.1
openssh-askpass-gnome-debuginfo-7.2p2-11.6.1
openssh-helpers-7.2p2-11.6.1
openssh-askpass-gnome-7.2p2-11.6.1

openssh-7.2p2-11.6.1
openssh-debugsource-7.2p2-11.6.1
openssh-cavs-debuginfo-7.2p2-11.6.1
openssh-fips-7.2p2-11.6.1
openssh-debuginfo-7.2p2-11.6.1

SuSE Linux 42.3
x86_64
openssh-7.2p2-15.1
openssh-debugsource-7.2p2-15.1
openssh-askpass-gnome-7.2p2-15.1
openssh-helpers-debuginfo-7.2p2-15.1
openssh-fips-7.2p2-15.1
openssh-cavs-debuginfo-7.2p2-15.1
openssh-helpers-7.2p2-15.1
openssh-cavs-7.2p2-15.1
openssh-askpass-gnome-debuginfo-7.2p2-15.1
openssh-debuginfo-7.2p2-15.1

i586
openssh-7.2p2-15.1
openssh-debugsource-7.2p2-15.1
openssh-askpass-gnome-7.2p2-15.1
openssh-helpers-debuginfo-7.2p2-15.1
openssh-fips-7.2p2-15.1
openssh-cavs-debuginfo-7.2p2-15.1
openssh-helpers-7.2p2-15.1
openssh-cavs-7.2p2-15.1
openssh-askpass-gnome-debuginfo-7.2p2-15.1
openssh-debuginfo-7.2p2-15.1

146142 - SuSE SLES 12 SP2 SUSE-SU-2017:3267-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12153, CVE-2017-13080, CVE-2017-14489, CVE-2017-15265, CVE-2017-15649

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3267-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003489.html

SuSE SLES 12 SP2
x86_64
cluster-md-kmp-rt-debuginfo-4.4.95-21.1
kernel-rt-base-4.4.95-21.1
gfs2-kmp-rt-debuginfo-4.4.95-21.1
kernel-rt_debug-devel-debuginfo-4.4.95-21.1
kernel-rt-base-debuginfo-4.4.95-21.1
kernel-rt-debuginfo-4.4.95-21.1
kernel-rt-devel-4.4.95-21.1
kernel-rt_debug-devel-4.4.95-21.1
ocfs2-kmp-rt-4.4.95-21.1

gfs2-kmp-rt-4.4.95-21.1
kernel-rt-4.4.95-21.1
cluster-network-kmp-rt-debuginfo-4.4.95-21.1
cluster-md-kmp-rt-4.4.95-21.1
ocfs2-kmp-rt-debuginfo-4.4.95-21.1
dlm-kmp-rt-4.4.95-21.1
kernel-rt-debugsource-4.4.95-21.1
kernel-rt_debug-debugsource-4.4.95-21.1
cluster-network-kmp-rt-4.4.95-21.1
kernel-syms-rt-4.4.95-21.1
dlm-kmp-rt-debuginfo-4.4.95-21.1
kernel-rt_debug-debuginfo-4.4.95-21.1

noarch
kernel-devel-rt-4.4.95-21.1
kernel-source-rt-4.4.95-21.1

146145 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3241-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16853

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3241-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00031.html

SuSE Linux 42.2
x86_64
libsaml-devel-2.5.5-3.3.1
libsaml8-2.5.5-3.3.1
opensaml-bin-debuginfo-2.5.5-3.3.1
opensaml-debugsource-2.5.5-3.3.1
opensaml-bin-2.5.5-3.3.1
libsaml8-debuginfo-2.5.5-3.3.1
opensaml-schemas-2.5.5-3.3.1

SuSE Linux 42.3
x86_64
opensaml-bin-2.5.5-6.1
libsaml-devel-2.5.5-6.1
opensaml-bin-debuginfo-2.5.5-6.1
opensaml-debugsource-2.5.5-6.1
libsaml8-debuginfo-2.5.5-6.1
libsaml8-2.5.5-6.1
opensaml-schemas-2.5.5-6.1

146147 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3234-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16853

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3234-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003480.html

SuSE SLES 12 SP3
x86_64
opensaml-debugsource-2.5.5-3.3.1
libsaml8-2.5.5-3.3.1
opensaml-bin-debuginfo-2.5.5-3.3.1
opensaml-bin-2.5.5-3.3.1
libsaml8-debuginfo-2.5.5-3.3.1
opensaml-schemas-2.5.5-3.3.1

SuSE SLES 12 SP2
x86_64
opensaml-debugsource-2.5.5-3.3.1
libsaml8-2.5.5-3.3.1
opensaml-bin-debuginfo-2.5.5-3.3.1
opensaml-bin-2.5.5-3.3.1
libsaml8-debuginfo-2.5.5-3.3.1
opensaml-schemas-2.5.5-3.3.1

146151 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3230-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2008-1483, CVE-2017-15906

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3230-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003476.html

SuSE SLES 12 SP2
x86_64
openssh-debuginfo-7.2p2-74.11.1
openssh-7.2p2-74.11.1
openssh-debugsource-7.2p2-74.11.1
openssh-helpers-7.2p2-74.11.1
openssh-helpers-debuginfo-7.2p2-74.11.1
openssh-askpass-gnome-7.2p2-74.11.3
openssh-askpass-gnome-debuginfo-7.2p2-74.11.3
openssh-fips-7.2p2-74.11.1

SuSE SLED 12 SP3
x86_64
openssh-debuginfo-7.2p2-74.11.1
openssh-7.2p2-74.11.1
openssh-debugsource-7.2p2-74.11.1
openssh-helpers-7.2p2-74.11.1
openssh-helpers-debuginfo-7.2p2-74.11.1
openssh-askpass-gnome-7.2p2-74.11.3
openssh-askpass-gnome-debuginfo-7.2p2-74.11.3

SuSE SLED 12 SP2
x86_64
openssh-debuginfo-7.2p2-74.11.1
openssh-7.2p2-74.11.1
openssh-debugsource-7.2p2-74.11.1
openssh-helpers-7.2p2-74.11.1
openssh-helpers-debuginfo-7.2p2-74.11.1
openssh-askpass-gnome-7.2p2-74.11.3
openssh-askpass-gnome-debuginfo-7.2p2-74.11.3

SuSE SLES 12 SP3
x86_64
openssh-debuginfo-7.2p2-74.11.1
openssh-7.2p2-74.11.1
openssh-debugsource-7.2p2-74.11.1
openssh-helpers-7.2p2-74.11.1
openssh-helpers-debuginfo-7.2p2-74.11.1
openssh-askpass-gnome-7.2p2-74.11.3
openssh-askpass-gnome-debuginfo-7.2p2-74.11.3
openssh-fips-7.2p2-74.11.1

146155 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3229-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16852

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3229-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00028.html

SuSE Linux 42.2
x86_64
shibboleth-sp-devel-2.5.5-6.3.1
libshibsp6-debuginfo-2.5.5-6.3.1
libshibsp6-2.5.5-6.3.1
libshibsp-lite6-2.5.5-6.3.1
shibboleth-sp-2.5.5-6.3.1
shibboleth-sp-debuginfo-2.5.5-6.3.1
libshibsp-lite6-debuginfo-2.5.5-6.3.1
shibboleth-sp-debugsource-2.5.5-6.3.1

SuSE Linux 42.3
x86_64
libshibsp6-2.5.5-9.2
libshibsp-lite6-2.5.5-9.2
shibboleth-sp-debugsource-2.5.5-9.2
libshibsp6-debuginfo-2.5.5-9.2
shibboleth-sp-devel-2.5.5-9.2
libshibsp-lite6-debuginfo-2.5.5-9.2
shibboleth-sp-2.5.5-9.2
shibboleth-sp-debuginfo-2.5.5-9.2

160336 - CentOS 6, 7 CESA-2017-3392 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10193, CVE-2017-10198, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
CESA-2017-3392

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-December/022689.html
http://lists.centos.org/pipermail/centos-announce/2017-December/022688.html

CentOS 7
x86_64
java-1.7.0-openjdk-accessibility-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-headless-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el7_4

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el7_4

CentOS 6
i686
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el6_9

x86_64
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9

163512 - Oracle Enterprise Linux ELSA-2017-3392 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10193, CVE-2017-10198, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
ELSA-2017-3392

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-December/007401.html
http://oss.oracle.com/pipermail/el-errata/2017-December/007402.html

OEL7
x86_64
java-1.7.0-openjdk-headless-1.7.0.161-2.6.12.0.0.1.el7_4
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.0.1.el7_4
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.0.1.el7_4
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.0.1.el7_4
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.0.1.el7_4
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.0.1.el7_4
java-1.7.0-openjdk-accessibility-1.7.0.161-2.6.12.0.0.1.el7_4

OEL6
x86_64
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.0.1.el6_9
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.0.1.el6_9
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.0.1.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.0.1.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.0.1.el6_9

i386
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.0.1.el6_9
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.0.1.el6_9
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.0.1.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.0.1.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.0.1.el6_9

175300 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1712-6341)

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

Risk Level: Medium

CVE: CVE-2017-10193, CVE-2017-10198, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1712-6341)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=6341

SL7
x86_64
java-1.7.0-openjdk-accessibility-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-headless-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el7_4
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el7_4

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el7_4

SL6
i386
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.el6_9

x86_64
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.el6_9

193030 - Fedora Linux 27 FEDORA-2017-b16cdbdc34 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000256

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b16cdbdc34

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/2017/12/?count=200&page=1

Fedora Core 27

libvirt-3.7.0-3.fc27

193043 - Fedora Linux 25 FEDORA-2017-9ae6e39bde Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14685, CVE-2017-14686, CVE-2017-14687, CVE-2017-15369, CVE-2017-15587, CVE-2017-9216

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9ae6e39bde

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/2017/12/?count=200&page=3

Fedora Core 25

mupdf-1.11-9.fc25

22800 - (K64505405) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-4956

Description

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

Observation

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

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

130967 - Debian Linux 8.0, 9.0 DSA-4060-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11408, CVE-2017-13766, CVE-2017-17083, CVE-2017-17084, CVE-2017-17085

Description

The scan detected that the host is missing the following update:
DSA-4060-1

Observation

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

http://www.debian.org/security/2017/dsa-4060

Debian 8.0
all
wireshark_1.12.1+g01b65bf-4+deb8u12

Debian 9.0
all
wireshark_2.2.6+g32dac6a-2+deb9u1

141804 - Red Hat Enterprise Linux RHSA-2017-3442 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10165, CVE-2017-10167, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10279, CVE-2017-10283, CVE-2017-10284, CVE-2017-10286, CVE-2017-10294, CVE-2017-10296, CVE-2017-10311, CVE-2017-10313, CVE-2017-10314, CVE-2017-10320, CVE-2017-10365, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

The scan detected that the host is missing the following update:
RHSA-2017-3442

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00016.html

RHEL7S
x86_64
rh-mysql57-mysql-test-5.7.20-1.el7
rh-mysql57-mysql-errmsg-5.7.20-1.el7
rh-mysql57-mysql-config-5.7.20-1.el7
rh-mysql57-mysql-common-5.7.20-1.el7
rh-mysql57-mysql-debuginfo-5.7.20-1.el7
rh-mysql57-mysql-server-5.7.20-1.el7
rh-mysql57-mysql-devel-5.7.20-1.el7
rh-mysql57-mysql-5.7.20-1.el7

RHEL6S
x86_64
rh-mysql57-mysql-errmsg-5.7.20-1.el6
rh-mysql57-mysql-config-5.7.20-1.el6
rh-mysql57-mysql-server-5.7.20-1.el6
rh-mysql57-mysql-debuginfo-5.7.20-1.el6
rh-mysql57-mysql-common-5.7.20-1.el6
rh-mysql57-mysql-devel-5.7.20-1.el6
rh-mysql57-mysql-5.7.20-1.el6
rh-mysql57-mysql-test-5.7.20-1.el6

RHEL6WS
x86_64
rh-mysql57-mysql-errmsg-5.7.20-1.el6
rh-mysql57-mysql-config-5.7.20-1.el6
rh-mysql57-mysql-server-5.7.20-1.el6
rh-mysql57-mysql-debuginfo-5.7.20-1.el6
rh-mysql57-mysql-common-5.7.20-1.el6
rh-mysql57-mysql-devel-5.7.20-1.el6
rh-mysql57-mysql-5.7.20-1.el6
rh-mysql57-mysql-test-5.7.20-1.el6

RHEL6_7S
x86_64

rh-mysql57-mysql-errmsg-5.7.20-1.el6
rh-mysql57-mysql-config-5.7.20-1.el6
rh-mysql57-mysql-server-5.7.20-1.el6
rh-mysql57-mysql-debuginfo-5.7.20-1.el6
rh-mysql57-mysql-common-5.7.20-1.el6
rh-mysql57-mysql-devel-5.7.20-1.el6
rh-mysql57-mysql-5.7.20-1.el6
rh-mysql57-mysql-test-5.7.20-1.el6

RHEL7_3S
x86_64
rh-mysql57-mysql-test-5.7.20-1.el7
rh-mysql57-mysql-errmsg-5.7.20-1.el7
rh-mysql57-mysql-config-5.7.20-1.el7
rh-mysql57-mysql-common-5.7.20-1.el7
rh-mysql57-mysql-debuginfo-5.7.20-1.el7
rh-mysql57-mysql-server-5.7.20-1.el7
rh-mysql57-mysql-devel-5.7.20-1.el7
rh-mysql57-mysql-5.7.20-1.el7

RHEL7WS
x86_64
rh-mysql57-mysql-test-5.7.20-1.el7
rh-mysql57-mysql-errmsg-5.7.20-1.el7
rh-mysql57-mysql-config-5.7.20-1.el7
rh-mysql57-mysql-common-5.7.20-1.el7
rh-mysql57-mysql-debuginfo-5.7.20-1.el7
rh-mysql57-mysql-server-5.7.20-1.el7
rh-mysql57-mysql-devel-5.7.20-1.el7
rh-mysql57-mysql-5.7.20-1.el7

146141 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3259-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-4226, CVE-2017-14804, CVE-2017-9274

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3259-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00040.html

SuSE Linux 42.2
noarch
build-mkdrpms-20171128-2.6.1
osc-0.162.0-7.7.1
build-mkbaselibs-20171128-2.6.1
obs-service-source_validator-0.7-13.6.1
build-initvm-x86_64-20171128-2.6.1
build-20171128-2.6.1
build-initvm-i586-20171128-2.6.1

SuSE Linux 42.3

noarch
build-initvm-i586-20171128-5.1
build-20171128-5.1
build-mkbaselibs-20171128-5.1
obs-service-source_validator-0.7-16.1
osc-0.162.0-10.1
build-mkdrpms-20171128-5.1
build-initvm-x86_64-20171128-5.1

146144 - SuSE SLES 12 SP3 SUSE-SU-2017:3232-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14970

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3232-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003478.html

SuSE SLES 12 SP3
x86_64
openvswitch-debuginfo-2.7.0-3.10.1
openvswitch-debugsource-2.7.0-3.10.1
openvswitch-2.7.0-3.10.1

146152 - SuSE Linux 42.3 openSUSE-SU-2017:3238-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14970

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3238-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00029.html

SuSE Linux 42.3
x86_64
openvswitch-vtep-2.7.0-7.1
openvswitch-ovn-vtep-debuginfo-2.7.0-7.1
openvswitch-vtep-debuginfo-2.7.0-7.1
python-openvswitch-test-2.7.0-7.1
openvswitch-ovn-host-debuginfo-2.7.0-7.1
openvswitch-ovn-docker-2.7.0-7.1
python-openvswitch-2.7.0-7.1

openvswitch-ovn-host-2.7.0-7.1
openvswitch-pki-2.7.0-7.1
openvswitch-ovn-central-debuginfo-2.7.0-7.1
openvswitch-test-debuginfo-2.7.0-7.1
openvswitch-debuginfo-2.7.0-7.1
openvswitch-devel-2.7.0-7.1
openvswitch-ovn-common-2.7.0-7.1
openvswitch-ovn-common-debuginfo-2.7.0-7.1
openvswitch-2.7.0-7.1
openvswitch-test-2.7.0-7.1
openvswitch-ovn-vtep-2.7.0-7.1
openvswitch-debugsource-2.7.0-7.1
openvswitch-ovn-central-2.7.0-7.1

160333 - CentOS 7 CESA-2017-3379 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
CESA-2017-3379

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-December/022685.html

CentOS 7
i686
sssd-client-1.15.2-50.el7_4.8
libsss_certmap-1.15.2-50.el7_4.8
libsss_idmap-devel-1.15.2-50.el7_4.8
libipa_hbac-1.15.2-50.el7_4.8
libsss_certmap-devel-1.15.2-50.el7_4.8
libsss_nss_idmap-devel-1.15.2-50.el7_4.8
libsss_idmap-1.15.2-50.el7_4.8
libsss_simpleifp-1.15.2-50.el7_4.8
sssd-libwbclient-devel-1.15.2-50.el7_4.8
libsss_nss_idmap-1.15.2-50.el7_4.8
libipa_hbac-devel-1.15.2-50.el7_4.8
libsss_simpleifp-devel-1.15.2-50.el7_4.8

noarch
python-sssdconfig-1.15.2-50.el7_4.8

x86_64
sssd-polkit-rules-1.15.2-50.el7_4.8
sssd-ldap-1.15.2-50.el7_4.8
sssd-libwbclient-devel-1.15.2-50.el7_4.8
sssd-ipa-1.15.2-50.el7_4.8
sssd-common-1.15.2-50.el7_4.8
python-sss-murmur-1.15.2-50.el7_4.8
libsss_simpleifp-1.15.2-50.el7_4.8
libsss_idmap-1.15.2-50.el7_4.8
sssd-krb5-common-1.15.2-50.el7_4.8

libsss_certmap-1.15.2-50.el7_4.8
libipa_hbac-devel-1.15.2-50.el7_4.8
sssd-client-1.15.2-50.el7_4.8
python-libsss_nss_idmap-1.15.2-50.el7_4.8
python-sss-1.15.2-50.el7_4.8
sssd-winbind-idmap-1.15.2-50.el7_4.8
libsss_certmap-devel-1.15.2-50.el7_4.8
libipa_hbac-1.15.2-50.el7_4.8
libsss_nss_idmap-devel-1.15.2-50.el7_4.8
libsss_autofs-1.15.2-50.el7_4.8
sssd-dbus-1.15.2-50.el7_4.8
sssd-1.15.2-50.el7_4.8
libsss_sudo-1.15.2-50.el7_4.8
sssd-tools-1.15.2-50.el7_4.8
libsss_simpleifp-devel-1.15.2-50.el7_4.8
sssd-ad-1.15.2-50.el7_4.8
sssd-krb5-1.15.2-50.el7_4.8
sssd-libwbclient-1.15.2-50.el7_4.8
libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-common-pac-1.15.2-50.el7_4.8
sssd-proxy-1.15.2-50.el7_4.8
sssd-kcm-1.15.2-50.el7_4.8
python-libipa_hbac-1.15.2-50.el7_4.8
libsss_idmap-devel-1.15.2-50.el7_4.8

160334 - CentOS 7 CESA-2017-3384 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15101

Description

The scan detected that the host is missing the following update:
CESA-2017-3384

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-December/022684.html

CentOS 7
i686
liblouis-2.5.2-12.el7_4
liblouis-devel-2.5.2-12.el7_4

noarch
liblouis-doc-2.5.2-12.el7_4
liblouis-python-2.5.2-12.el7_4

x86_64
liblouis-2.5.2-12.el7_4
liblouis-utils-2.5.2-12.el7_4
liblouis-devel-2.5.2-12.el7_4

170903 - Amazon Linux AMI ALAS-2017-926 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10279, CVE-2017-10283, CVE-2017-10286, CVE-2017-10294, CVE-2017-10314, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

The scan detected that the host is missing the following update:
ALAS-2017-926

Observation

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

https://alas.aws.amazon.com/ALAS-2017-926.html

Amazon Linux AMI
x86_64
mysql56-embedded-devel-5.6.38-1.27.amzn1
mysql56-test-5.6.38-1.27.amzn1
mysql57-devel-5.7.20-2.5.amzn1
mysql56-errmsg-5.6.38-1.27.amzn1
mysql56-debuginfo-5.6.38-1.27.amzn1
mysql56-devel-5.6.38-1.27.amzn1
mysql56-libs-5.6.38-1.27.amzn1
mysql57-common-5.7.20-2.5.amzn1
mysql57-test-5.7.20-2.5.amzn1
mysql56-5.6.38-1.27.amzn1
mysql57-server-5.7.20-2.5.amzn1
mysql57-embedded-devel-5.7.20-2.5.amzn1
mysql56-common-5.6.38-1.27.amzn1
mysql57-errmsg-5.7.20-2.5.amzn1
mysql56-embedded-5.6.38-1.27.amzn1
mysql56-bench-5.6.38-1.27.amzn1
mysql57-embedded-5.7.20-2.5.amzn1
mysql57-debuginfo-5.7.20-2.5.amzn1
mysql57-libs-5.7.20-2.5.amzn1
mysql57-5.7.20-2.5.amzn1
mysql56-server-5.6.38-1.27.amzn1

i686
mysql56-embedded-devel-5.6.38-1.27.amzn1
mysql56-test-5.6.38-1.27.amzn1
mysql57-devel-5.7.20-2.5.amzn1
mysql56-errmsg-5.6.38-1.27.amzn1
mysql56-debuginfo-5.6.38-1.27.amzn1
mysql56-devel-5.6.38-1.27.amzn1
mysql56-libs-5.6.38-1.27.amzn1
mysql57-common-5.7.20-2.5.amzn1
mysql57-test-5.7.20-2.5.amzn1
mysql56-5.6.38-1.27.amzn1
mysql57-server-5.7.20-2.5.amzn1
mysql57-embedded-devel-5.7.20-2.5.amzn1
mysql56-common-5.6.38-1.27.amzn1
mysql57-errmsg-5.7.20-2.5.amzn1
mysql56-embedded-5.6.38-1.27.amzn1
mysql56-bench-5.6.38-1.27.amzn1
mysql57-embedded-5.7.20-2.5.amzn1
mysql57-debuginfo-5.7.20-2.5.amzn1
mysql57-libs-5.7.20-2.5.amzn1
mysql57-5.7.20-2.5.amzn1

mysql56-server-5.6.38-1.27.amzn1

182543 - FreeBSD FreeBSD OpenSSL Multiple Vulnerabilities (9442a811-dab3-11e7-b5af-a4badb2f4699)

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

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

The scan detected that the host is missing the following update:
FreeBSD -- OpenSSL multiple vulnerabilities (9442a811-dab3-11e7-b5af-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/9442a811-dab3-11e7-b5af-a4badb2f4699.html

Affected packages:
11.1 <= FreeBSD < 11.1_5
11.0 <= FreeBSD < 11.0_16
10.4 <= FreeBSD < 10.4_4
10.3 <= FreeBSD < 10.3_25

193036 - Fedora Linux 26 FEDORA-2017-7cbd8a00b7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11661, CVE-2017-11662, CVE-2017-11663, CVE-2017-11664

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7cbd8a00b7

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/2017/12/?count=200&page=5

Fedora Core 26

wildmidi-0.4.2-1.fc26

193055 - Fedora Linux 27 FEDORA-2017-dabf9a64d9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11661, CVE-2017-11662, CVE-2017-11663, CVE-2017-11664

Description

The scan detected that the host is missing the following update:
FEDORA-2017-dabf9a64d9

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/2017/12/?count=200&page=3

Fedora Core 27

wildmidi-0.4.2-1.fc27

193067 - Fedora Linux 25 FEDORA-2017-78f0991378 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15906

Description

The scan detected that the host is missing the following update:
FEDORA-2017-78f0991378

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/2017/12/?count=200&page=1

Fedora Core 25

openssh-7.4p1-5.fc25

193071 - Fedora Linux 26 FEDORA-2017-b0b4cc40c1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16899

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b0b4cc40c1

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/2017/12/?count=200&page=5

Fedora Core 26

transfig-3.2.6a-1.fc26

193076 - Fedora Linux 27 FEDORA-2017-96d1995b70 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15906

Description

The scan detected that the host is missing the following update:
FEDORA-2017-96d1995b70

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/2017/12/?count=200&page=4

Fedora Core 27

openssh-7.6p1-2.fc27

193084 - Fedora Linux 27 FEDORA-2017-c448cf31d6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16899

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c448cf31d6

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/2017/12/?count=200&page=4

Fedora Core 27

transfig-3.2.6a-1.fc27

130965 - Debian Linux 9.0 DSA-4056-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16239

Description

The scan detected that the host is missing the following update:
DSA-4056-1

Observation

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

http://www.debian.org/security/2017/dsa-4056

Debian 9.0
all
nova-cert_2:14.0.0-4+deb9u1

nova-api_2:14.0.0-4+deb9u1
nova-compute-lxc_2:14.0.0-4+deb9u1
nova-conductor_2:14.0.0-4+deb9u1
python-nova_2:14.0.0-4+deb9u1
nova-common_2:14.0.0-4+deb9u1
nova-placement-api_2:14.0.0-4+deb9u1
nova-console_2:14.0.0-4+deb9u1
nova-doc_2:14.0.0-4+deb9u1
nova-network_2:14.0.0-4+deb9u1
nova-consoleauth_2:14.0.0-4+deb9u1
nova-volume_2:14.0.0-4+deb9u1
nova-compute_2:14.0.0-4+deb9u1
nova-cells_2:14.0.0-4+deb9u1
nova-compute-kvm_2:14.0.0-4+deb9u1
nova-compute-ironic_2:14.0.0-4+deb9u1
nova-compute-qemu_2:14.0.0-4+deb9u1
nova-scheduler_2:14.0.0-4+deb9u1
nova-consoleproxy_2:14.0.0-4+deb9u1

170906 - Amazon Linux AMI ALAS-2017-927 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10268, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

The scan detected that the host is missing the following update:
ALAS-2017-927

Observation

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

https://alas.aws.amazon.com/ALAS-2017-927.html

Amazon Linux AMI
x86_64
mysql55-libs-5.5.58-1.19.amzn1
mysql55-devel-5.5.58-1.19.amzn1
mysql55-5.5.58-1.19.amzn1
mysql-config-5.5.58-1.19.amzn1
mysql55-debuginfo-5.5.58-1.19.amzn1
mysql55-bench-5.5.58-1.19.amzn1
mysql55-test-5.5.58-1.19.amzn1
mysql55-server-5.5.58-1.19.amzn1
mysql55-embedded-devel-5.5.58-1.19.amzn1
mysql55-embedded-5.5.58-1.19.amzn1

i686
mysql55-libs-5.5.58-1.19.amzn1
mysql55-devel-5.5.58-1.19.amzn1
mysql55-5.5.58-1.19.amzn1
mysql-config-5.5.58-1.19.amzn1
mysql55-debuginfo-5.5.58-1.19.amzn1
mysql55-bench-5.5.58-1.19.amzn1
mysql55-test-5.5.58-1.19.amzn1
mysql55-server-5.5.58-1.19.amzn1
mysql55-embedded-devel-5.5.58-1.19.amzn1

mysql55-embedded-5.5.58-1.19.amzn1

182541 - FreeBSD FreeBSD WPA2 Protocol Vulnerability (1f8de723-dab3-11e7-b5af-a4badb2f4699)

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

Risk Level: Medium

CVE: CVE-2017-1307, CVE-2017-1308

Description

The scan detected that the host is missing the following update:
FreeBSD -- WPA2 protocol vulnerability (1f8de723-dab3-11e7-b5af-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/1f8de723-dab3-11e7-b5af-a4badb2f4699.html

Affected packages:
11.1 <= FreeBSD < 11.1_2
11.0 <= FreeBSD < 11.0_13
10.4 <= FreeBSD < 10.4_1
10.3 <= FreeBSD < 10.3_22

182545 - FreeBSD FreeBSD POSIX Shm Allows Jails To Access Global Namespace (5b1463dd-dab3-11e7-b5af-a4badb2f4699)

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

Risk Level: Medium

CVE: CVE-2017-1087

Description

The scan detected that the host is missing the following update:
FreeBSD -- POSIX shm allows jails to access global namespace (5b1463dd-dab3-11e7-b5af-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/5b1463dd-dab3-11e7-b5af-a4badb2f4699.html

Affected packages:
10.4 <= FreeBSD-kernel < 10.4_3
10.3 <= FreeBSD-kernel < 10.3_24

193033 - Fedora Linux 25 FEDORA-2017-cdfd888e2e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15298

Description

The scan detected that the host is missing the following update:
FEDORA-2017-cdfd888e2e

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/2017/12/?count=200&page=5

Fedora Core 25

git-2.9.5-3.fc25

193035 - Fedora Linux 27 FEDORA-2017-c8712c7fc3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7496

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c8712c7fc3

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/2017/12/?count=200&page=3

Fedora Core 27

fedora-arm-installer-2.1-1.fc27

193040 - Fedora Linux 26 FEDORA-2017-0e4021062c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7496

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0e4021062c

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/2017/12/?count=200&page=1

Fedora Core 26

fedora-arm-installer-2.1-1.fc26

193068 - Fedora Linux 26 FEDORA-2017-3976710f1e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14992

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3976710f1e

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/2017/12/?count=200&page=4

Fedora Core 26

docker-1.13.1-44.git584d391.fc26

193072 - Fedora Linux 25 FEDORA-2017-62f44716bb Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7496

Description

The scan detected that the host is missing the following update:
FEDORA-2017-62f44716bb

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/2017/12/?count=200&page=1

Fedora Core 25

fedora-arm-installer-2.1-1.fc25

88904 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-342-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3737, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
SSA:2017-342-01

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=2017&m=slackware-security.792871

Slackware 14.0
x86_64

openssl-1.0.1u-x86_64-1
openssl-solibs-1.0.1u-x86_64-1

Slackware 13.37
x86_64
openssl-solibs-0.9.8zh-x86_64-2
openssl-0.9.8zh-x86_64-2

Slackware 14.1
x86_64
openssl-1.0.1u-x86_64-1
openssl-solibs-1.0.1u-x86_64-1

Slackware 13.1
x86_64
openssl-solibs-0.9.8zh-x86_64-2
openssl-0.9.8zh-x86_64-2

Slackware 14.2
x86_64
openssl-1.0.2n-x86_64-1
openssl-solibs-1.0.2n-x86_64-1

i586
openssl-1.0.2n-i586-1
openssl-solibs-1.0.2n-i586-1

Slackware 13.0
x86_64
openssl-solibs-0.9.8zh-x86_64-2
openssl-0.9.8zh-x86_64-2

130963 - Debian Linux 8.0, 9.0 DSA-4057-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000385

Description

The scan detected that the host is missing the following update:
DSA-4057-1

Observation

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

http://www.debian.org/security/2017/dsa-4057

Debian 8.0
all
erlang_1:17.3-dfsg-4+deb8u2

Debian 9.0
all
erlang_1:19.2.1+dfsg-2+deb9u1

130964 - Debian Linux 9.0 DSA-4061-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
DSA-4061-1

Observation

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

http://www.debian.org/security/2017/dsa-4061

Debian 9.0
all
thunderbird_1:52.5.0-1~deb9u1

130966 - Debian Linux 8.0, 9.0 DSA-4059-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16612

Description

The scan detected that the host is missing the following update:
DSA-4059-1

Observation

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

http://www.debian.org/security/2017/dsa-4059

Debian 8.0
all
libxcursor1-udeb_1:1.1.14-1+deb8u1
libxcursor1_1:1.1.14-1+deb8u1
libxcursor1-dbg_1:1.1.14-1+deb8u1
libxcursor-dev_1:1.1.14-1+deb8u1

Debian 9.0
all
libxcursor1-udeb_1:1.1.14-1+deb9u1
libxcursor-dev_1:1.1.14-1+deb9u1
libxcursor1-dbg_1:1.1.14-1+deb9u1
libxcursor1_1:1.1.14-1+deb9u1

130968 - Debian Linux 9.0 DSA-4064-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427

Description

The scan detected that the host is missing the following update:
DSA-4064-1

Observation

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

http://www.debian.org/security/2017/dsa-4064

Debian 9.0
all
chromium-shell_63.0.3239.84-1~deb9u1
chromium-widevine_63.0.3239.84-1~deb9u1
chromium-l10n_63.0.3239.84-1~deb9u1
chromium_63.0.3239.84-1~deb9u1
chromium-driver_63.0.3239.84-1~deb9u1
chromedriver_63.0.3239.84-1~deb9u1

130970 - Debian Linux 9.0 DSA-4063-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15120

Description

The scan detected that the host is missing the following update:
DSA-4063-1

Observation

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

http://www.debian.org/security/2017/dsa-4063

Debian 9.0
all
pdns-recursor_4.0.4-1+deb9u3

130971 - Debian Linux 9.0 DSA-4055-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17439

Description

The scan detected that the host is missing the following update:
DSA-4055-1

Observation

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

http://www.debian.org/security/2017/dsa-4055

Debian 9.0
all
libroken18-heimdal_7.1.0+dfsg-13+deb9u2
libwind0-heimdal_7.1.0+dfsg-13+deb9u2
libkrb5-26-heimdal_7.1.0+dfsg-13+deb9u2
libheimbase1-heimdal_7.1.0+dfsg-13+deb9u2
libhcrypto4-heimdal_7.1.0+dfsg-13+deb9u2
heimdal-multidev_7.1.0+dfsg-13+deb9u2
libhdb9-heimdal_7.1.0+dfsg-13+deb9u2
libsl0-heimdal_7.1.0+dfsg-13+deb9u2
libkdc2-heimdal_7.1.0+dfsg-13+deb9u2
libkadm5clnt7-heimdal_7.1.0+dfsg-13+deb9u2
heimdal-clients_7.1.0+dfsg-13+deb9u2
heimdal-kdc_7.1.0+dfsg-13+deb9u2
heimdal-dbg_7.1.0+dfsg-13+deb9u2
libkafs0-heimdal_7.1.0+dfsg-13+deb9u2
libasn1-8-heimdal_7.1.0+dfsg-13+deb9u2
libheimntlm0-heimdal_7.1.0+dfsg-13+deb9u2
heimdal-dev_7.1.0+dfsg-13+deb9u2
heimdal-docs_7.1.0+dfsg-13+deb9u2
libgssapi3-heimdal_7.1.0+dfsg-13+deb9u2
libhx509-5-heimdal_7.1.0+dfsg-13+deb9u2
libkadm5srv8-heimdal_7.1.0+dfsg-13+deb9u2
heimdal-servers_7.1.0+dfsg-13+deb9u2
libotp0-heimdal_7.1.0+dfsg-13+deb9u2
heimdal-kcm_7.1.0+dfsg-13+deb9u2

130972 - Debian Linux 8.0, 9.0 DSA-4062-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7843

Description

The scan detected that the host is missing the following update:
DSA-4062-1

Observation

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

http://www.debian.org/security/2017/dsa-4062

Debian 8.0
all
firefox-esr_52.5.2esr-1~deb8u1

Debian 9.0
all
firefox-esr_52.5.2esr-1~deb9u1

146160 - SuSE Linux 42.2 openSUSE-SU-2017:3256-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3256-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00037.html

SuSE Linux 42.2
x86_64
libXfont-debugsource-1.5.1-9.3.1
libXfont-devel-1.5.1-9.3.1
libXfont1-debuginfo-32bit-1.5.1-9.3.1
libXfont1-1.5.1-9.3.1
libXfont-devel-32bit-1.5.1-9.3.1
libXfont1-32bit-1.5.1-9.3.1
libXfont1-debuginfo-1.5.1-9.3.1

i586
libXfont-devel-1.5.1-9.3.1
libXfont-debugsource-1.5.1-9.3.1
libXfont1-1.5.1-9.3.1
libXfont1-debuginfo-1.5.1-9.3.1

170905 - Amazon Linux AMI ALAS-2017-928 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12613

Description

The scan detected that the host is missing the following update:
ALAS-2017-928

Observation

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

https://alas.aws.amazon.com/ALAS-2017-928.html

Amazon Linux AMI
x86_64
apr-debuginfo-1.5.2-5.13.amzn1
apr-1.5.2-5.13.amzn1
apr-devel-1.5.2-5.13.amzn1

i686
apr-devel-1.5.2-5.13.amzn1
apr-1.5.2-5.13.amzn1
apr-debuginfo-1.5.2-5.13.amzn1

182540 - FreeBSD OpenSSL Multiple Vulnerabilities (3bb451fc-db64-11e7-ac58-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-3737, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
OpenSSL -- multiple vulnerabilities (3bb451fc-db64-11e7-ac58-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/3bb451fc-db64-11e7-ac58-b499baebfeaf.html

Affected packages:
1.0.2 < openssl < 1.0.2n

182547 - FreeBSD wireshark Multiple Security Issues (4b228e69-22e1-4019-afd0-8aa716d0ec0b)

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

Risk Level: Low

CVE: CVE-2017-17083, CVE-2017-17084, CVE-2017-17085

Description

The scan detected that the host is missing the following update:
wireshark -- multiple security issues (4b228e69-22e1-4019-afd0-8aa716d0ec0b)

Observation

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

http://www.vuxml.org/freebsd/4b228e69-22e1-4019-afd0-8aa716d0ec0b.html

Affected packages:
2.2.0 <= wireshark <= 2.2.10
2.4.0 <= wireshark <= 2.4.2
2.2.0 <= wireshark-lite <= 2.2.10
2.4.0 <= wireshark-lite <= 2.4.2
2.2.0 <= wireshark-qt5 <= 2.2.10
2.4.0 <= wireshark-qt5 <= 2.4.2
2.2.0 <= tshark <= 2.2.10
2.4.0 <= tshark <= 2.4.2
2.2.0 <= tshark-lite <= 2.2.10
2.4.0 <= tshark-lite <= 2.4.2

186011 - Ubuntu Linux 16.04, 17.04, 17.10 USN-3512-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3737, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
USN-3512-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004193.html

Ubuntu 16.04

libssl1.0.0_1.0.2g-1ubuntu4.10

Ubuntu 17.04

libssl1.0.0_1.0.2g-1ubuntu11.4

Ubuntu 17.10

libssl1.0.0_1.0.2g-1ubuntu13.3

193034 - Fedora Linux 26 FEDORA-2017-69cc374b0d 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-2017-69cc374b0d

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/2017/12/?count=200&page=5

Fedora Core 26

mrbs-1.7.0-1.fc26

193037 - Fedora Linux 27 FEDORA-2017-386e856a4f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17042

Description

The scan detected that the host is missing the following update:
FEDORA-2017-386e856a4f

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/2017/12/?count=200&page=2

Fedora Core 27

rubygem-yard-0.9.8-4.fc27

193038 - Fedora Linux 26 FEDORA-2017-463cb2af78 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-2017-463cb2af78

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/2017/12/?count=200&page=1

Fedora Core 26

thunderbird-52.5.0-1.fc26

193041 - Fedora Linux 27 FEDORA-2017-97b730736f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16818

Description

The scan detected that the host is missing the following update:
FEDORA-2017-97b730736f

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/2017/12/?count=200&page=1

Fedora Core 27

ceph-12.2.2-1.fc27

193042 - Fedora Linux 25 FEDORA-2017-81fe39ad9f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15090, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

Description

The scan detected that the host is missing the following update:
FEDORA-2017-81fe39ad9f

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/2017/12/?count=200&page=1

Fedora Core 25

pdns-recursor-4.0.7-1.fc25

193044 - Fedora Linux 27 FEDORA-2017-7d33609b3d 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-2017-7d33609b3d

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/2017/12/?count=200&page=3

Fedora Core 27

thunderbird-52.5.0-1.fc27

193045 - Fedora Linux 27 FEDORA-2017-fba4c155be 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-2017-fba4c155be

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/2017/12/?count=200&page=3

Fedora Core 27

ca-certificates-2017.2.20-1.0.fc27

193047 - Fedora Linux 27 FEDORA-2017-4bfcd57172 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17044, CVE-2017-17045

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4bfcd57172

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/2017/12/?count=200&page=3

Fedora Core 27

xen-4.9.1-2.fc27

193048 - Fedora Linux 25 FEDORA-2017-ca05b30e86 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17042

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ca05b30e86

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/2017/12/?count=200&page=1

Fedora Core 25

rubygem-yard-0.8.7.6-4.fc25

193049 - Fedora Linux 26 FEDORA-2017-7b0a42338c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15914

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7b0a42338c

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/2017/12/?count=200&page=3

Fedora Core 26

borgbackup-1.1.3-1.fc26

193052 - Fedora Linux 26 FEDORA-2017-1585789772 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15090, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1585789772

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/2017/12/?count=200&page=1

Fedora Core 26

pdns-recursor-4.0.7-1.fc26

193054 - Fedora Linux 27 FEDORA-2017-f93ebc905e 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-2017-f93ebc905e

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/2017/12/?count=200&page=4

Fedora Core 27

mrbs-1.7.0-1.fc27

193056 - Fedora Linux 26 FEDORA-2017-efbe206b58 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-2017-efbe206b58

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/2017/12/?count=200&page=3

Fedora Core 26

dhcp-4.3.5-10.fc26

193057 - Fedora Linux 27 FEDORA-2017-81115c3047 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15914

Description

The scan detected that the host is missing the following update:
FEDORA-2017-81115c3047

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/2017/12/?count=200&page=3

Fedora Core 27

borgbackup-1.1.3-1.fc27

193058 - Fedora Linux 27 FEDORA-2017-45bdf4dace Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8816, CVE-2017-8817

Description

The scan detected that the host is missing the following update:
FEDORA-2017-45bdf4dace

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/2017/12/?count=200&page=3

Fedora Core 27

curl-7.55.1-8.fc27

193059 - Fedora Linux 25 FEDORA-2017-b5bcfedf10 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-2017-b5bcfedf10

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/2017/12/?count=200&page=5

Fedora Core 25

mrbs-1.7.0-1.fc25

193060 - Fedora Linux 26 FEDORA-2017-c6c6e9beae Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17042

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c6c6e9beae

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/2017/12/?count=200&page=1

Fedora Core 26

rubygem-yard-0.9.8-4.fc26

193062 - Fedora Linux 27 FEDORA-2017-d0046bc0ae 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-2017-d0046bc0ae

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/2017/12/?count=200&page=1

Fedora Core 27

dhcp-4.3.6-7.fc27

193063 - Fedora Linux 25 FEDORA-2017-2c15e19fb5 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-2017-2c15e19fb5

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/2017/12/?count=200&page=1

Fedora Core 25

firefox-57.0.1-1.fc25

193065 - Fedora Linux 27 FEDORA-2017-bfd2d4afce 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-2017-bfd2d4afce

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/2017/12/?count=200&page=3

Fedora Core 27

firefox-57.0.1-1.fc27

193066 - Fedora Linux 27 FEDORA-2017-608b6f5945 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15090, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

Description

The scan detected that the host is missing the following update:
FEDORA-2017-608b6f5945

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/2017/12/?count=200&page=2

Fedora Core 27

pdns-recursor-4.0.7-1.fc27

193070 - Fedora Linux 27 FEDORA-2017-9e6df1e099 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000385

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9e6df1e099

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/2017/12/?count=200&page=2

Fedora Core 27

erlang-19.3.6.4-1.fc27

193073 - Fedora Linux 26 FEDORA-2017-0c062324cd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8816, CVE-2017-8817

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0c062324cd

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/2017/12/?count=200&page=4

Fedora Core 26

curl-7.53.1-13.fc26

193074 - Fedora Linux 27 FEDORA-2017-15ce66d344 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-2017-15ce66d344

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/2017/12/?count=200&page=2

Fedora Core 27

wordpress-4.9.1-1.fc27

193075 - Fedora Linux 26 FEDORA-2017-93b6236635 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000385

Description

The scan detected that the host is missing the following update:
FEDORA-2017-93b6236635

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/2017/12/?count=200&page=1

Fedora Core 26

erlang-19.3.6.4-1.fc26

193079 - Fedora Linux 26 FEDORA-2017-3a8cbd86a1 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-2017-3a8cbd86a1

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/2017/12/?count=200&page=4

Fedora Core 26

ca-certificates-2017.2.20-1.0.fc26

193081 - Fedora Linux 25 FEDORA-2017-7f8abb1866 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-2017-7f8abb1866

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/2017/12/?count=200&page=5

Fedora Core 25

ca-certificates-2017.2.20-1.0.fc25

193082 - Fedora Linux 26 FEDORA-2017-1be05999bb 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-2017-1be05999bb

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/2017/12/?count=200&page=4

Fedora Core 26

firefox-57.0.1-1.fc26

193083 - Fedora Linux 26 FEDORA-2017-994ff5ced8 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-2017-994ff5ced8

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/2017/12/?count=200&page=1

Fedora Core 26

wordpress-4.9.1-1.fc26

160332 - CentOS 7 CESA-2017-3315 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000380

Description

The scan detected that the host is missing the following update:
CESA-2017-3315

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-December/022682.html

CentOS 7
x86_64
python-perf-3.10.0-693.11.1.el7
kernel-devel-3.10.0-693.11.1.el7
kernel-tools-libs-3.10.0-693.11.1.el7
kernel-tools-3.10.0-693.11.1.el7
kernel-3.10.0-693.11.1.el7
kernel-debug-3.10.0-693.11.1.el7
kernel-debug-devel-3.10.0-693.11.1.el7
kernel-tools-libs-devel-3.10.0-693.11.1.el7
kernel-headers-3.10.0-693.11.1.el7
perf-3.10.0-693.11.1.el7

noarch
kernel-abi-whitelists-3.10.0-693.11.1.el7
kernel-doc-3.10.0-693.11.1.el7

182542 - FreeBSD FreeBSD OpenSSL Multiple Vulnerabilities (9f7a0f39-ddc0-11e7-b5af-a4badb2f4699)

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

Risk Level: Low

CVE: CVE-2016-0701, CVE-2017-3737, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
FreeBSD -- OpenSSL multiple vulnerabilities (9f7a0f39-ddc0-11e7-b5af-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/9f7a0f39-ddc0-11e7-b5af-a4badb2f4699.html

Affected packages:
11.1 <= FreeBSD < 11.1_6
10.4 <= FreeBSD < 10.4_5
10.3 <= FreeBSD < 10.3_26

182544 - FreeBSD FreeBSD Kernel Data Leak Via Ptrace (PT_LWPINFO) (34a3f9b5-dab3-11e7-b5af-

a4badb2f4699)

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

Risk Level: Low

CVE: CVE-2017-1086

Description

The scan detected that the host is missing the following update:
FreeBSD -- Kernel data leak via ptrace(PT_LWPINFO) (34a3f9b5-dab3-11e7-b5af-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/34a3f9b5-dab3-11e7-b5af-a4badb2f4699.html

Affected packages:
11.1 <= FreeBSD-kernel < 11.1_4
11.0 <= FreeBSD-kernel < 11.0_15
10.4 <= FreeBSD-kernel < 10.4_3
10.3 <= FreeBSD-kernel < 10.3_24

182546 - FreeBSD FreeBSD Information Leak In Kldstat (2) (759059ac-dab3-11e7-b5af-a4badb2f4699)

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

Risk Level: Low

CVE: CVE-2017-1088

Description

The scan detected that the host is missing the following update:
FreeBSD -- Information leak in kldstat(2) (759059ac-dab3-11e7-b5af-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/759059ac-dab3-11e7-b5af-a4badb2f4699.html

Affected packages:
11.1 <= FreeBSD-kernel < 11.1_4
11.0 <= FreeBSD-kernel < 11.0_15
10.4 <= FreeBSD-kernel < 10.4_3
10.3 <= FreeBSD-kernel < 10.3_24

170904 - Amazon Linux AMI ALAS-2017-929 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12618

Description

The scan detected that the host is missing the following update:
ALAS-2017-929

Observation

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

https://alas.aws.amazon.com/ALAS-2017-929.html

Amazon Linux AMI
x86_64
apr-util-debuginfo-1.5.4-6.18.amzn1
apr-util-odbc-1.5.4-6.18.amzn1
apr-util-pgsql-1.5.4-6.18.amzn1
apr-util-ldap-1.5.4-6.18.amzn1
apr-util-nss-1.5.4-6.18.amzn1
apr-util-devel-1.5.4-6.18.amzn1
apr-util-1.5.4-6.18.amzn1
apr-util-mysql-1.5.4-6.18.amzn1
apr-util-sqlite-1.5.4-6.18.amzn1
apr-util-openssl-1.5.4-6.18.amzn1
apr-util-freetds-1.5.4-6.18.amzn1

i686
apr-util-debuginfo-1.5.4-6.18.amzn1
apr-util-openssl-1.5.4-6.18.amzn1
apr-util-pgsql-1.5.4-6.18.amzn1
apr-util-freetds-1.5.4-6.18.amzn1
apr-util-odbc-1.5.4-6.18.amzn1
apr-util-devel-1.5.4-6.18.amzn1
apr-util-1.5.4-6.18.amzn1
apr-util-mysql-1.5.4-6.18.amzn1
apr-util-ldap-1.5.4-6.18.amzn1
apr-util-sqlite-1.5.4-6.18.amzn1
apr-util-nss-1.5.4-6.18.amzn1

22861 - Microsoft Office 2016 Click-To-Run December 2017 Updates

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

Risk Level: Informational

CVE: CVE-2017-11934, CVE-2017-11935, CVE-2017-11939

Description

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

Observation

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

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run. The flaws are present in multiple components. Such defects could lead the product to software vulnerabilities, malfunction or unexpected behavior in some of its affected components.

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.

139072 - Oracle Solaris 11.3.25.3.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2015-7511, CVE-2016-3492, CVE-2016-5584, CVE-2016-5612, CVE-2016-5624, CVE-2016-5629, CVE-2016-6313, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-7440, CVE-2016-8283, CVE-2016-8318, CVE-2017-12150, CVE-2017-12151, CVE-2017-12163, CVE-2017-13765, CVE-2017-13766, CVE-2017-13767, CVE-2017-14482, CVE-2017-3238, CVE-2017-3244, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-2017-3273, CVE-2017-3291, CVE-2017-3312, CVE-2017-3634, CVE-2017-3635, CVE-2017-3636, CVE-2017-3641, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653, CVE-2017-3732, CVE-2017-7526, CVE-2017-7674, CVE-2017-7675, CVE-2017-7793, CVE-2017-7805, CVE-2017-7810, CVE-2017-7814, CVE-2017-7818, CVE-2017-7819, CVE-2017-7823, CVE-2017-7824, CVE-2017-7825

Update Details

CVE is updated

139073 - Oracle Solaris 11.3.14.6.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2014-0015, CVE-2015-0005, CVE-2015-1782, CVE-2015-4473, CVE-2015-4474, CVE-2015-4477, CVE-2015-4481, CVE-2015-4482, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4491, CVE-2015-4500, CVE-2015-4501, CVE-2015-4505, CVE-2015-4506, CVE-2015-4509, CVE-2015-4511, CVE-2015-4513, CVE-2015-4514, CVE-2015-4517, CVE-2015-4519, CVE-2015-4520, CVE-2015-4521, CVE-2015-4522, CVE-2015-5296, CVE-2015-5370, CVE-2015-5621, CVE-2015-7174, CVE-2015-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7178, CVE-2015-7179, CVE-2015-7180, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200, CVE-2015-7201, CVE-2015-7202, CVE-2015-7205, CVE-2015-7207, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222, CVE-2015-7575, CVE-2015-8704, CVE-2015-8705, CVE-2015-8957, CVE-2015-8958, CVE-2016-0755, CVE-2016-0787, CVE-2016-1523, CVE-2016-1930, CVE-2016-1931, CVE-2016-1935, CVE-2016-1938, CVE-2016-1950, CVE-2016-1952, CVE-2016-1953, CVE-2016-1954, CVE-2016-1955, CVE-2016-1956, CVE-2016-1957, CVE-2016-1958, CVE-2016-1960, CVE-2016-1961, CVE-2016-1962, CVE-2016-1964, CVE-2016-1965, CVE-2016-1966, CVE-2016-1967, CVE-2016-1969, CVE-2016-1974, CVE-2016-1977, CVE-2016-1978, CVE-2016-1979, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118, CVE-2016-2119, CVE-2016-2776, CVE-2016-2790, CVE-2016-2791, CVE-2016-2792, CVE-2016-2793, CVE-2016-2794, CVE-2016-2795, CVE-2016-2796, CVE-2016-2797, CVE-2016-2798, CVE-2016-2799, CVE-2016-2800, CVE-2016-2801, CVE-2016-2802, CVE-2016-2804, CVE-2016-2805, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814, CVE-2016-2815, CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822

Update Details

CVE is updated

139088 - Oracle Solaris 11.3.19.5.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2016-3614, CVE-2016-3615, CVE-2016-5436, CVE-2016-5437, CVE-2016-5439, CVE-2016-5440, CVE-2016-5441, CVE-2016-5442, CVE-2016-5443, CVE-2016-5444, CVE-2016-5507, CVE-2016-5584, CVE-2016-5598, CVE-2016-5609, CVE-2016-5612, CVE-2016-5624, CVE-2016-5625, CVE-2016-5626, CVE-2016-5627, CVE-2016-5628, CVE-2016-5629, CVE-2016-5630, CVE-2016-5631, CVE-2016-5632, CVE-2016-5633, CVE-2016-5634, CVE-2016-5635, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-7440, CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8283, CVE-2016-8284, CVE-2016-8286, CVE-2016-8287, CVE-2016-8288, CVE-2016-8289, CVE-2016-8290, CVE-2016-8318, CVE-2016-8327, CVE-2016-8574, CVE-2016-8575, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3251, CVE-2017-3256, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-2017-3273, CVE-2017-3291, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3319, CVE-2017-3320, CVE-2017-3564, CVE-2017-3565, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204,

CVE-2017-5205, CVE-2017-5341, CVE-2017-5342, CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5409, CVE-2017-5410, CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486, CVE-2017-6467, CVE-2017-6468, CVE-2017-6469, CVE-2017-6470, CVE-2017-6471, CVE-2017-6472, CVE-2017-6473, CVE-2017-6474

Update Details

CVE is updated

182521 - FreeBSD procmail Heap-based Buffer Overflow (288f7cee-ced6-11e7-8ae9-0050569f0b83)

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

Risk Level: High

CVE: CVE-2017-16844

Update Details

FASLScript is updated

139071 - Oracle Solaris 11.2.9.5.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2014-5353, CVE-2014-9623, CVE-2015-0255, CVE-2015-0471, CVE-2015-1802, CVE-2015-1803, CVE-2015-1804, CVE-2015-2188, CVE-2015-2189, CVE-2015-2190, CVE-2015-2191, CVE-2016-5480

Update Details

CVE is updated

22794 - MacOS High Sierra Login As Root With No Password Vulnerability

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

Risk Level: High

CVE: CVE-2017-13872

Update Details

FASLScript is updated

22832 - (MSPT-Dec2017) Microsoft Windows Malware Protection Engine Remote Code Execution (CVE-2017-11937)

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

Risk Level: High

CVE: CVE-2017-11937

Update Details

Risk is updated

130951 - Debian Linux 9.0 DSA-4044-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16613

Update Details

Risk is updated

139060 - Oracle Solaris 11.3.20.5.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2015-7545, CVE-2015-8107, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10164, CVE-2016-10349, CVE-2016-10350, CVE-2016-3105, CVE-2016-6855, CVE-2016-8745, CVE-2016-8747, CVE-2016-9042, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2017-10095, CVE-2017-2619, CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5408, CVE-2017-5410, CVE-2017-5429, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5469, CVE-2017-5618, CVE-2017-5647, CVE-2017-6451, CVE-2017-6452, CVE-2017-6455, CVE-2017-6458, CVE-2017-6459, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464, CVE-2017-7214, CVE-2017-7585, CVE-2017-7586, CVE-2017-7741, CVE-2017-7742, CVE-2017-8361, CVE-2017-8362, CVE-2017-8363, CVE-2017-8365

Update Details

CVE is updated

139063 - Oracle Solaris 11.3.15.4.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2015-8325, CVE-2016-0762, CVE-2016-3739, CVE-2016-5018, CVE-2016-5290, CVE-2016-5291, CVE-2016-5296, CVE-2016-5297, CVE-2016-5384, CVE-2016-5407, CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-6210, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797, CVE-2016-7076, CVE-2016-7167, CVE-2016-7942, CVE-2016-7943, CVE-2016-7944, CVE-2016-7945, CVE-2016-7946, CVE-2016-7947, CVE-2016-7948, CVE-2016-7949, CVE-2016-7950, CVE-2016-7951, CVE-2016-7952, CVE-2016-7953, CVE-2016-8330, CVE-2016-8858, CVE-2016-8864, CVE-2016-9064, CVE-2016-9066, CVE-2016-9074, CVE-2016-9189, CVE-2016-9190, CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633, CVE-2017-3276

Update Details

CVE is updated

192908 - Fedora Linux 27 FEDORA-2017-2dd6c320a4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15088

Update Details

Risk is updated

192938 - Fedora Linux 26 FEDORA-2017-41957e0f90 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15088

Update Details

Risk is updated

22821 - (MSPT-Dec2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11890)

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

Risk Level: Medium

CVE: CVE-2017-11890

Update Details

Recommendation is updated

130933 - Debian Linux 9.0 DSA-4028-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15098, CVE-2017-15099

Update Details

Risk is updated

130937 - Debian Linux 8.0 DSA-4027-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15098

Update Details

Risk is updated

182514 - FreeBSD PostgreSQL Vulnerabilities (1f02af5d-c566-11e7-a12d-6cc21735f730)

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

Risk Level: Medium

CVE: CVE-2017-15098, CVE-2017-15099

Update Details

Risk is updated

185963 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3479-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15098, CVE-2017-15099

Update Details

Risk is updated

22784 - (SYM17-014) Install Norton Security Certificate Spoof Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: Medium
CVE: CVE-2017-15528

Update Details
Risk is updated

96048 - Fedora Linux 25 FEDORA-2017-ab57a100f3 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7500, CVE-2017-7501

Update Details
Risk is updated

192842 - Fedora Linux 26 FEDORA-2017-9232eac8e8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7500, CVE-2017-7501

Update Details
Risk is updated

182531 - FreeBSD cURL Multiple Vulnerabilities (301a01b7-d50e-11e7-ac58-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2017-8816, CVE-2017-8817, CVE-2017-8818

Update Details
FASLScript is updated

70046 - macosx.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category
Risk Level: Informational
CVE: CVE-MAP-NOMATCH

Update Details
FASLScript is updated

DELETED CHECKS

21678 - (VMSA-2017-0006) VMware ESXi Privilege Escalation Vulnerability (CVE-2017-4903)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server
Risk Level: High

CVE: CVE-2017-4903

21680 - (VMSA-2017-0006) VMware ESXi Privilege Escalation Vulnerability (CVE-2017-4904)

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

Risk Level: High

CVE: CVE-2017-4904

21682 - (VMSA-2017-0006) VMware ESXi Information Disclosure Vulnerability (CVE-2017-4905)

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

Risk Level: Medium

CVE: CVE-2017-4905

ADDITIONAL NOTES

- 21678 - is deleted due to FP in certain situations.
- 21680 - is deleted due to FP in certain situations.
- 21682 - is deleted due to FP in certain situations.

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.