2017-SEP-21
FSL version 7.5.960

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

22409 - Moxa SoftCMS Live Viewer Security Bypass Vulnerability Prior To 1.7

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

Risk Level: High

CVE: CVE-2017-12729

Description

A SQL injection vulnerability is present in some versions of Moxa SoftCMS.

Observation

Moxa SoftCMS is an IP surveillance software.

A SQL injection vulnerability is present in some versions of Moxa SoftCMS. The flaw is due to an improper sanitization of elements used in an SQL command. Successful exploitation could allow an attacker to gain access SoftCMS.

22445 - Advantech WebAccess Multiple Vulnerabilities Prior To 8.2.20170817

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

Risk Level: High

CVE: CVE-2017-12698, CVE-2017-12702, CVE-2017-12704, CVE-2017-12706, CVE-2017-12708, CVE-2017-12710, CVE-2017-12711, CVE-2017-12713, CVE-2017-12717

Description

Multiple vulnerabilities are present in some versions of Advantech WebAccess.

Observation

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

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

22456 - Google Chrome Multiple Vulnerabilities Prior To 61.0.3163.79

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

Risk Level: High

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation allows an attacker to execute arbitrary code.

22457 - Google Chrome Multiple Vulnerabilities Prior To 61.0.3163.79

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation allows an attacker to execute arbitrary code.

141716 - Red Hat Enterprise Linux RHSA-2017-2732 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-7895

Description

The scan detected that the host is missing the following update:
RHSA-2017-2732

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00040.html

RHEL6_2S
x86_64
kernel-2.6.32-220.75.1.el6
kernel-debug-devel-2.6.32-220.75.1.el6
perf-2.6.32-220.75.1.el6
python-perf-2.6.32-220.75.1.el6
kernel-headers-2.6.32-220.75.1.el6
perf-debuginfo-2.6.32-220.75.1.el6
kernel-debug-2.6.32-220.75.1.el6
kernel-debuginfo-common-x86_64-2.6.32-220.75.1.el6
kernel-debuginfo-2.6.32-220.75.1.el6
kernel-debug-debuginfo-2.6.32-220.75.1.el6
kernel-devel-2.6.32-220.75.1.el6
python-perf-debuginfo-2.6.32-220.75.1.el6

noarch
kernel-doc-2.6.32-220.75.1.el6

kernel-firmware-2.6.32-220.75.1.el6

185879 - Ubuntu Linux 16.04 USN-3420-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-10663, CVE-2017-12762, CVE-2017-8831

Description

The scan detected that the host is missing the following update:
USN-3420-1

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-September/004051.html

Ubuntu 16.04

linux-image-4.4.0-1076-snapdragon_4.4.0-1076.81
linux-image-4.4.0-96-powerpc-smp_4.4.0-96.119
linux-image-4.4.0-96-powerpc64-smp_4.4.0-96.119
linux-image-aws_4.4.0.1035.37
linux-image-generic-lpae_4.4.0.96.101
linux-image-4.4.0-1031-gke_4.4.0-1031.31
linux-image-snapdragon_4.4.0.1076.68
linux-image-4.4.0-96-generic_4.4.0-96.119
linux-image-4.4.0-1007-kvm_4.4.0-1007.12
linux-image-generic_4.4.0.96.101
linux-image-lowlatency_4.4.0.96.101
linux-image-powerpc-e500mc_4.4.0.96.101
linux-image-4.4.0-96-powerpc64-emb_4.4.0-96.119
linux-image-4.4.0-96-lowlatency_4.4.0-96.119
linux-image-4.4.0-96-generic-lpae_4.4.0-96.119
linux-image-4.4.0-96-powerpc-e500mc_4.4.0-96.119
linux-image-powerpc64-smp_4.4.0.96.101
linux-image-4.4.0-1074-raspi2_4.4.0-1074.82
linux-image-powerpc-smp_4.4.0.96.101
linux-image-gke_4.4.0.1031.32
linux-image-kvm_4.4.0.1007.7
linux-image-powerpc64-emb_4.4.0.96.101
linux-image-raspi2_4.4.0.1074.74
linux-image-4.4.0-1035-aws_4.4.0-1035.44

185886 - Ubuntu Linux 14.04 USN-3420-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-10663, CVE-2017-12762, CVE-2017-8831

Description

The scan detected that the host is missing the following update:
USN-3420-2

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-September/004055.html

Ubuntu 14.04

linux-image-powerpc-e500mc-lts-xenial_4.4.0.96.80
linux-image-4.4.0-96-lowlatency_4.4.0-96.119~14.04.1
linux-image-4.4.0-96-powerpc64-emb_4.4.0-96.119~14.04.1
linux-image-4.4.0-96-generic-lpae_4.4.0-96.119~14.04.1
linux-image-powerpc-smp-lts-xenial_4.4.0.96.80
linux-image-generic-lpae-lts-xenial_4.4.0.96.80
linux-image-powerpc64-emb-lts-xenial_4.4.0.96.80
linux-image-4.4.0-96-generic_4.4.0-96.119~14.04.1
linux-image-4.4.0-96-powerpc-e500mc_4.4.0-96.119~14.04.1
linux-image-generic-lts-xenial_4.4.0.96.80
linux-image-powerpc64-smp-lts-xenial_4.4.0.96.80
linux-image-lowlatency-lts-xenial_4.4.0.96.80
linux-image-4.4.0-96-powerpc-smp_4.4.0-96.119~14.04.1
linux-image-4.4.0-96-powerpc64-smp_4.4.0-96.119~14.04.1

178493 - Gentoo Linux GLSA-201709-13 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7692

Description

The scan detected that the host is missing the following update:
GLSA-201709-13

Observation

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

https://security.gentoo.org/glsa/201709-13

Affected packages:
mail-client/squirrelmail < 1.4.23_pre20140426

182443 - FreeBSD GitLab Multiple Vulnerabilities (6a177c87-9933-11e7-93f7-d43d7e971a1b)

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

Risk Level: High

CVE: CVE-2016-4738, CVE-2017-5029

Description

The scan detected that the host is missing the following update:
GitLab -- multiple vulnerabilities (6a177c87-9933-11e7-93f7-d43d7e971a1b)

Observation

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

http://www.vuxml.org/freebsd/6a177c87-9933-11e7-93f7-d43d7e971a1b.html

Affected packages:
1.0.0 <= gitlab <= 9.3.10
9.4.0 <= gitlab <= 9.4.5
9.5.0 <= gitlab <= 9.5.3

22439 - IBM AIX Java Multiple Vulnerabilities (July 2017)

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

Risk Level: High

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10078, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10105, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10115, CVE-2017-10116, CVE-2017-10125, CVE-2017-10243, CVE-2017-1376, CVE-2017-1541

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.

141715 - Red Hat Enterprise Linux RHSA-2017-2760 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583

Description

The scan detected that the host is missing the following update:
RHSA-2017-2760

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00044.html

RHEL6_7S
i386
perf-debuginfo-2.6.32-573.47.1.el6
kernel-debuginfo-2.6.32-573.47.1.el6
kernel-debuginfo-common-i686-2.6.32-573.47.1.el6
kernel-2.6.32-573.47.1.el6
kernel-debug-debuginfo-2.6.32-573.47.1.el6
python-perf-2.6.32-573.47.1.el6
kernel-debug-2.6.32-573.47.1.el6
perf-2.6.32-573.47.1.el6
python-perf-debuginfo-2.6.32-573.47.1.el6
kernel-devel-2.6.32-573.47.1.el6
kernel-debug-devel-2.6.32-573.47.1.el6
kernel-headers-2.6.32-573.47.1.el6

noarch
kernel-firmware-2.6.32-573.47.1.el6

kernel-abi-whitelists-2.6.32-573.47.1.el6
kernel-doc-2.6.32-573.47.1.el6

x86_64
kernel-debug-2.6.32-573.47.1.el6
kernel-debug-debuginfo-2.6.32-573.47.1.el6
kernel-debug-devel-2.6.32-573.47.1.el6
python-perf-2.6.32-573.47.1.el6
kernel-debuginfo-2.6.32-573.47.1.el6
perf-debuginfo-2.6.32-573.47.1.el6
python-perf-debuginfo-2.6.32-573.47.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.47.1.el6
kernel-debuginfo-common-i686-2.6.32-573.47.1.el6
perf-2.6.32-573.47.1.el6
kernel-2.6.32-573.47.1.el6
kernel-devel-2.6.32-573.47.1.el6
kernel-headers-2.6.32-573.47.1.el6

141717 - Red Hat Enterprise Linux RHSA-2017-2728 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547

Description

The scan detected that the host is missing the following update:
RHSA-2017-2728

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00039.html

RHEL7D
x86_64
postgresql-contrib-9.2.23-1.el7_4
postgresql-pltcl-9.2.23-1.el7_4
postgresql-test-9.2.23-1.el7_4
postgresql-devel-9.2.23-1.el7_4
postgresql-static-9.2.23-1.el7_4
postgresql-plpython-9.2.23-1.el7_4
postgresql-upgrade-9.2.23-1.el7_4
postgresql-debuginfo-9.2.23-1.el7_4
postgresql-plperl-9.2.23-1.el7_4
postgresql-docs-9.2.23-1.el7_4
postgresql-server-9.2.23-1.el7_4
postgresql-libs-9.2.23-1.el7_4
postgresql-9.2.23-1.el7_4

RHEL7S
x86_64
postgresql-contrib-9.2.23-1.el7_4
postgresql-pltcl-9.2.23-1.el7_4
postgresql-test-9.2.23-1.el7_4
postgresql-devel-9.2.23-1.el7_4
postgresql-static-9.2.23-1.el7_4
postgresql-plpython-9.2.23-1.el7_4

postgresql-upgrade-9.2.23-1.el7_4
postgresql-debuginfo-9.2.23-1.el7_4
postgresql-plperl-9.2.23-1.el7_4
postgresql-docs-9.2.23-1.el7_4
postgresql-server-9.2.23-1.el7_4
postgresql-libs-9.2.23-1.el7_4
postgresql-9.2.23-1.el7_4

RHEL7WS
x86_64
postgresql-contrib-9.2.23-1.el7_4
postgresql-pltcl-9.2.23-1.el7_4
postgresql-test-9.2.23-1.el7_4
postgresql-devel-9.2.23-1.el7_4
postgresql-static-9.2.23-1.el7_4
postgresql-plpython-9.2.23-1.el7_4
postgresql-upgrade-9.2.23-1.el7_4
postgresql-debuginfo-9.2.23-1.el7_4
postgresql-plperl-9.2.23-1.el7_4
postgresql-docs-9.2.23-1.el7_4
postgresql-server-9.2.23-1.el7_4
postgresql-libs-9.2.23-1.el7_4
postgresql-9.2.23-1.el7_4

141718 - Red Hat Enterprise Linux RHSA-2017-2771 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
RHSA-2017-2771

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00046.html

RHEL7D
x86_64
emacs-nox-24.3-20.el7_4
emacs-common-24.3-20.el7_4
emacs-24.3-20.el7_4
emacs-debuginfo-24.3-20.el7_4

noarch
emacs-el-24.3-20.el7_4
emacs-filesystem-24.3-20.el7_4
emacs-terminal-24.3-20.el7_4

RHEL7S
noarch
emacs-el-24.3-20.el7_4
emacs-filesystem-24.3-20.el7_4
emacs-terminal-24.3-20.el7_4

x86_64
emacs-nox-24.3-20.el7_4
emacs-common-24.3-20.el7_4
emacs-24.3-20.el7_4
emacs-debuginfo-24.3-20.el7_4

RHEL7WS
x86_64
emacs-nox-24.3-20.el7_4
emacs-common-24.3-20.el7_4
emacs-24.3-20.el7_4
emacs-debuginfo-24.3-20.el7_4

noarch
emacs-el-24.3-20.el7_4
emacs-filesystem-24.3-20.el7_4
emacs-terminal-24.3-20.el7_4

141719 - Red Hat Enterprise Linux RHSA-2017-2731 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
RHSA-2017-2731

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00041.html

RHEL6_6S
x86_64
perf-2.6.32-504.63.2.el6
perf-debuginfo-2.6.32-504.63.2.el6
kernel-debuginfo-2.6.32-504.63.2.el6
kernel-debug-devel-2.6.32-504.63.2.el6
kernel-2.6.32-504.63.2.el6
kernel-debug-2.6.32-504.63.2.el6
kernel-debuginfo-common-x86_64-2.6.32-504.63.2.el6
kernel-devel-2.6.32-504.63.2.el6
kernel-headers-2.6.32-504.63.2.el6
python-perf-2.6.32-504.63.2.el6
python-perf-debuginfo-2.6.32-504.63.2.el6
kernel-debug-debuginfo-2.6.32-504.63.2.el6

noarch
kernel-doc-2.6.32-504.63.2.el6
kernel-abi-whitelists-2.6.32-504.63.2.el6
kernel-firmware-2.6.32-504.63.2.el6

145919 - SuSE Linux 42.3 openSUSE-SU-2017:2514-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14316, CVE-2017-14317, CVE-2017-14318, CVE-2017-14319

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2514-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00081.html

SuSE Linux 42.3
x86_64
xen-4.9.0_12-7.1
xen-tools-domU-4.9.0_12-7.1
xen-devel-4.9.0_12-7.1
xen-debugsource-4.9.0_12-7.1
xen-tools-domU-debuginfo-4.9.0_12-7.1
xen-tools-4.9.0_12-7.1
xen-doc-html-4.9.0_12-7.1
xen-libs-4.9.0_12-7.1
xen-tools-debuginfo-4.9.0_12-7.1
xen-libs-debuginfo-4.9.0_12-7.1

145920 - SuSE Linux 42.2 openSUSE-SU-2017:2495-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-11472, CVE-2017-12134, CVE-2017-14051, CVE-2017-14106

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2495-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00074.html

SuSE Linux 42.2
x86_64
kernel-debug-devel-4.4.87-18.29.1
kernel-default-debuginfo-4.4.87-18.29.1
kernel-debug-4.4.87-18.29.1
kernel-vanilla-base-debuginfo-4.4.87-18.29.1
kernel-vanilla-debuginfo-4.4.87-18.29.1
kernel-debug-base-4.4.87-18.29.1
kernel-default-devel-4.4.87-18.29.1
kernel-vanilla-4.4.87-18.29.1
kernel-syms-4.4.87-18.29.1
kernel-obs-qa-4.4.87-18.29.1
kernel-default-base-debuginfo-4.4.87-18.29.1
kernel-obs-build-4.4.87-18.29.1
kernel-default-4.4.87-18.29.1

kernel-default-debugsource-4.4.87-18.29.1
kernel-debug-debuginfo-4.4.87-18.29.1
kernel-obs-build-debugsource-4.4.87-18.29.1
kernel-vanilla-devel-4.4.87-18.29.1
kernel-debug-base-debuginfo-4.4.87-18.29.1
kernel-default-base-4.4.87-18.29.1
kernel-debug-debugsource-4.4.87-18.29.1
kernel-vanilla-base-4.4.87-18.29.1
kernel-debug-devel-debuginfo-4.4.87-18.29.1
kernel-vanilla-debugsource-4.4.87-18.29.1

noarch
kernel-macros-4.4.87-18.29.1
kernel-docs-pdf-4.4.87-18.29.2
kernel-docs-4.4.87-18.29.2
kernel-devel-4.4.87-18.29.1
kernel-source-4.4.87-18.29.1
kernel-docs-html-4.4.87-18.29.2
kernel-source-vanilla-4.4.87-18.29.1

145923 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2491-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2491-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00070.html

SuSE Linux 42.2
x86_64
chromedriver-debuginfo-61.0.3163.79-104.24.1
chromium-debuginfo-61.0.3163.79-104.24.1
chromium-61.0.3163.79-104.24.1
chromium-debugsource-61.0.3163.79-104.24.1
chromedriver-61.0.3163.79-104.24.1

SuSE Linux 42.3
x86_64
chromium-debuginfo-61.0.3163.79-110.1
chromedriver-debuginfo-61.0.3163.79-110.1
chromium-debugsource-61.0.3163.79-110.1
chromium-61.0.3163.79-110.1
chromedriver-61.0.3163.79-110.1

145924 - SuSE Linux 42.2 openSUSE-SU-2017:2501-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11399, CVE-2017-14054, CVE-2017-14055, CVE-2017-14056, CVE-2017-14057, CVE-2017-14058, CVE-2017-14059, CVE-2017-14169, CVE-2017-14170, CVE-2017-14171, CVE-2017-14222, CVE-2017-14223, CVE-2017-14225

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2501-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00076.html

SuSE Linux 42.2
x86_64
libavresample2-debuginfo-32bit-2.8.13-25.10.1
libavutil54-debuginfo-32bit-2.8.13-25.10.1
libavformat56-debuginfo-32bit-2.8.13-25.10.1
libpostproc53-debuginfo-32bit-2.8.13-25.10.1
ffmpeg-debugsource-3.3.4-6.16.1
libpostproc54-debuginfo-3.3.4-6.16.1
libavdevice56-2.8.13-25.10.1
libmp3lame0-32bit-3.99.5-2.1
ffmpeg-debuginfo-3.3.4-6.16.1
libavdevice56-debuginfo-32bit-2.8.13-25.10.1
libavformat56-debuginfo-2.8.13-25.10.1
libavcodec56-32bit-2.8.13-25.10.1
libtwolame0-debuginfo-32bit-0.3.13-2.1
twolame-debuginfo-0.3.13-2.1
lame-doc-3.99.5-2.1
libpostproc53-2.8.13-25.10.1
libavfilter5-2.8.13-25.10.1
libavcodec57-debuginfo-3.3.4-6.16.1
libavdevice56-debuginfo-2.8.13-25.10.1
libavformat57-debuginfo-3.3.4-6.16.1
libswresample2-debuginfo-3.3.4-6.16.1
libswresample2-debuginfo-32bit-3.3.4-6.16.1
libswscale3-32bit-2.8.13-25.10.1
libavutil54-2.8.13-25.10.1
libavformat57-32bit-3.3.4-6.16.1
libswresample1-debuginfo-32bit-2.8.13-25.10.1
libavformat57-debuginfo-32bit-3.3.4-6.16.1
libtwolame-devel-0.3.13-2.1
libswresample-devel-3.3.4-6.16.1
libavutil-devel-3.3.4-6.16.1
libswscale4-debuginfo-32bit-3.3.4-6.16.1
libavfilter6-32bit-3.3.4-6.16.1
libmp3lame-devel-3.99.5-2.1
libavresample3-32bit-3.3.4-6.16.1
libavfilter-devel-3.3.4-6.16.1
libavformat-devel-3.3.4-6.16.1
libavutil54-32bit-2.8.13-25.10.1
libswscale4-3.3.4-6.16.1
libavdevice56-32bit-2.8.13-25.10.1
libavcodec-devel-3.3.4-6.16.1
libswscale3-debuginfo-32bit-2.8.13-25.10.1
libavcodec57-32bit-3.3.4-6.16.1
libavfilter5-debuginfo-2.8.13-25.10.1
libavfilter6-3.3.4-6.16.1

libavresample3-debuginfo-32bit-3.3.4-6.16.1
lame-debuginfo-3.99.5-2.1
libswresample1-32bit-2.8.13-25.10.1
libtwolame0-debuginfo-0.3.13-2.1
ffmpeg-3.3.4-6.16.1
libavutil54-debuginfo-2.8.13-25.10.1
libavdevice-devel-3.3.4-6.16.1
libpostproc53-32bit-2.8.13-25.10.1
libswresample2-3.3.4-6.16.1
libavformat56-2.8.13-25.10.1
libavutil55-3.3.4-6.16.1
libpostproc54-32bit-3.3.4-6.16.1
libavresample2-2.8.13-25.10.1
libavdevice57-debuginfo-3.3.4-6.16.1
twolame-debugsource-0.3.13-2.1
libavfilter6-debuginfo-3.3.4-6.16.1
libswscale-devel-3.3.4-6.16.1
libavdevice57-debuginfo-32bit-3.3.4-6.16.1
libavformat57-3.3.4-6.16.1
libavcodec57-3.3.4-6.16.1
libavfilter5-32bit-2.8.13-25.10.1
libavutil55-debuginfo-3.3.4-6.16.1
ffmpeg2-devel-2.8.13-25.10.1
libpostproc54-3.3.4-6.16.1
libmp3lame0-3.99.5-2.1
libavcodec56-2.8.13-25.10.1
libmp3lame0-debuginfo-3.99.5-2.1
libavresample2-32bit-2.8.13-25.10.1
libswresample1-2.8.13-25.10.1
libavresample3-debuginfo-3.3.4-6.16.1
libavdevice57-32bit-3.3.4-6.16.1
libavresample2-debuginfo-2.8.13-25.10.1
libpostproc54-debuginfo-32bit-3.3.4-6.16.1
libswscale3-2.8.13-25.10.1
libpostproc-devel-3.3.4-6.16.1
libavutil55-debuginfo-32bit-3.3.4-6.16.1
twolame-0.3.13-2.1
libtwolame0-32bit-0.3.13-2.1
libavcodec56-debuginfo-2.8.13-25.10.1
libavcodec57-debuginfo-32bit-3.3.4-6.16.1
libavfilter5-debuginfo-32bit-2.8.13-25.10.1
lame-3.99.5-2.1
lame-debugsource-3.99.5-2.1
lame-mp3rtp-debuginfo-3.99.5-2.1
libavresample-devel-3.3.4-6.16.1
lame-mp3rtp-3.99.5-2.1
libavdevice57-3.3.4-6.16.1
libavresample3-3.3.4-6.16.1
libavfilter6-debuginfo-32bit-3.3.4-6.16.1
libtwolame0-0.3.13-2.1
libmp3lame0-debuginfo-32bit-3.99.5-2.1
libavutil55-32bit-3.3.4-6.16.1
libswresample2-32bit-3.3.4-6.16.1
libavcodec56-debuginfo-32bit-2.8.13-25.10.1
libpostproc53-debuginfo-2.8.13-25.10.1
libavformat56-32bit-2.8.13-25.10.1
libswscale3-debuginfo-2.8.13-25.10.1
libswresample1-debuginfo-2.8.13-25.10.1
libswscale4-debuginfo-3.3.4-6.16.1
ffmpeg2-debugsource-2.8.13-25.10.1

libswscale4-32bit-3.3.4-6.16.1

i586
ffmpeg-debugsource-3.3.4-6.16.1
libpostproc54-debuginfo-3.3.4-6.16.1
libavdevice56-2.8.13-25.10.1
ffmpeg-debuginfo-3.3.4-6.16.1
libavformat56-debuginfo-2.8.13-25.10.1
twolame-debuginfo-0.3.13-2.1
lame-doc-3.99.5-2.1
libpostproc53-2.8.13-25.10.1
libavfilter5-2.8.13-25.10.1
libavcodec57-debuginfo-3.3.4-6.16.1
libavdevice56-debuginfo-2.8.13-25.10.1
libavformat57-debuginfo-3.3.4-6.16.1
libswresample2-debuginfo-3.3.4-6.16.1
libavutil54-2.8.13-25.10.1
libtwolame-devel-0.3.13-2.1
libswresample-devel-3.3.4-6.16.1
libavutil-devel-3.3.4-6.16.1
libmp3lame-devel-3.99.5-2.1
libavfilter-devel-3.3.4-6.16.1
libavformat-devel-3.3.4-6.16.1
libswscale4-3.3.4-6.16.1
libavcodec-devel-3.3.4-6.16.1
libavfilter5-debuginfo-2.8.13-25.10.1
libavfilter6-3.3.4-6.16.1
lame-debuginfo-3.99.5-2.1
libtwolame0-debuginfo-0.3.13-2.1
ffmpeg-3.3.4-6.16.1
libavutil54-debuginfo-2.8.13-25.10.1
libavdevice-devel-3.3.4-6.16.1
libswresample2-3.3.4-6.16.1
libavformat56-2.8.13-25.10.1
libavutil55-3.3.4-6.16.1
libavresample2-2.8.13-25.10.1
libavdevice57-debuginfo-3.3.4-6.16.1
twolame-debugsource-0.3.13-2.1
libavfilter6-debuginfo-3.3.4-6.16.1
libswscale-devel-3.3.4-6.16.1
libavformat57-3.3.4-6.16.1
libavcodec57-3.3.4-6.16.1
libavutil55-debuginfo-3.3.4-6.16.1
ffmpeg2-devel-2.8.13-25.10.1
libpostproc54-3.3.4-6.16.1
libmp3lame0-3.99.5-2.1
libavcodec56-2.8.13-25.10.1
libmp3lame0-debuginfo-3.99.5-2.1
libswresample1-2.8.13-25.10.1
libavresample3-debuginfo-3.3.4-6.16.1
libavresample2-debuginfo-2.8.13-25.10.1
libswscale3-2.8.13-25.10.1
libpostproc-devel-3.3.4-6.16.1
twolame-0.3.13-2.1
libavcodec56-debuginfo-2.8.13-25.10.1
lame-3.99.5-2.1
lame-debugsource-3.99.5-2.1
lame-mp3rtp-debuginfo-3.99.5-2.1
libavresample-devel-3.3.4-6.16.1
lame-mp3rtp-3.99.5-2.1

libavdevice57-3.3.4-6.16.1
libavresample3-3.3.4-6.16.1
libtwolame0-0.3.13-2.1
libpostproc53-debuginfo-2.8.13-25.10.1
libswscale3-debuginfo-2.8.13-25.10.1
libswresample1-debuginfo-2.8.13-25.10.1
libswscale4-debuginfo-3.3.4-6.16.1
ffmpeg2-debugsource-2.8.13-25.10.1

145925 - SuSE Linux 42.3 openSUSE-SU-2017:2502-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10190, CVE-2016-10191, CVE-2016-10192, CVE-2016-9561, CVE-2017-11399, CVE-2017-14054, CVE-2017-14055, CVE-2017-14056, CVE-2017-14057, CVE-2017-14058, CVE-2017-14059, CVE-2017-14169, CVE-2017-14170, CVE-2017-14171, CVE-2017-14222, CVE-2017-14223, CVE-2017-14225, CVE-2017-7863, CVE-2017-7865, CVE-2017-7866

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2502-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00077.html

SuSE Linux 42.3
x86_64
libavcodec57-32bit-3.3.4-7.1
libswresample1-2.8.13-32.1
libavutil54-debuginfo-32bit-2.8.13-32.1
libavdevice56-32bit-2.8.13-32.1
libavformat56-debuginfo-2.8.13-32.1
libmp3lame0-32bit-3.99.5-2.1
libavdevice57-32bit-3.3.4-7.1
libavcodec57-debuginfo-32bit-3.3.4-7.1
libavformat56-debuginfo-32bit-2.8.13-32.1
libavresample-devel-3.3.4-7.1
libavcodec56-32bit-2.8.13-32.1
ffmpeg-3.3.4-7.1
lame-doc-3.99.5-2.1
libswscale4-debuginfo-3.3.4-7.1
libavcodec56-2.8.13-32.1
libpostproc53-32bit-2.8.13-32.1
libavresample3-3.3.4-7.1
libswresample1-32bit-2.8.13-32.1
libavcodec-devel-3.3.4-7.1
libavresample2-debuginfo-2.8.13-32.1
libpostproc53-2.8.13-32.1
libavfilter5-debuginfo-2.8.13-32.1
libavdevice-devel-3.3.4-7.1
libavformat57-debuginfo-3.3.4-7.1
libavformat57-3.3.4-7.1
libavresample2-2.8.13-32.1
libpostproc53-debuginfo-32bit-2.8.13-32.1
libavdevice56-debuginfo-32bit-2.8.13-32.1
libavdevice57-debuginfo-32bit-3.3.4-7.1

libavfilter5-32bit-2.8.13-32.1
libavdevice56-debuginfo-2.8.13-32.1
libmp3lame-devel-3.99.5-2.1
libavfilter6-debuginfo-3.3.4-7.1
libavfilter6-debuginfo-32bit-3.3.4-7.1
libavdevice56-2.8.13-32.1
libpostproc54-32bit-3.3.4-7.1
ffmpeg2-debugsource-2.8.13-32.1
libavresample2-32bit-2.8.13-32.1
libswscale-devel-3.3.4-7.1
libswscale3-debuginfo-32bit-2.8.13-32.1
libavresample2-debuginfo-32bit-2.8.13-32.1
libswscale4-debuginfo-32bit-3.3.4-7.1
libswresample1-debuginfo-32bit-2.8.13-32.1
libavcodec56-debuginfo-2.8.13-32.1
ffmpeg-debuginfo-3.3.4-7.1
lame-debuginfo-3.99.5-2.1
libtwolame0-debuginfo-0.3.13-2.1
libswresample2-debuginfo-32bit-3.3.4-7.1
libavfilter5-debuginfo-32bit-2.8.13-32.1
twolame-debugsource-0.3.13-2.1
libavutil54-debuginfo-2.8.13-32.1
libavresample3-32bit-3.3.4-7.1
libavcodec57-debuginfo-3.3.4-7.1
libavutil55-3.3.4-7.1
libswresample-devel-3.3.4-7.1
libavutil55-debuginfo-32bit-3.3.4-7.1
libswresample2-debuginfo-3.3.4-7.1
libavcodec56-debuginfo-32bit-2.8.13-32.1
ffmpeg-debugsource-3.3.4-7.1
libavdevice57-debuginfo-3.3.4-7.1
libmp3lame0-debuginfo-32bit-3.99.5-2.1
libswscale3-debuginfo-2.8.13-32.1
libavformat57-32bit-3.3.4-7.1
twolame-debuginfo-0.3.13-2.1
libtwolame0-debuginfo-32bit-0.3.13-2.1
libswresample2-3.3.4-7.1
libswresample2-32bit-3.3.4-7.1
libavresample3-debuginfo-3.3.4-7.1
libavfilter-devel-3.3.4-7.1
libmp3lame0-3.99.5-2.1
libpostproc54-3.3.4-7.1
libmp3lame0-debuginfo-3.99.5-2.1
libswscale3-32bit-2.8.13-32.1
libpostproc-devel-3.3.4-7.1
libavutil54-2.8.13-32.1
libavformat57-debuginfo-32bit-3.3.4-7.1
libpostproc54-debuginfo-32bit-3.3.4-7.1
libavresample3-debuginfo-32bit-3.3.4-7.1
libswscale4-3.3.4-7.1
libswresample1-debuginfo-2.8.13-32.1
twolame-0.3.13-2.1
libswscale4-32bit-3.3.4-7.1
libtwolame-devel-0.3.13-2.1
libavformat56-2.8.13-32.1
libavutil55-32bit-3.3.4-7.1
libavformat56-32bit-2.8.13-32.1
libavutil-devel-3.3.4-7.1
lame-3.99.5-2.1
lame-debugsource-3.99.5-2.1

lame-mp3rtp-debuginfo-3.99.5-2.1
lame-mp3rtp-3.99.5-2.1
libpostproc53-debuginfo-2.8.13-32.1
ffmpeg2-devel-2.8.13-32.1
libavfilter6-3.3.4-7.1
libavdevice57-3.3.4-7.1
libavutil54-32bit-2.8.13-32.1
libavformat-devel-3.3.4-7.1
libtwolame0-32bit-0.3.13-2.1
libpostproc54-debuginfo-3.3.4-7.1
libswscale3-2.8.13-32.1
libavcodec57-3.3.4-7.1
libavfilter6-32bit-3.3.4-7.1
libavutil55-debuginfo-3.3.4-7.1
libtwolame0-0.3.13-2.1
libavfilter5-2.8.13-32.1

i586
libswresample1-2.8.13-32.1
libavformat56-debuginfo-2.8.13-32.1
libavresample-devel-3.3.4-7.1
ffmpeg-3.3.4-7.1
lame-doc-3.99.5-2.1
libswscale4-debuginfo-3.3.4-7.1
libavcodec56-2.8.13-32.1
libavresample3-3.3.4-7.1
libavcodec-devel-3.3.4-7.1
libavresample2-debuginfo-2.8.13-32.1
libpostproc53-2.8.13-32.1
libavfilter5-debuginfo-2.8.13-32.1
libavdevice-devel-3.3.4-7.1
libavformat57-debuginfo-3.3.4-7.1
libavformat57-3.3.4-7.1
libavresample2-2.8.13-32.1
libavdevice56-debuginfo-2.8.13-32.1
libmp3lame-devel-3.99.5-2.1
libavfilter6-debuginfo-3.3.4-7.1
libavdevice56-2.8.13-32.1
ffmpeg2-debugsource-2.8.13-32.1
libswscale-devel-3.3.4-7.1
libavcodec56-debuginfo-2.8.13-32.1
ffmpeg-debuginfo-3.3.4-7.1
lame-debuginfo-3.99.5-2.1
libtwolame0-debuginfo-0.3.13-2.1
twolame-debugsource-0.3.13-2.1
libavutil54-debuginfo-2.8.13-32.1
libavcodec57-debuginfo-3.3.4-7.1
libavutil55-3.3.4-7.1
libswresample-devel-3.3.4-7.1
libswresample2-debuginfo-3.3.4-7.1
ffmpeg-debugsource-3.3.4-7.1
libavdevice57-debuginfo-3.3.4-7.1
libswscale3-debuginfo-2.8.13-32.1
twolame-debuginfo-0.3.13-2.1
libswresample2-3.3.4-7.1
libavresample3-debuginfo-3.3.4-7.1
libavfilter-devel-3.3.4-7.1
libmp3lame0-3.99.5-2.1
libpostproc54-3.3.4-7.1
libmp3lame0-debuginfo-3.99.5-2.1

libpostproc-devel-3.3.4-7.1
libavutil54-2.8.13-32.1
libswscale4-3.3.4-7.1
libswresample1-debuginfo-2.8.13-32.1
twolame-0.3.13-2.1
libtwolame-devel-0.3.13-2.1
libavformat56-2.8.13-32.1
libavutil-devel-3.3.4-7.1
lame-3.99.5-2.1
lame-debugsource-3.99.5-2.1
lame-mp3rtp-debuginfo-3.99.5-2.1
lame-mp3rtp-3.99.5-2.1
libpostproc53-debuginfo-2.8.13-32.1
ffmpeg2-devel-2.8.13-32.1
libavfilter6-3.3.4-7.1
libavdevice57-3.3.4-7.1
libavformat-devel-3.3.4-7.1
libpostproc54-debuginfo-3.3.4-7.1
libswscale3-2.8.13-32.1
libavcodec57-3.3.4-7.1
libavutil55-debuginfo-3.3.4-7.1
libtwolame0-0.3.13-2.1
libavfilter5-2.8.13-32.1

145927 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2488-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8947, CVE-2016-10327, CVE-2016-2052, CVE-2017-7870, CVE-2017-7882, CVE-2017-8358, CVE-2017-9433

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2488-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00065.html

SuSE Linux 42.2
x86_64
libreoffice-sdk-debuginfo-5.3.5.2-18.9.4
libreoffice-calc-5.3.5.2-18.9.4
libreoffice-writer-5.3.5.2-18.9.4
libreoffice-draw-5.3.5.2-18.9.4
libreoffice-impress-5.3.5.2-18.9.4
libreoffice-officebean-debuginfo-5.3.5.2-18.9.4
libreoffice-kde4-debuginfo-5.3.5.2-18.9.4
libreoffice-base-drivers-mysql-5.3.5.2-18.9.4
libreofficekit-5.3.5.2-18.9.4
libreoffice-mailmerge-5.3.5.2-18.9.4
libreoffice-filters-optional-5.3.5.2-18.9.4
libreofficekit-devel-5.3.5.2-18.9.4
libreoffice-debuginfo-5.3.5.2-18.9.4
libreoffice-pyuno-debuginfo-5.3.5.2-18.9.4
libreoffice-base-drivers-postgresql-5.3.5.2-18.9.4
libreoffice-draw-debuginfo-5.3.5.2-18.9.4

libreoffice-debugsource-5.3.5.2-18.9.4
libreoffice-gtk3-5.3.5.2-18.9.4
libreoffice-math-5.3.5.2-18.9.4
libreoffice-base-debuginfo-5.3.5.2-18.9.4
libreoffice-calc-extensions-5.3.5.2-18.9.4
libreoffice-gtk3-debuginfo-5.3.5.2-18.9.4
libreoffice-5.3.5.2-18.9.4
libreoffice-pyuno-5.3.5.2-18.9.4
libreoffice-base-drivers-postgresql-debuginfo-5.3.5.2-18.9.4
libreoffice-calc-debuginfo-5.3.5.2-18.9.4
libreoffice-officebean-5.3.5.2-18.9.4
libreoffice-writer-debuginfo-5.3.5.2-18.9.4
libreoffice-gnome-5.3.5.2-18.9.4
libreoffice-sdk-5.3.5.2-18.9.4
libreoffice-base-drivers-mysql-debuginfo-5.3.5.2-18.9.4
libreoffice-impress-debuginfo-5.3.5.2-18.9.4
libreoffice-gnome-debuginfo-5.3.5.2-18.9.4
libreoffice-sdk-doc-5.3.5.2-18.9.4
libreoffice-kde4-5.3.5.2-18.9.4
libreoffice-writer-extensions-5.3.5.2-18.9.4
libreoffice-math-debuginfo-5.3.5.2-18.9.4
libreoffice-base-5.3.5.2-18.9.4

noarch
libreoffice-l10n-ru-5.3.5.2-18.9.4
libreoffice-l10n-as-5.3.5.2-18.9.4
libreoffice-l10n-cy-5.3.5.2-18.9.4
libreoffice-l10n-nr-5.3.5.2-18.9.4
libreoffice-l10n-cs-5.3.5.2-18.9.4
libreoffice-l10n-nn-5.3.5.2-18.9.4
libreoffice-l10n-xh-5.3.5.2-18.9.4
libreoffice-l10n-bg-5.3.5.2-18.9.4
libreoffice-l10n-pt_BR-5.3.5.2-18.9.4
libreoffice-l10n-ja-5.3.5.2-18.9.4
libreoffice-l10n-es-5.3.5.2-18.9.4
libreoffice-l10n-af-5.3.5.2-18.9.4
libreoffice-l10n-kn-5.3.5.2-18.9.4
libreoffice-l10n-ro-5.3.5.2-18.9.4
libreoffice-icon-theme-tango-5.3.5.2-18.9.4
libreoffice-l10n-zh_CN-5.3.5.2-18.9.4
libreoffice-l10n-sk-5.3.5.2-18.9.4
libreoffice-l10n-ss-5.3.5.2-18.9.4
libreoffice-l10n-de-5.3.5.2-18.9.4
libreoffice-l10n-th-5.3.5.2-18.9.4
libreoffice-l10n-si-5.3.5.2-18.9.4
libreoffice-l10n-ga-5.3.5.2-18.9.4
libreoffice-l10n-et-5.3.5.2-18.9.4
libreoffice-l10n-fa-5.3.5.2-18.9.4
libreoffice-l10n-mai-5.3.5.2-18.9.4
libreoffice-l10n-sv-5.3.5.2-18.9.4
libreoffice-l10n-br-5.3.5.2-18.9.4
libreoffice-l10n-ml-5.3.5.2-18.9.4
libreoffice-l10n-nb-5.3.5.2-18.9.4
libreoffice-icon-theme-oxygen-5.3.5.2-18.9.4
libreoffice-l10n-hr-5.3.5.2-18.9.4
libreoffice-l10n-st-5.3.5.2-18.9.4
libreoffice-l10n-sl-5.3.5.2-18.9.4
libreoffice-l10n-pa-5.3.5.2-18.9.4
libreoffice-l10n-ve-5.3.5.2-18.9.4
libreoffice-icon-theme-breeze-5.3.5.2-18.9.4

libreoffice-l10n-fr-5.3.5.2-18.9.4
libreoffice-branding-upstream-5.3.5.2-18.9.4
libreoffice-l10n-te-5.3.5.2-18.9.4
libreoffice-l10n-el-5.3.5.2-18.9.4
libreoffice-l10n-ko-5.3.5.2-18.9.4
libreoffice-l10n-lv-5.3.5.2-18.9.4
libreoffice-l10n-gl-5.3.5.2-18.9.4
libreoffice-l10n-dz-5.3.5.2-18.9.4
libreoffice-l10n-tr-5.3.5.2-18.9.4
libreoffice-l10n-eu-5.3.5.2-18.9.4
libreoffice-l10n-da-5.3.5.2-18.9.4
libreoffice-icon-theme-sifr-5.3.5.2-18.9.4
libreoffice-l10n-gu-5.3.5.2-18.9.4
libreoffice-l10n-hu-5.3.5.2-18.9.4
libreoffice-l10n-mr-5.3.5.2-18.9.4
libreoffice-l10n-pt_PT-5.3.5.2-18.9.4
libreoffice-l10n-en-5.3.5.2-18.9.4
libreoffice-gdb-pretty-printers-5.3.5.2-18.9.4
libreoffice-l10n-or-5.3.5.2-18.9.4
libreoffice-l10n-nl-5.3.5.2-18.9.4
libreoffice-l10n-he-5.3.5.2-18.9.4
libreoffice-l10n-ar-5.3.5.2-18.9.4
libreoffice-icon-theme-galaxy-5.3.5.2-18.9.4
libreoffice-glade-5.3.5.2-18.9.4
libreoffice-l10n-uk-5.3.5.2-18.9.4
libreoffice-l10n-pl-5.3.5.2-18.9.4
libreoffice-l10n-it-5.3.5.2-18.9.4
libreoffice-l10n-lt-5.3.5.2-18.9.4
libreoffice-l10n-ta-5.3.5.2-18.9.4
libreoffice-l10n-fi-5.3.5.2-18.9.4
libreoffice-l10n-zu-5.3.5.2-18.9.4
libreoffice-l10n-nso-5.3.5.2-18.9.4
libreoffice-l10n-tn-5.3.5.2-18.9.4
libreoffice-l10n-kk-5.3.5.2-18.9.4
libreoffice-l10n-ts-5.3.5.2-18.9.4
libreoffice-icon-theme-hicontrast-5.3.5.2-18.9.4
libreoffice-l10n-hi-5.3.5.2-18.9.4
libreoffice-l10n-sr-5.3.5.2-18.9.4
libreoffice-l10n-zh_TW-5.3.5.2-18.9.4
libreoffice-l10n-bn-5.3.5.2-18.9.4
libreoffice-l10n-ca-5.3.5.2-18.9.4

SuSE Linux 42.3
x86_64
libreoffice-debuginfo-5.3.5.2-3.4
libreoffice-sdk-5.3.5.2-3.4
libreoffice-base-drivers-postgresql-debuginfo-5.3.5.2-3.4
libreoffice-impress-debuginfo-5.3.5.2-3.4
libreoffice-writer-5.3.5.2-3.4
libreoffice-writer-debuginfo-5.3.5.2-3.4
libreoffice-gtk3-5.3.5.2-3.4
libreoffice-math-debuginfo-5.3.5.2-3.4
libreoffice-debugsource-5.3.5.2-3.4
libreoffice-pyuno-debuginfo-5.3.5.2-3.4
libreoffice-gnome-5.3.5.2-3.4
libreoffice-filters-optional-5.3.5.2-3.4
libreoffice-calc-extensions-5.3.5.2-3.4
libreofficekit-devel-5.3.5.2-3.4
libreoffice-mailmerge-5.3.5.2-3.4
libreoffice-pyuno-5.3.5.2-3.4

libreoffice-5.3.5.2-3.4
libreoffice-draw-5.3.5.2-3.4
libreoffice-impress-5.3.5.2-3.4
libreoffice-base-drivers-postgresql-5.3.5.2-3.4
libreoffice-kde4-5.3.5.2-3.4
libreoffice-draw-debuginfo-5.3.5.2-3.4
libreoffice-sdk-debuginfo-5.3.5.2-3.4
libreoffice-officebean-5.3.5.2-3.4
libreoffice-base-drivers-mysql-5.3.5.2-3.4
libreoffice-gtk3-debuginfo-5.3.5.2-3.4
libreoffice-math-5.3.5.2-3.4
libreoffice-writer-extensions-5.3.5.2-3.4
libreoffice-officebean-debuginfo-5.3.5.2-3.4
libreofficekit-5.3.5.2-3.4
libreoffice-calc-debuginfo-5.3.5.2-3.4
libreoffice-calc-5.3.5.2-3.4
libreoffice-gnome-debuginfo-5.3.5.2-3.4
libreoffice-kde4-debuginfo-5.3.5.2-3.4
libreoffice-base-debuginfo-5.3.5.2-3.4
libreoffice-base-5.3.5.2-3.4
libreoffice-sdk-doc-5.3.5.2-3.4
libreoffice-base-drivers-mysql-debuginfo-5.3.5.2-3.4

noarch
libreoffice-gdb-pretty-printers-5.3.5.2-3.4
libreoffice-l10n-th-5.3.5.2-3.4
libreoffice-l10n-kn-5.3.5.2-3.4
libreoffice-l10n-hi-5.3.5.2-3.4
libreoffice-l10n-ve-5.3.5.2-3.4
libreoffice-l10n-tn-5.3.5.2-3.4
libreoffice-l10n-uk-5.3.5.2-3.4
libreoffice-l10n-et-5.3.5.2-3.4
libreoffice-l10n-it-5.3.5.2-3.4
libreoffice-l10n-sl-5.3.5.2-3.4
libreoffice-glade-5.3.5.2-3.4
libreoffice-l10n-gu-5.3.5.2-3.4
libreoffice-l10n-gl-5.3.5.2-3.4
libreoffice-l10n-pl-5.3.5.2-3.4
libreoffice-l10n-bg-5.3.5.2-3.4
libreoffice-l10n-ml-5.3.5.2-3.4
libreoffice-l10n-nb-5.3.5.2-3.4
libreoffice-l10n-lt-5.3.5.2-3.4
libreoffice-l10n-cy-5.3.5.2-3.4
libreoffice-l10n-ts-5.3.5.2-3.4
libreoffice-l10n-af-5.3.5.2-3.4
libreoffice-l10n-es-5.3.5.2-3.4
libreoffice-l10n-hu-5.3.5.2-3.4
libreoffice-l10n-ru-5.3.5.2-3.4
libreoffice-l10n-mai-5.3.5.2-3.4
libreoffice-l10n-ta-5.3.5.2-3.4
libreoffice-l10n-as-5.3.5.2-3.4
libreoffice-l10n-nl-5.3.5.2-3.4
libreoffice-l10n-pa-5.3.5.2-3.4
libreoffice-l10n-en-5.3.5.2-3.4
libreoffice-l10n-ga-5.3.5.2-3.4
libreoffice-l10n-st-5.3.5.2-3.4
libreoffice-l10n-zu-5.3.5.2-3.4
libreoffice-l10n-ca-5.3.5.2-3.4

145929 - SuSE SLES 11 SP4 SUSE-SU-2017:2522-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10168, CVE-2016-10397, CVE-2016-5766, CVE-2017-11144, CVE-2017-11145, CVE-2017-11146, CVE-2017-11147, CVE-2017-11628, CVE-2017-12933, CVE-2017-7890

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2522-1

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-September/003246.html

SuSE SLES 11 SP4
i586
php53-dom-5.3.17-112.5.1
php53-sysvmsg-5.3.17-112.5.1
php53-ctype-5.3.17-112.5.1
php53-gd-5.3.17-112.5.1
php53-sysvsem-5.3.17-112.5.1
php53-zlib-5.3.17-112.5.1
php53-calendar-5.3.17-112.5.1
php53-snmp-5.3.17-112.5.1
php53-gettext-5.3.17-112.5.1
php53-mcrypt-5.3.17-112.5.1
php53-openssl-5.3.17-112.5.1
php53-curl-5.3.17-112.5.1
php53-bz2-5.3.17-112.5.1
php53-json-5.3.17-112.5.1
php53-mysql-5.3.17-112.5.1
php53-sysvshm-5.3.17-112.5.1
php53-pcntl-5.3.17-112.5.1
php53-xmlrpc-5.3.17-112.5.1
php53-pspell-5.3.17-112.5.1
php53-wddx-5.3.17-112.5.1
php53-fastcgi-5.3.17-112.5.1
php53-zip-5.3.17-112.5.1
php53-shmop-5.3.17-112.5.1
php53-ldap-5.3.17-112.5.1
php53-fileinfo-5.3.17-112.5.1
php53-gmp-5.3.17-112.5.1
php53-soap-5.3.17-112.5.1
php53-pgsql-5.3.17-112.5.1
php53-ftp-5.3.17-112.5.1
php53-odbc-5.3.17-112.5.1
php53-xmlreader-5.3.17-112.5.1
php53-xsl-5.3.17-112.5.1
php53-intl-5.3.17-112.5.1
php53-pdo-5.3.17-112.5.1
apache2-mod_php53-5.3.17-112.5.1
php53-pear-5.3.17-112.5.1
php53-mbstring-5.3.17-112.5.1
php53-iconv-5.3.17-112.5.1
php53-dba-5.3.17-112.5.1
php53-tokenizer-5.3.17-112.5.1
php53-bcmath-5.3.17-112.5.1

php53-xmlwriter-5.3.17-112.5.1
php53-5.3.17-112.5.1
php53-exif-5.3.17-112.5.1
php53-suhosin-5.3.17-112.5.1

x86_64
php53-dom-5.3.17-112.5.1
php53-sysvmsg-5.3.17-112.5.1
php53-ctype-5.3.17-112.5.1
php53-gd-5.3.17-112.5.1
php53-sysvsem-5.3.17-112.5.1
php53-zlib-5.3.17-112.5.1
php53-calendar-5.3.17-112.5.1
php53-snmp-5.3.17-112.5.1
php53-gettext-5.3.17-112.5.1
php53-mcrypt-5.3.17-112.5.1
php53-openssl-5.3.17-112.5.1
php53-curl-5.3.17-112.5.1
php53-bz2-5.3.17-112.5.1
php53-json-5.3.17-112.5.1
php53-mysql-5.3.17-112.5.1
php53-sysvshm-5.3.17-112.5.1
php53-pcntl-5.3.17-112.5.1
php53-xmlrpc-5.3.17-112.5.1
php53-pspell-5.3.17-112.5.1
php53-wddx-5.3.17-112.5.1
php53-fastcgi-5.3.17-112.5.1
php53-zip-5.3.17-112.5.1
php53-shmop-5.3.17-112.5.1
php53-ldap-5.3.17-112.5.1
php53-fileinfo-5.3.17-112.5.1
php53-gmp-5.3.17-112.5.1
php53-soap-5.3.17-112.5.1
php53-pgsql-5.3.17-112.5.1
php53-ftp-5.3.17-112.5.1
php53-odbc-5.3.17-112.5.1
php53-xmlreader-5.3.17-112.5.1
php53-xsl-5.3.17-112.5.1
php53-intl-5.3.17-112.5.1
php53-pdo-5.3.17-112.5.1
apache2-mod_php53-5.3.17-112.5.1
php53-pear-5.3.17-112.5.1
php53-mbstring-5.3.17-112.5.1
php53-iconv-5.3.17-112.5.1
php53-dba-5.3.17-112.5.1
php53-tokenizer-5.3.17-112.5.1
php53-bcmath-5.3.17-112.5.1
php53-xmlwriter-5.3.17-112.5.1
php53-5.3.17-112.5.1
php53-exif-5.3.17-112.5.1
php53-suhosin-5.3.17-112.5.1

145930 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2523-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2523-1

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-September/003247.html

SuSE SLED 12 SP3
x86_64
kernel-default-debugsource-4.4.82-6.6.1
kernel-default-4.4.82-6.6.1
kernel-default-extra-debuginfo-4.4.82-6.6.1
kernel-syms-4.4.82-6.6.1
kernel-default-debuginfo-4.4.82-6.6.1
kernel-default-devel-4.4.82-6.6.1
kernel-default-extra-4.4.82-6.6.1

noarch
kernel-source-4.4.82-6.6.1
kernel-macros-4.4.82-6.6.1
kernel-devel-4.4.82-6.6.1

SuSE SLES 12 SP3
noarch
kernel-source-4.4.82-6.6.1
kernel-macros-4.4.82-6.6.1
kernel-devel-4.4.82-6.6.1

x86_64
kernel-default-debugsource-4.4.82-6.6.1
kernel-default-4.4.82-6.6.1
kernel-default-base-4.4.82-6.6.1
kernel-syms-4.4.82-6.6.1
kernel-default-base-debuginfo-4.4.82-6.6.1
kernel-default-devel-4.4.82-6.6.1
kernel-default-debuginfo-4.4.82-6.6.1

145931 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2521-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2521-1

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-September/003245.html

SuSE SLED 12 SP2
x86_64

kernel-default-extra-4.4.74-92.38.1
kernel-default-devel-4.4.74-92.38.1
kernel-default-extra-debuginfo-4.4.74-92.38.1
kernel-default-4.4.74-92.38.1
kernel-default-debuginfo-4.4.74-92.38.1
kernel-syms-4.4.74-92.38.1
kernel-default-debugsource-4.4.74-92.38.1

noarch
kernel-macros-4.4.74-92.38.1
kernel-source-4.4.74-92.38.1
kernel-devel-4.4.74-92.38.1

SuSE SLES 12 SP2
noarch
kernel-macros-4.4.74-92.38.1
kernel-source-4.4.74-92.38.1
kernel-devel-4.4.74-92.38.1

x86_64
kernel-default-base-4.4.74-92.38.1
kernel-syms-4.4.74-92.38.1
kernel-default-devel-4.4.74-92.38.1
kernel-default-debugsource-4.4.74-92.38.1
kernel-default-4.4.74-92.38.1
kernel-default-base-debuginfo-4.4.74-92.38.1
kernel-default-debuginfo-4.4.74-92.38.1

145932 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2519-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14316, CVE-2017-14317, CVE-2017-14318, CVE-2017-14319

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2519-1

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-September/003244.html

SuSE SLED 12 SP2
x86_64
xen-libs-4.7.3_04-43.12.1
xen-debugsource-4.7.3_04-43.12.1
xen-libs-32bit-4.7.3_04-43.12.1
xen-4.7.3_04-43.12.1
xen-libs-debuginfo-4.7.3_04-43.12.1
xen-libs-debuginfo-32bit-4.7.3_04-43.12.1

SuSE SLES 12 SP2
x86_64
xen-libs-4.7.3_04-43.12.1
xen-debugsource-4.7.3_04-43.12.1
xen-doc-html-4.7.3_04-43.12.1

xen-libs-32bit-4.7.3_04-43.12.1
xen-4.7.3_04-43.12.1
xen-libs-debuginfo-4.7.3_04-43.12.1
xen-tools-domU-debuginfo-4.7.3_04-43.12.1
xen-tools-debuginfo-4.7.3_04-43.12.1
xen-tools-4.7.3_04-43.12.1
xen-libs-debuginfo-32bit-4.7.3_04-43.12.1
xen-tools-domU-4.7.3_04-43.12.1

163456 - Oracle Enterprise Linux ELSA-2017-2771 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
ELSA-2017-2771

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007210.html

OEL7
x86_64
emacs-24.3-20.el7_4
emacs-common-24.3-20.el7_4
emacs-terminal-24.3-20.el7_4
emacs-el-24.3-20.el7_4
emacs-nox-24.3-20.el7_4
emacs-filesystem-24.3-20.el7_4

163457 - Oracle Enterprise Linux ELSA-2017-2728 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547

Description

The scan detected that the host is missing the following update:
ELSA-2017-2728

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007209.html

OEL7
x86_64
postgresql-pltcl-9.2.23-1.el7_4
postgresql-plpython-9.2.23-1.el7_4
postgresql-test-9.2.23-1.el7_4
postgresql-static-9.2.23-1.el7_4

postgresql-docs-9.2.23-1.el7_4
postgresql-libs-9.2.23-1.el7_4
postgresql-contrib-9.2.23-1.el7_4
postgresql-plperl-9.2.23-1.el7_4
postgresql-9.2.23-1.el7_4
postgresql-server-9.2.23-1.el7_4
postgresql-upgrade-9.2.23-1.el7_4
postgresql-devel-9.2.23-1.el7_4

163458 - Oracle Enterprise Linux ELSA-2017-3620 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
ELSA-2017-3620

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007211.html
http://oss.oracle.com/pipermail/el-errata/2017-September/007212.html

OEL7
x86_64
kernel-uek-debug-devel-4.1.12-103.3.8.1.el7uek
kernel-uek-4.1.12-103.3.8.1.el7uek
kernel-uek-doc-4.1.12-103.3.8.1.el7uek
kernel-uek-devel-4.1.12-103.3.8.1.el7uek
kernel-uek-firmware-4.1.12-103.3.8.1.el7uek
kernel-uek-debug-4.1.12-103.3.8.1.el7uek
dtrace-modules-4.1.12-103.3.8.1.el7uek-0.6.1-3.el7

OEL6
x86_64
kernel-uek-debug-devel-4.1.12-103.3.8.1.el6uek
kernel-uek-firmware-4.1.12-103.3.8.1.el6uek
kernel-uek-4.1.12-103.3.8.1.el6uek
kernel-uek-doc-4.1.12-103.3.8.1.el6uek
kernel-uek-devel-4.1.12-103.3.8.1.el6uek
kernel-uek-debug-4.1.12-103.3.8.1.el6uek
dtrace-modules-4.1.12-103.3.8.1.el6uek-0.6.1-3.el6

170869 - Amazon Linux AMI ALAS-2017-892 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3167, CVE-2017-3169, CVE-2017-7679, CVE-2017-9788

Description

The scan detected that the host is missing the following update:
ALAS-2017-892

Observation

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

https://alas.aws.amazon.com/ALAS-2017-892.html

Amazon Linux AMI
i686
httpd-2.2.34-1.12.amzn1
httpd-debuginfo-2.2.34-1.12.amzn1
httpd-tools-2.2.34-1.12.amzn1
httpd-devel-2.2.34-1.12.amzn1
mod_ssl-2.2.34-1.12.amzn1

noarch
httpd-manual-2.2.34-1.12.amzn1

x86_64
httpd-2.2.34-1.12.amzn1
httpd-debuginfo-2.2.34-1.12.amzn1
httpd-tools-2.2.34-1.12.amzn1
httpd-devel-2.2.34-1.12.amzn1
mod_ssl-2.2.34-1.12.amzn1

170870 - Amazon Linux AMI ALAS-2017-893 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000115, CVE-2017-1000116

Description

The scan detected that the host is missing the following update:
ALAS-2017-893

Observation

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

https://alas.aws.amazon.com/ALAS-2017-893.html

Amazon Linux AMI
x86_64
emacs-mercurial-4.2.3-1.29.amzn1
mercurial-debuginfo-4.2.3-1.29.amzn1
mercurial-common-4.2.3-1.29.amzn1
mercurial-python27-4.2.3-1.29.amzn1
mercurial-python26-4.2.3-1.29.amzn1
emacs-mercurial-el-4.2.3-1.29.amzn1

i686
emacs-mercurial-4.2.3-1.29.amzn1
mercurial-debuginfo-4.2.3-1.29.amzn1
mercurial-common-4.2.3-1.29.amzn1
mercurial-python27-4.2.3-1.29.amzn1
mercurial-python26-4.2.3-1.29.amzn1
emacs-mercurial-el-4.2.3-1.29.amzn1

170872 - Amazon Linux AMI ALAS-2017-896 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
ALAS-2017-896

Observation

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

https://alas.aws.amazon.com/ALAS-2017-896.html

Amazon Linux AMI
i686
mod24_ssl-2.4.27-3.73.amzn1
httpd24-tools-2.4.27-3.73.amzn1
mod_ssl-2.2.34-1.15.amzn1
mod24_ldap-2.4.27-3.73.amzn1
httpd24-2.4.27-3.73.amzn1
httpd-debuginfo-2.2.34-1.15.amzn1
mod24_proxy_html-2.4.27-3.73.amzn1
httpd-devel-2.2.34-1.15.amzn1
httpd24-devel-2.4.27-3.73.amzn1
httpd-2.2.34-1.15.amzn1
httpd-tools-2.2.34-1.15.amzn1
httpd24-debuginfo-2.4.27-3.73.amzn1
mod24_session-2.4.27-3.73.amzn1

noarch
httpd24-manual-2.4.27-3.73.amzn1
httpd-manual-2.2.34-1.15.amzn1

x86_64
mod24_ssl-2.4.27-3.73.amzn1
httpd24-tools-2.4.27-3.73.amzn1
mod_ssl-2.2.34-1.15.amzn1
mod24_ldap-2.4.27-3.73.amzn1
httpd24-2.4.27-3.73.amzn1
httpd-debuginfo-2.2.34-1.15.amzn1
mod24_proxy_html-2.4.27-3.73.amzn1
httpd-devel-2.2.34-1.15.amzn1
httpd24-devel-2.4.27-3.73.amzn1
httpd-2.2.34-1.15.amzn1
httpd-tools-2.2.34-1.15.amzn1
httpd24-debuginfo-2.4.27-3.73.amzn1
mod24_session-2.4.27-3.73.amzn1

170873 - Amazon Linux AMI ALAS-2017-897 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12134

Description

The scan detected that the host is missing the following update:
ALAS-2017-897

Observation

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

https://alas.aws.amazon.com/ALAS-2017-897.html

Amazon Linux AMI
i686
kernel-debuginfo-common-i686-4.9.43-17.39.amzn1
kernel-4.9.43-17.39.amzn1
kernel-debuginfo-4.9.43-17.39.amzn1
kernel-tools-debuginfo-4.9.43-17.39.amzn1
kernel-tools-devel-4.9.43-17.39.amzn1
kernel-devel-4.9.43-17.39.amzn1
perf-debuginfo-4.9.43-17.39.amzn1
kernel-tools-4.9.43-17.39.amzn1
perf-4.9.43-17.39.amzn1
kernel-headers-4.9.43-17.39.amzn1

noarch
kernel-doc-4.9.43-17.39.amzn1

x86_64
kernel-devel-4.9.43-17.39.amzn1
kernel-debuginfo-4.9.43-17.39.amzn1
kernel-tools-debuginfo-4.9.43-17.39.amzn1
kernel-tools-devel-4.9.43-17.39.amzn1
kernel-headers-4.9.43-17.39.amzn1
perf-debuginfo-4.9.43-17.39.amzn1
kernel-tools-4.9.43-17.39.amzn1
perf-4.9.43-17.39.amzn1
kernel-debuginfo-common-x86_64-4.9.43-17.39.amzn1
kernel-4.9.43-17.39.amzn1

170874 - Amazon Linux AMI ALAS-2017-895 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
ALAS-2017-895

Observation

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

https://alas.aws.amazon.com/ALAS-2017-895.html

Amazon Linux AMI
noarch
aws-cfn-bootstrap-1.4-22.14.amzn1

175260 - Scientific Linux Security ERRATA Moderate: postgresql on SL7.x x86_64 (1709-1415)

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: postgresql on SL7.x x86_64 (1709-1415)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1709&L=scientific-linux-errata&F=&S=&P=1415

SL7
x86_64
postgresql-contrib-9.2.23-1.el7_4
postgresql-pltcl-9.2.23-1.el7_4
postgresql-test-9.2.23-1.el7_4
postgresql-devel-9.2.23-1.el7_4
postgresql-static-9.2.23-1.el7_4
postgresql-plpython-9.2.23-1.el7_4
postgresql-upgrade-9.2.23-1.el7_4
postgresql-debuginfo-9.2.23-1.el7_4
postgresql-plperl-9.2.23-1.el7_4
postgresql-docs-9.2.23-1.el7_4
postgresql-server-9.2.23-1.el7_4
postgresql-libs-9.2.23-1.el7_4
postgresql-9.2.23-1.el7_4

175261 - Scientific Linux Security ERRATA Important: emacs on SL7.x x86_64 (1709-1762)

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

Risk Level: High

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: emacs on SL7.x x86_64 (1709-1762)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1709&L=scientific-linux-errata&F=&S=&P=1762

SL7
x86_64
emacs-nox-24.3-20.el7_4
emacs-common-24.3-20.el7_4
emacs-24.3-20.el7_4
emacs-debuginfo-24.3-20.el7_4

noarch
emacs-el-24.3-20.el7_4
emacs-filesystem-24.3-20.el7_4
emacs-terminal-24.3-20.el7_4

178494 - Gentoo Linux GLSA-201709-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-05

Observation

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

https://security.gentoo.org/glsa/201709-05

Affected packages:
app-forensics/chkrootkit < 0.50

178497 - Gentoo Linux GLSA-201709-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-06

Observation

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

https://security.gentoo.org/glsa/201709-06

Affected packages:
app-admin/supervisor < 3.1.4

178501 - Gentoo Linux GLSA-201709-11 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-11

Observation

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

https://security.gentoo.org/glsa/201709-11

Affected packages:
sci-mathematics/gimps < 28.10-r1

182441 - FreeBSD ruby Multiple Vulnerabilities (95b01379-9d52-11e7-a25c-471bafc3262f)

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

Risk Level: High

CVE: CVE-2017-0898, CVE-2017-10784, CVE-2017-14033, CVE-2017-14064

Description

The scan detected that the host is missing the following update:
ruby -- multiple vulnerabilities (95b01379-9d52-11e7-a25c-471bafc3262f)

Observation

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

http://www.vuxml.org/freebsd/95b01379-9d52-11e7-a25c-471bafc3262f.html

Affected packages:
2.2.0 <= ruby < 2.2.8
2.3.0 <= ruby < 2.3.5
2.4.0 <= ruby < 2.4.2

185877 - Ubuntu Linux 14.04 USN-3422-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10044, CVE-2016-10200, CVE-2016-7097, CVE-2016-8650, CVE-2016-9083, CVE-2016-9084, CVE-2016-9178, CVE-2016-9191, CVE-2016-9604, CVE-2016-9754, CVE-2017-1000251, CVE-2017-5970, CVE-2017-6214, CVE-2017-6346, CVE-2017-6951, CVE-2017-7187, CVE-2017-7472, CVE-2017-7541

Description

The scan detected that the host is missing the following update:
USN-3422-1

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-September/004052.html

Ubuntu 14.04

linux-image-3.13.0-132-powerpc-smp_3.13.0-132.181
linux-image-3.13.0-132-powerpc64-smp_3.13.0-132.181
linux-image-3.13.0-132-powerpc64-emb_3.13.0-132.181
linux-image-3.13.0-132-lowlatency_3.13.0-132.181
linux-image-generic_3.13.0.132.141
linux-image-3.13.0-132-powerpc-e500mc_3.13.0-132.181
linux-image-3.13.0-132-powerpc-e500_3.13.0-132.181

linux-image-powerpc64-emb_3.13.0.132.141
linux-image-powerpc64-smp_3.13.0.132.141
linux-image-powerpc-smp_3.13.0.132.141
linux-image-lowlatency_3.13.0.132.141
linux-image-generic-lpae_3.13.0.132.141
linux-image-powerpc-e500_3.13.0.132.141
linux-image-3.13.0-132-generic_3.13.0-132.181
linux-image-powerpc-e500mc_3.13.0.132.141
linux-image-3.13.0-132-generic-lpae_3.13.0-132.181

185878 - Ubuntu Linux 12.04 USN-3422-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10044, CVE-2016-10200, CVE-2016-7097, CVE-2016-8650, CVE-2016-9083, CVE-2016-9084, CVE-2016-9178, CVE-2016-9191, CVE-2016-9604, CVE-2016-9754, CVE-2017-1000251, CVE-2017-5970, CVE-2017-6214, CVE-2017-6346, CVE-2017-6951, CVE-2017-7187, CVE-2017-7472, CVE-2017-7541

Description

The scan detected that the host is missing the following update:
USN-3422-2

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-September/004056.html

Ubuntu 12.04

linux-image-generic-lpae-lts-trusty_3.13.0.132.122
linux-image-3.13.0-132-generic-lpae_3.13.0-132.181~precise1
linux-image-3.13.0-132-generic_3.13.0-132.181~precise1
linux-image-generic-lts-trusty_3.13.0.132.122

185880 - Ubuntu Linux 16.04 USN-3419-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-7541

Description

The scan detected that the host is missing the following update:
USN-3419-2

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-September/004054.html

Ubuntu 16.04

linux-image-4.10.0-35-lowlatency_4.10.0-35.39~16.04.1
linux-image-lowlatency-hwe-16.04_4.10.0.35.37
linux-image-generic-lpae-hwe-16.04_4.10.0.35.37

linux-image-4.10.0-35-generic-lpae_4.10.0-35.39~16.04.1
linux-image-generic-hwe-16.04_4.10.0.35.37
linux-image-4.10.0-35-generic_4.10.0-35.39~16.04.1

185881 - Ubuntu Linux 12.04 USN-3415-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004, CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010, CVE-2017-13011, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016, CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022, CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028, CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034, CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040, CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046, CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052, CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689, CVE-2017-13690, CVE-2017-13725

Description

The scan detected that the host is missing the following update:
USN-3415-2

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-September/004043.html

Ubuntu 12.04

tcpdump_4.9.2-0ubuntu0.12.04.1

185882 - Ubuntu Linux 17.04 USN-3419-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-7541

Description

The scan detected that the host is missing the following update:
USN-3419-1

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-September/004050.html

Ubuntu 17.04

linux-image-raspi2_4.10.0.1018.19
linux-image-generic-lpae_4.10.0.35.35

linux-image-4.10.0-35-generic-lpae_4.10.0-35.39
linux-image-generic_4.10.0.35.35
linux-image-4.10.0-35-generic_4.10.0-35.39
linux-image-4.10.0-35-lowlatency_4.10.0-35.39
linux-image-lowlatency_4.10.0.35.35
linux-image-4.10.0-1018-raspi2_4.10.0-1018.21

185885 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3415-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004, CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010, CVE-2017-13011, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016, CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022, CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028, CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034, CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040, CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046, CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052, CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689, CVE-2017-13690, CVE-2017-13725

Description

The scan detected that the host is missing the following update:
USN-3415-1

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-September/004042.html

Ubuntu 16.04

tcpdump_4.9.2-0ubuntu0.16.04.1

Ubuntu 14.04

tcpdump_4.9.2-0ubuntu0.14.04.1

Ubuntu 17.04

tcpdump_4.9.2-0ubuntu0.17.04.2

192636 - Fedora Linux 26 FEDORA-2017-8f27031c8f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9907, CVE-2015-8957, CVE-2015-8958, CVE-2015-8959, CVE-2016-5010, CVE-2016-5841, CVE-2016-5842, CVE-2016-6491, CVE-2016-6823, CVE-2016-7101, CVE-2016-7513, CVE-2016-7514, CVE-2016-7515, CVE-2016-7516, CVE-2016-7517, CVE-2016-7518, CVE-2016-7519, CVE-2016-7520, CVE-2016-7521, CVE-2016-8707, CVE-2016-9556, CVE-2016-9559, CVE-2017-10928, CVE-2017-10995, CVE-2017-11141, CVE-2017-11170, CVE-2017-11188, CVE-2017-11352, CVE-2017-11360, CVE-2017-11446, CVE-2017-11447, CVE-2017-11448, CVE-2017-11449, CVE-2017-11450, CVE-2017-11478, CVE-2017-11523, CVE-2017-11639, CVE-2017-11640, CVE-2017-11644, CVE-2017-11724, CVE-2017-11750, CVE-2017-11751, CVE-2017-11752, CVE-2017-

11753, CVE-2017-11754, CVE-2017-11755, CVE-2017-12140, CVE-2017-12418, CVE-2017-12427, CVE-2017-12428, CVE-2017-12429, CVE-2017-12430, CVE-2017-12432, CVE-2017-12433, CVE-2017-12434, CVE-2017-12435, CVE-2017-12587, CVE-2017-12640, CVE-2017-12641, CVE-2017-12642, CVE-2017-12643, CVE-2017-12644, CVE-2017-12654, CVE-2017-12662, CVE-2017-12663, CVE-2017-12664, CVE-2017-12665, CVE-2017-12666, CVE-2017-7941, CVE-2017-7942, CVE-2017-7943, CVE-2017-8352, CVE-2017-9098, CVE-2017-9141, CVE-2017-9142, CVE-2017-9143, CVE-2017-9144

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8f27031c8f

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/2017/9/?count=200&page=1

Fedora Core 26

vips-8.5.8-2.fc26
vdr-scraper2vdr-1.0.5-4.20170611git254122b.fc26
perl-Image-SubImageFind-0.03-13.fc26
techne-0.2.3-20.fc26
imageinfo-0.05-27.fc26
rss-glx-0.9.1.p-29.fc26.1
dmtx-utils-0.7.4-4.fc26
kxstitch-1.2.0-9.fc26
drawtiming-0.7.1-22.fc26
autotrace-0.31.1-49.fc26
inkscape-0.92.1-4.20170510bzr15686.fc26.1
q-7.11-29.fc26
synfigstudio-1.2.0-5.fc26
ImageMagick-6.9.9.13-1.fc26
gtatool-2.2.0-6.fc26
ripright-0.11-5.fc26
php-pecl-imagick-3.4.3-2.fc26
k3d-0.8.0.6-8.fc26
emacs-25.3-3.fc26
converseen-0.9.6.2-3.fc26
rubygem-rmagick-2.16.0-4.fc26.2
synfig-1.2.0-9.fc26.1
pfstools-2.0.6-3.fc26
WindowMaker-0.95.8-3.fc26
psiconv-0.9.8-22.fc26

192643 - Fedora Linux 25 FEDORA-2017-ed735463e3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10664, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855, CVE-2017-5579, CVE-2017-7718, CVE-2017-8309, CVE-2017-8379, CVE-2017-9330

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ed735463e3

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/2017/9/?count=200&page=2

Fedora Core 25

xen-4.7.3-4.fc25

192644 - Fedora Linux 25 FEDORA-2017-e136d63c99 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0899, CVE-2017-0900, CVE-2017-0901, CVE-2017-0902, CVE-2017-14064

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e136d63c99

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/2017/9/?count=200&page=2

Fedora Core 25

ruby-2.3.4-64.fc25

192649 - Fedora Linux 25 FEDORA-2017-7dacb3c21c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7555

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7dacb3c21c

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/2017/9/?count=200&page=3

Fedora Core 25

augeas-1.8.1-1.fc25

192650 - Fedora Linux 26 FEDORA-2017-80c4677540 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13735, CVE-2017-14265

Description

The scan detected that the host is missing the following update:
FEDORA-2017-80c4677540

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/2017/9/?count=200&page=2

Fedora Core 26

LibRaw-0.18.4-1.fc26

22357 - IBM WebSphere Application Server Multiple Java Vulnerabilities (swg22007002)

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

Risk Level: Medium

CVE: CVE-2017-10102, CVE-2017-10115, CVE-2017-10116

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server.

Observation

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

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaws lie in the IBM Java SDK component. Exploitation could allow a malicious unauthenticated user to obtain sensitive information or take control of the system.

22358 - AzeoTech DAQFactory Multiple Vulnerabilities Prior To 17.1

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

Risk Level: Medium

CVE: CVE-2017-12699, CVE-2017-5147

Description

Multiple Vulnerabilities are present in some versions of AzeoTech DAQFactory.

Observation

AzeoTech DAQFactory is a popular Supervisory Control (SCADA) software.

Multiple Vulnerabilities are present in some versions of AzeoTech DAQFactory. The flaws lie in multiple components of AzeoTech DAQFactory. Successful exploitation could allow a local attacker to escalate its privileges.

22442 - SpiderControl SCADA Web Server Privilege Escalation Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-12728

Description

A vulnerability is present in some versions of SpiderControl SCADA Web Server.

Observation

SpiderControl SCADA Web Server is a software management platform.

A vulnerability is present in some versions of SpiderControl SCADA Web Server. The flaw lies in privilege management. Successful exploitation could allow an attacker to gain elevated privileges and execute code in the system.

130887 - Debian Linux 8.0, 9.0 DSA-3978-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2862

Description

The scan detected that the host is missing the following update:
DSA-3978-1

Observation

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

http://www.debian.org/security/2017/dsa-3978

Debian 8.0
all
libgdk-pixbuf2.0-doc_2.31.1-2+deb8u6
libgdk-pixbuf2.0-common_2.31.1-2+deb8u6
libgdk-pixbuf2.0-0_2.31.1-2+deb8u6
libgdk-pixbuf2.0-0-dbg_2.31.1-2+deb8u6
libgdk-pixbuf2.0-dev_2.31.1-2+deb8u6
gir1.2-gdkpixbuf-2.0_2.31.1-2+deb8u6
libgdk-pixbuf2.0-0-udeb_2.31.1-2+deb8u6

Debian 9.0
all
libgdk-pixbuf2.0-0_2.36.5-2+deb9u1
gir1.2-gdkpixbuf-2.0_2.36.5-2+deb9u1
libgdk-pixbuf2.0-doc_2.36.5-2+deb9u1
libgdk-pixbuf2.0-common_2.36.5-2+deb9u1
libgdk-pixbuf2.0-dev_2.36.5-2+deb9u1
libgdk-pixbuf2.0-0-udeb_2.36.5-2+deb9u1

170868 - Amazon Linux AMI ALAS-2017-891 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11403

Description

The scan detected that the host is missing the following update:
ALAS-2017-891

Observation

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

https://alas.aws.amazon.com/ALAS-2017-891.html

Amazon Linux AMI
i686
GraphicsMagick-c++-devel-1.3.26-3.11.amzn1
GraphicsMagick-debuginfo-1.3.26-3.11.amzn1
GraphicsMagick-1.3.26-3.11.amzn1
GraphicsMagick-devel-1.3.26-3.11.amzn1
GraphicsMagick-c++-1.3.26-3.11.amzn1
GraphicsMagick-perl-1.3.26-3.11.amzn1

noarch
GraphicsMagick-doc-1.3.26-3.11.amzn1

x86_64
GraphicsMagick-c++-devel-1.3.26-3.11.amzn1
GraphicsMagick-debuginfo-1.3.26-3.11.amzn1
GraphicsMagick-1.3.26-3.11.amzn1
GraphicsMagick-devel-1.3.26-3.11.amzn1
GraphicsMagick-c++-1.3.26-3.11.amzn1
GraphicsMagick-perl-1.3.26-3.11.amzn1

185873 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3424-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0663, CVE-2017-7375, CVE-2017-7376, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050

Description

The scan detected that the host is missing the following update:
USN-3424-1

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-September/004057.html

Ubuntu 16.04

libxml2_2.9.3+dfsg1-1ubuntu0.3

Ubuntu 14.04

libxml2_2.9.1+dfsg1-3ubuntu4.10

Ubuntu 17.04

libxml2_2.9.4+dfsg1-2.2ubuntu0.1

192645 - Fedora Linux 26 FEDORA-2017-caa564d86f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13709

Description

The scan detected that the host is missing the following update:
FEDORA-2017-caa564d86f

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/2017/9/?count=200&page=2

Fedora Core 26

FlightGear-2017.2.1-2.fc26

192646 - Fedora Linux 25 FEDORA-2017-292c77b3c1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13709

Description

The scan detected that the host is missing the following update:
FEDORA-2017-292c77b3c1

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/2017/9/?count=200&page=2

Fedora Core 25

FlightGear-2016.3.1-5.fc25

22440 - IBM AIX ITDS Multiple Vulnerabilities (itds_advisory)

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

Risk Level: Medium

CVE: CVE-2016-2183

Description

A vulnerability is present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

A vulnerability is present in some versions of IBM AIX. The flaws lie in IBM Tivoli Directory Server and IBM Security Directory Server. Successful exploitation could allow an attacker to obtain sensitive information.

22441 - Cisco IOS Software IPv6 SNMP Message Handling Denial of Service Vulnerability (CSCvb14640)

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-12211

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw lies in the SNMP component. Successful exploitation could allow an attacker to cause a denial of service condition.

22450 - (K43650115) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-0723

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to cause unauthorized disclosure of information or cause a denial of service condition.

130884 - Debian Linux 8.0, 9.0 DSA-3979-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11424

Description

The scan detected that the host is missing the following update:
DSA-3979-1

Observation

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

http://www.debian.org/security/2017/dsa-3979

Debian 8.0
all
python3-jwt_0.2.1-1+deb8u2
python-jwt_0.2.1-1+deb8u2

Debian 9.0
all
python-jwt_1.4.2-1+deb9u1
python3-jwt_1.4.2-1+deb9u1

130885 - Debian Linux 8.0, 9.0 DSA-3974-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7674, CVE-2017-7675

Description

The scan detected that the host is missing the following update:
DSA-3974-1

Observation

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

http://www.debian.org/security/2017/dsa-3974

Debian 8.0
all
tomcat8_8.0.14-1+deb8u11

Debian 9.0
all
tomcat8_8.5.14-1+deb9u2

145921 - SuSE Linux 42.3 openSUSE-SU-2017:2513-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10664, CVE-2017-10806, CVE-2017-11334, CVE-2017-11434

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2513-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00080.html

SuSE Linux 42.3
i586
qemu-linux-user-debugsource-2.9.0-32.1
qemu-linux-user-debuginfo-2.9.0-32.1
qemu-linux-user-2.9.0-32.1

noarch
qemu-vgabios-1.10.2-32.4
qemu-ipxe-1.0.0-32.4
qemu-seabios-1.10.2-32.4
qemu-sgabios-8-32.4

x86_64
qemu-ppc-debuginfo-2.9.0-32.4
qemu-block-iscsi-2.9.0-32.4
qemu-x86-2.9.0-32.4
qemu-x86-debuginfo-2.9.0-32.4

qemu-lang-2.9.0-32.4
qemu-ppc-2.9.0-32.4
qemu-block-dmg-2.9.0-32.4
qemu-2.9.0-32.4
qemu-kvm-2.9.0-32.4
qemu-block-curl-2.9.0-32.4
qemu-block-ssh-debuginfo-2.9.0-32.4
qemu-debugsource-2.9.0-32.4
qemu-guest-agent-debuginfo-2.9.0-32.4
qemu-tools-2.9.0-32.4
qemu-block-iscsi-debuginfo-2.9.0-32.4
qemu-block-dmg-debuginfo-2.9.0-32.4
qemu-block-rbd-debuginfo-2.9.0-32.4
qemu-block-curl-debuginfo-2.9.0-32.4
qemu-linux-user-debugsource-2.9.0-32.1
qemu-s390-debuginfo-2.9.0-32.4
qemu-arm-2.9.0-32.4
qemu-ksm-2.9.0-32.4
qemu-block-rbd-2.9.0-32.4
qemu-extra-2.9.0-32.4
qemu-guest-agent-2.9.0-32.4
qemu-extra-debuginfo-2.9.0-32.4
qemu-arm-debuginfo-2.9.0-32.4
qemu-linux-user-2.9.0-32.1
qemu-block-ssh-2.9.0-32.4
qemu-s390-2.9.0-32.4
qemu-testsuite-2.9.0-32.4
qemu-linux-user-debuginfo-2.9.0-32.1
qemu-tools-debuginfo-2.9.0-32.4

145926 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2483-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12836

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2483-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00067.html

SuSE Linux 42.2
i586
cvs-1.12.12-185.3.1
cvs-debuginfo-1.12.12-185.3.1
cvs-debugsource-1.12.12-185.3.1

noarch
cvs-doc-1.12.12-185.3.1

x86_64
cvs-1.12.12-185.3.1
cvs-debuginfo-1.12.12-185.3.1

cvs-debugsource-1.12.12-185.3.1

SuSE Linux 42.3
i586
cvs-1.12.12-188.1
cvs-debugsource-1.12.12-188.1
cvs-debuginfo-1.12.12-188.1

noarch
cvs-doc-1.12.12-188.1

x86_64
cvs-1.12.12-188.1
cvs-debugsource-1.12.12-188.1
cvs-debuginfo-1.12.12-188.1

160298 - CentOS 7 CESA-2017-2728 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2728

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-September/022540.html

CentOS 7
x86_64
postgresql-pltcl-9.2.23-1.el7_4
postgresql-plpython-9.2.23-1.el7_4
postgresql-test-9.2.23-1.el7_4
postgresql-static-9.2.23-1.el7_4
postgresql-docs-9.2.23-1.el7_4
postgresql-libs-9.2.23-1.el7_4
postgresql-contrib-9.2.23-1.el7_4
postgresql-plperl-9.2.23-1.el7_4
postgresql-9.2.23-1.el7_4
postgresql-server-9.2.23-1.el7_4
postgresql-upgrade-9.2.23-1.el7_4
postgresql-devel-9.2.23-1.el7_4

i686
postgresql-9.2.23-1.el7_4
postgresql-static-9.2.23-1.el7_4
postgresql-libs-9.2.23-1.el7_4
postgresql-devel-9.2.23-1.el7_4

170867 - Amazon Linux AMI ALAS-2017-890 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000061

Description

The scan detected that the host is missing the following update:
ALAS-2017-890

Observation

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

https://alas.aws.amazon.com/ALAS-2017-890.html

Amazon Linux AMI
x86_64
xmlsec1-gcrypt-1.2.20-7.4.amzn1
xmlsec1-1.2.20-7.4.amzn1
xmlsec1-openssl-1.2.20-7.4.amzn1
xmlsec1-openssl-devel-1.2.20-7.4.amzn1
xmlsec1-gnutls-1.2.20-7.4.amzn1
xmlsec1-gcrypt-devel-1.2.20-7.4.amzn1
xmlsec1-debuginfo-1.2.20-7.4.amzn1
xmlsec1-devel-1.2.20-7.4.amzn1
xmlsec1-nss-1.2.20-7.4.amzn1
xmlsec1-gnutls-devel-1.2.20-7.4.amzn1
xmlsec1-nss-devel-1.2.20-7.4.amzn1

i686
xmlsec1-gcrypt-1.2.20-7.4.amzn1
xmlsec1-1.2.20-7.4.amzn1
xmlsec1-openssl-1.2.20-7.4.amzn1
xmlsec1-openssl-devel-1.2.20-7.4.amzn1
xmlsec1-gcrypt-devel-1.2.20-7.4.amzn1
xmlsec1-debuginfo-1.2.20-7.4.amzn1
xmlsec1-gnutls-1.2.20-7.4.amzn1
xmlsec1-nss-1.2.20-7.4.amzn1
xmlsec1-gnutls-devel-1.2.20-7.4.amzn1
xmlsec1-nss-devel-1.2.20-7.4.amzn1
xmlsec1-devel-1.2.20-7.4.amzn1

170871 - Amazon Linux AMI ALAS-2017-894 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7529

Description

The scan detected that the host is missing the following update:
ALAS-2017-894

Observation

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

https://alas.aws.amazon.com/ALAS-2017-894.html

Amazon Linux AMI
x86_64

nginx-all-modules-1.12.1-1.32.amzn1
nginx-mod-http-image-filter-1.12.1-1.32.amzn1
nginx-debuginfo-1.12.1-1.32.amzn1
nginx-mod-mail-1.12.1-1.32.amzn1
nginx-mod-stream-1.12.1-1.32.amzn1
nginx-mod-http-xslt-filter-1.12.1-1.32.amzn1
nginx-mod-http-perl-1.12.1-1.32.amzn1
nginx-mod-http-geoip-1.12.1-1.32.amzn1
nginx-1.12.1-1.32.amzn1

i686
nginx-all-modules-1.12.1-1.32.amzn1
nginx-mod-http-image-filter-1.12.1-1.32.amzn1
nginx-debuginfo-1.12.1-1.32.amzn1
nginx-mod-mail-1.12.1-1.32.amzn1
nginx-mod-stream-1.12.1-1.32.amzn1
nginx-mod-http-xslt-filter-1.12.1-1.32.amzn1
nginx-mod-http-perl-1.12.1-1.32.amzn1
nginx-mod-http-geoip-1.12.1-1.32.amzn1
nginx-1.12.1-1.32.amzn1

178490 - Gentoo Linux GLSA-201709-10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-10

Observation

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

https://security.gentoo.org/glsa/201709-10

Affected packages:
dev-vcs/git < 2.13.5

178491 - Gentoo Linux GLSA-201709-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-02

Observation

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

https://security.gentoo.org/glsa/201709-02

Affected packages:
sys-devel/binutils < 2.28.1

178492 - Gentoo Linux GLSA-201709-08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-08

Observation

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

https://security.gentoo.org/glsa/201709-08

Affected packages:
x11-libs/gdk-pixbuf < 2.36.9

178496 - Gentoo Linux GLSA-201709-07 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-07

Observation

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

https://security.gentoo.org/glsa/201709-07

Affected packages:
dev-libs/kpathsea < 6.2.2_p20160523

178498 - Gentoo Linux GLSA-201709-04 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-04

Observation

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

For more information see:

https://security.gentoo.org/glsa/201709-04

Affected packages:
www-apache/mod_gnutls < 0.7.3

178499 - Gentoo Linux GLSA-201709-12 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-12

Observation

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

https://security.gentoo.org/glsa/201709-12

Affected packages:
dev-lang/perl < 5.24.1-r2
perl-core/File-Path < 2.130.0
virtual/perl-File-Path < 2.130.0

178500 - Gentoo Linux GLSA-201709-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201709-03

Observation

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

https://security.gentoo.org/glsa/201709-03

Affected packages:
net-libs/webkit-gtk < 2.16.5

185883 - Ubuntu Linux 17.04 USN-3417-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0379

Description

The scan detected that the host is missing the following update:
USN-3417-1

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-September/004044.html

Ubuntu 17.04

libgcrypt20_1.7.6-1ubuntu0.2

192631 - Fedora Linux 26 FEDORA-2017-b10e1a9166 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13735

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b10e1a9166

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/2017/9/?count=200&page=1

Fedora Core 26

rawtherapee-5.2-2.fc26

192648 - Fedora Linux 25 FEDORA-2017-c5d7fd07c5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13735

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c5d7fd07c5

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/2017/9/?count=200&page=2

Fedora Core 25

LibRaw-0.17.2-2.fc25

192654 - Fedora Linux 26 FEDORA-2017-769793738f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000050

Description

The scan detected that the host is missing the following update:
FEDORA-2017-769793738f

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/2017/9/?count=200&page=1

Fedora Core 26

jasper-2.0.14-1.fc26

22353 - (K31925518) F5 BIG-IP APM Access Logs Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-1497

Description

A 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 vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the configuration utility component. Successful exploitation could allow an attacker to bypass security restrictions and retrieve sensitive data.

22468 - IBM WebSphere Portal Cross-Site Scripting Vulnerability (swg22008028)

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

Risk Level: Medium

CVE: CVE-2017-1189

Description

A vulnerability is present in some versions of IBM WebSphere Portal.

Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in Web UI. Successful exploitation could allow an attacker to perform cross-site scripting attacks.

130888 - Debian Linux 8.0, 9.0 DSA-3973-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14313

Description

The scan detected that the host is missing the following update:
DSA-3973-1

Observation

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

http://www.debian.org/security/2017/dsa-3973

Debian 8.0
all
wordpress-shibboleth_1.4-2+deb8u1

Debian 9.0
all
wordpress-shibboleth_1.4-2+deb9u1

145922 - SuSE Linux 42.3 openSUSE-SU-2017:2494-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000251, CVE-2017-11472, CVE-2017-14106

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2494-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00073.html

SuSE Linux 42.3
x86_64
kernel-vanilla-base-4.4.87-25.1
kernel-debug-debuginfo-4.4.87-25.1
kernel-obs-build-debugsource-4.4.87-25.1
kernel-debug-base-debuginfo-4.4.87-25.1
kernel-default-debuginfo-4.4.87-25.1
kernel-default-debugsource-4.4.87-25.1
kernel-debug-4.4.87-25.1
kernel-vanilla-debugsource-4.4.87-25.1
kernel-obs-qa-4.4.87-25.1
kernel-default-devel-4.4.87-25.1
kernel-obs-build-4.4.87-25.1
kernel-default-base-4.4.87-25.1
kernel-debug-debugsource-4.4.87-25.1
kernel-vanilla-base-debuginfo-4.4.87-25.1
kernel-default-4.4.87-25.1
kernel-vanilla-4.4.87-25.1
kernel-vanilla-devel-4.4.87-25.1
kernel-debug-devel-4.4.87-25.1
kernel-default-base-debuginfo-4.4.87-25.1

kernel-debug-base-4.4.87-25.1
kernel-vanilla-debuginfo-4.4.87-25.1
kernel-syms-4.4.87-25.1
kernel-debug-devel-debuginfo-4.4.87-25.1

noarch
kernel-docs-4.4.87-25.2
kernel-docs-html-4.4.87-25.2
kernel-macros-4.4.87-25.1
kernel-docs-pdf-4.4.87-25.2
kernel-source-vanilla-4.4.87-25.1
kernel-source-4.4.87-25.1
kernel-devel-4.4.87-25.1

192632 - Fedora Linux 26 FEDORA-2017-ab0def38cd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7674

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ab0def38cd

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/2017/9/?count=200&page=3

Fedora Core 26

tomcat-8.0.46-1.fc26

192633 - Fedora Linux 26 FEDORA-2017-4d4914a260 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14107

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4d4914a260

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/2017/9/?count=200&page=1

Fedora Core 26

mingw-libzip-1.3.0-1.fc26

192647 - Fedora Linux 25 FEDORA-2017-bb5d87e9de Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14107

Description

The scan detected that the host is missing the following update:
FEDORA-2017-bb5d87e9de

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/2017/9/?count=200&page=1

Fedora Core 25

mingw-libzip-1.1.3-3.fc25

192652 - Fedora Linux 25 FEDORA-2017-a00a087fd4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7674

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a00a087fd4

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/2017/9/?count=200&page=2

Fedora Core 25

tomcat-8.0.46-1.fc25

192655 - Fedora Linux 26 FEDORA-2017-8614a6e905 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12794

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8614a6e905

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/2017/9/?count=200&page=2

Fedora Core 26

python-django-1.10.8-1.fc26

130882 - Debian Linux 8.0, 9.0 DSA-3976-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2923, CVE-2017-2924

Description

The scan detected that the host is missing the following update:
DSA-3976-1

Observation

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

http://www.debian.org/security/2017/dsa-3976

Debian 8.0
all
libfreexl-dev_1.0.0g-1+deb8u4
libfreexl1_1.0.0g-1+deb8u4
libfreexl1-dbg_1.0.0g-1+deb8u4

Debian 9.0
all
libfreexl-dev_1.0.2-2+deb9u1
libfreexl1_1.0.2-2+deb9u1
libfreexl1-dbg_1.0.2-2+deb9u1

130883 - Debian Linux 8.0, 9.0 DSA-3977-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14500

Description

The scan detected that the host is missing the following update:
DSA-3977-1

Observation

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

http://www.debian.org/security/2017/dsa-3977

Debian 8.0
all
newsbeuter_2.8-2+deb8u2

Debian 9.0
all
newsbeuter_2.9-5+deb9u2

130886 - Debian Linux 9.0 DSA-3975-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
DSA-3975-1

Observation

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

http://www.debian.org/security/2017/dsa-3975

Debian 9.0
all
emacs25_25.1+1-4+deb9u1

182442 - FreeBSD Apache HTTP OPTIONS Method Can Leak Server Memory (76b085e2-9d33-11e7-9260-000c292ee6b8)

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

Risk Level: Low

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
Apache -- HTTP OPTIONS method can leak server memory (76b085e2-9d33-11e7-9260-000c292ee6b8)

Observation

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

http://www.vuxml.org/freebsd/76b085e2-9d33-11e7-9260-000c292ee6b8.html

Affected packages:
apache24 < 2.4.27_1
apache22 < 2.2.34_1

182444 - FreeBSD asterisk RTP/RTCP Information Leak (c2ea3b31-9d75-11e7-bb13-001999f8d30b)

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

Risk Level: Low

CVE: CVE-2017-14099

Description

The scan detected that the host is missing the following update:
asterisk -- RTP/RTCP information leak (c2ea3b31-9d75-11e7-bb13-001999f8d30b)

Observation

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

http://www.vuxml.org/freebsd/c2ea3b31-9d75-11e7-bb13-001999f8d30b.html

Affected packages:
asterisk11 < 11.25.3
asterisk13 < 13.17.2

182445 - FreeBSD rubygem-geminabox XSS & CSRF Vulnerabilities (2bffdf2f-9d45-11e7-a25c-471bafc3262f)

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

Risk Level: Low

CVE: CVE-2017-14506

Description

The scan detected that the host is missing the following update:
rubygem-geminabox -- XSS & CSRF vulnerabilities (2bffdf2f-9d45-11e7-a25c-471bafc3262f)

Observation

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

http://www.vuxml.org/freebsd/2bffdf2f-9d45-11e7-a25c-471bafc3262f.html

Affected packages:
rubygem-geminabox < 0.13.6

185872 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3346-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3142, CVE-2017-3143

Description

The scan detected that the host is missing the following update:
USN-3346-2

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-September/004047.html

Ubuntu 16.04

bind9_9.10.3.dfsg.P4-8ubuntu1.8

Ubuntu 14.04

bind9_9.9.5.dfsg-3ubuntu0.16

Ubuntu 17.04

bind9_9.10.3.dfsg.P4-10.1ubuntu5.2

185875 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3416-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7807, CVE-2017-7809

Description

The scan detected that the host is missing the following update:
USN-3416-1

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-September/004045.html

Ubuntu 16.04

thunderbird_52.3.0+build1-0ubuntu0.16.04.1

Ubuntu 14.04

thunderbird_52.3.0+build1-0ubuntu0.14.04.1

Ubuntu 17.04

thunderbird_52.3.0+build1-0ubuntu0.17.04.1

185884 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3425-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
USN-3425-1

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-September/004058.html

Ubuntu 16.04

apache2-bin_2.4.18-2ubuntu3.5

Ubuntu 14.04

apache2-bin_2.4.7-1ubuntu4.18

Ubuntu 17.04

apache2-bin_2.4.25-3ubuntu2.3

185887 - Ubuntu Linux 12.04 USN-3423-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
USN-3423-1

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-September/004053.html

Ubuntu 12.04

linux-image-3.2.0-131-omap_3.2.0-131.177
linux-image-generic-pae_3.2.0.131.145
linux-image-3.2.0-131-virtual_3.2.0-131.177
linux-image-powerpc64-smp_3.2.0.131.145
linux-image-3.2.0-131-powerpc-smp_3.2.0-131.177
linux-image-3.2.0-131-powerpc64-smp_3.2.0-131.177
linux-image-virtual_3.2.0.131.145
linux-image-generic_3.2.0.131.145
linux-image-powerpc-smp_3.2.0.131.145
linux-image-3.2.0-131-highbank_3.2.0-131.177
linux-image-3.2.0-131-generic-pae_3.2.0-131.177
linux-image-omap_3.2.0.131.145
linux-image-highbank_3.2.0.131.145
linux-image-3.2.0-131-generic_3.2.0-131.177

192635 - Fedora Linux 25 FEDORA-2017-3a568adb31 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3a568adb31

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/2017/9/?count=200&page=1

Fedora Core 25

imageinfo-0.05-27.fc25
rss-glx-0.9.1.p-27.fc25.1
converseen-0.9.6.2-3.fc25
gtatool-2.2.0-6.fc25
kxstitch-1.2.0-9.fc25
rubygem-rmagick-2.16.0-4.fc25.2

drawtiming-0.7.1-22.fc25
WindowMaker-0.95.7-3.fc25.1
php-pecl-imagick-3.4.3-2.fc25
k3d-0.8.0.6-8.fc25
synfigstudio-1.2.0-5.fc25
vdr-scraper2vdr-1.0.5-4.20170611git254122b.fc25
inkscape-0.92.1-4.20170510bzr15686.fc25.1
ImageMagick-6.9.9.13-1.fc25
ripright-0.11-5.fc25
synfig-1.2.0-1.fc25.1
pfstools-2.0.6-3.fc25
vips-8.4.4-1.fc25.1
techne-0.2.3-20.fc25
perl-Image-SubImageFind-0.03-13.fc25
q-7.11-29.fc25
emacs-25.3-3.fc25
psiconv-0.9.8-22.fc25
autotrace-0.31.1-49.fc25

192638 - Fedora Linux 26 FEDORA-2017-7369ea045c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000251, CVE-2017-12153, CVE-2017-12154

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7369ea045c

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/2017/9/?count=200&page=2

Fedora Core 26

kernel-4.12.13-300.fc26

192639 - Fedora Linux 26 FEDORA-2017-63ff51c0dc Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14226

Description

The scan detected that the host is missing the following update:
FEDORA-2017-63ff51c0dc

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/2017/9/?count=200&page=1

Fedora Core 26

libwpd-0.10.2-1.fc26

192640 - Fedora Linux 26 FEDORA-2017-e7ae1ed967 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12164

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e7ae1ed967

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/2017/9/?count=200&page=2

Fedora Core 26

gdm-3.24.3-1.fc26

192641 - Fedora Linux 26 FEDORA-2017-6679a0a2e1 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-2017-6679a0a2e1

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/2017/9/?count=200&page=2

Fedora Core 26

freexl-1.0.4-1.fc26

192642 - Fedora Linux 26 FEDORA-2017-e4609f71f6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14230

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e4609f71f6

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/2017/9/?count=200&page=2

Fedora Core 26

cyrus-imapd-3.0.4-1.fc26

192651 - Fedora Linux 26 FEDORA-2017-e399a9008c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14316, CVE-2017-14317, CVE-2017-14318, CVE-2017-14319

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e399a9008c

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/2017/9/?count=200&page=2

Fedora Core 26

xen-4.8.2-2.fc26

192653 - Fedora Linux 25 FEDORA-2017-b7e6e4cfc1 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-b7e6e4cfc1

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/2017/9/?count=200&page=2

Fedora Core 25

freexl-1.0.4-1.fc25

145928 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2526-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-11671

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2526-1

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-September/003249.html

SuSE SLED 12 SP2
x86_64
libgcj48-debugsource-4.8.5-31.3.1
gcc48-4.8.5-31.3.1
libstdc++48-devel-32bit-4.8.5-31.3.1
libasan0-4.8.5-31.3.1
libgcj48-debuginfo-4.8.5-31.3.1
cpp48-debuginfo-4.8.5-31.3.1
gcc48-32bit-4.8.5-31.3.1
libgcj48-debuginfo-32bit-4.8.5-31.3.1
gcc48-debugsource-4.8.5-31.3.1
libgcj48-32bit-4.8.5-31.3.1
gcc48-c++-debuginfo-4.8.5-31.3.1
libgcj48-4.8.5-31.3.1
gcc48-gij-debuginfo-4.8.5-31.3.1
gcc48-debuginfo-4.8.5-31.3.1
libasan0-debuginfo-4.8.5-31.3.1
libgcj_bc1-4.8.5-31.3.1
libstdc++48-devel-4.8.5-31.3.1
libasan0-32bit-4.8.5-31.3.1
gcc48-gij-debuginfo-32bit-4.8.5-31.3.1
cpp48-4.8.5-31.3.1
libgcj48-jar-4.8.5-31.3.1
gcc48-gij-32bit-4.8.5-31.3.1
gcc48-c++-4.8.5-31.3.1
gcc48-gij-4.8.5-31.3.1

noarch
gcc48-info-4.8.5-31.3.1

SuSE SLES 12 SP3
noarch
gcc48-info-4.8.5-31.3.1

x86_64
libstdc++48-devel-32bit-4.8.5-31.3.1
libasan0-debuginfo-4.8.5-31.3.1
cpp48-debuginfo-4.8.5-31.3.1
gcc48-32bit-4.8.5-31.3.1
gcc48-c++-debuginfo-4.8.5-31.3.1
libasan0-4.8.5-31.3.1
gcc48-c++-4.8.5-31.3.1
gcc48-debuginfo-4.8.5-31.3.1
gcc48-debugsource-4.8.5-31.3.1
libstdc++48-devel-4.8.5-31.3.1
libasan0-32bit-4.8.5-31.3.1
cpp48-4.8.5-31.3.1
gcc48-4.8.5-31.3.1
gcc48-locale-4.8.5-31.3.1

SuSE SLES 12 SP2
noarch
gcc48-info-4.8.5-31.3.1

x86_64
libstdc++48-devel-32bit-4.8.5-31.3.1
libasan0-debuginfo-4.8.5-31.3.1
cpp48-debuginfo-4.8.5-31.3.1
gcc48-32bit-4.8.5-31.3.1
gcc48-c++-debuginfo-4.8.5-31.3.1
libasan0-4.8.5-31.3.1
gcc48-c++-4.8.5-31.3.1
gcc48-debuginfo-4.8.5-31.3.1
gcc48-debugsource-4.8.5-31.3.1
libstdc++48-devel-4.8.5-31.3.1
libasan0-32bit-4.8.5-31.3.1
cpp48-4.8.5-31.3.1
gcc48-4.8.5-31.3.1
gcc48-locale-4.8.5-31.3.1

SuSE SLED 12 SP3
x86_64
libgcj48-debugsource-4.8.5-31.3.1
gcc48-4.8.5-31.3.1
libstdc++48-devel-32bit-4.8.5-31.3.1
libasan0-4.8.5-31.3.1
libgcj48-debuginfo-4.8.5-31.3.1
cpp48-debuginfo-4.8.5-31.3.1
gcc48-32bit-4.8.5-31.3.1
libgcj48-debuginfo-32bit-4.8.5-31.3.1
gcc48-debugsource-4.8.5-31.3.1
libgcj48-32bit-4.8.5-31.3.1
gcc48-c++-debuginfo-4.8.5-31.3.1
libgcj48-4.8.5-31.3.1
gcc48-gij-debuginfo-4.8.5-31.3.1
gcc48-debuginfo-4.8.5-31.3.1
libasan0-debuginfo-4.8.5-31.3.1
libgcj_bc1-4.8.5-31.3.1
libstdc++48-devel-4.8.5-31.3.1
libasan0-32bit-4.8.5-31.3.1
gcc48-gij-debuginfo-32bit-4.8.5-31.3.1
cpp48-4.8.5-31.3.1
libgcj48-jar-4.8.5-31.3.1
gcc48-gij-32bit-4.8.5-31.3.1
gcc48-c++-4.8.5-31.3.1
gcc48-gij-4.8.5-31.3.1

noarch
gcc48-info-4.8.5-31.3.1

178495 - Gentoo Linux GLSA-201709-14 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000099, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-7407, CVE-2017-7468

Description

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

GLSA-201709-14

Observation

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

https://security.gentoo.org/glsa/201709-14

Affected packages:
net-misc/curl < 7.55.1

192634 - Fedora Linux 26 FEDORA-2017-d793fef58f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8900

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d793fef58f

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/2017/9/?count=200&page=3

Fedora Core 26

lightdm-1.24.0-1.fc26

192637 - Fedora Linux 25 FEDORA-2017-66adafeb3b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8900

Description

The scan detected that the host is missing the following update:
FEDORA-2017-66adafeb3b

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/2017/9/?count=200&page=2

Fedora Core 25

lightdm-1.18.3-5.fc25

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.

32160 - Oracle Solaris 136882-07 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2004-0981, CVE-2005-0397, CVE-2005-0759, CVE-2005-0760, CVE-2005-0761, CVE-2005-0762, CVE-2005-1739, CVE-2005-4601, CVE-2006-0082, CVE-2006-3744, CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988, CVE-2010-4167

Update Details

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

32163 - Oracle Solaris 136883-07 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2004-0981, CVE-2005-0397, CVE-2005-0759, CVE-2005-0760, CVE-2005-0761, CVE-2005-0762, CVE-2005-1739, CVE-2005-4601, CVE-2006-0082, CVE-2006-3744, CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988, CVE-2010-4167

Update Details

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

182338 - FreeBSD mozilla Multiple Vulnerabilities (5e0a038a-ca30-416d-a2f5-38cbf5e7df33)

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2017-5429, CVE-2017-5430, 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-2017-5449, CVE-2017-5450, CVE-2017-5451, CVE-2017-5452, CVE-2017-5453, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5458, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5463, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5468, CVE-2017-5469

Update Details

FASLScript is updated

130869 - Debian Linux 8.0, 9.0 DSA-3961-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6362

Update Details

Risk is updated

182434 - FreeBSD asterisk Remote Crash Vulerability In Res_pjsip (ec1df2a1-8ee6-11e7-8be8-001999f8d30b)

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

Risk Level: Medium

CVE: CVE-2017-14098

Update Details

Risk is updated

182436 - FreeBSD Django Possible XSS In Traceback Section Of Technical 500 Debug Page (aaab03be-932d-11e7-92d8-4b26fc968492)

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

Risk Level: Medium

CVE: CVE-2017-12794

Update Details

Risk is updated

192605 - Fedora Linux 25 FEDORA-2017-270ab2baa3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12133

Update Details

Risk is updated

33234 - Oracle Solaris 146697-06 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33235 - Oracle Solaris 146696-06 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

130875 - Debian Linux 8.0, 9.0 DSA-3970-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14482

Update Details

CVE is updated

182370 - FreeBSD mozilla Multiple Vulnerabilities (6cec1b0a-da15-467d-8691-1dea392d4c8d)

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

Risk Level: Low

CVE: CVE-2017-5470, CVE-2017-5471, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-

2017-7754, CVE-2017-7755, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7759, CVE-2017-7760, CVE-2017-7761, CVE-2017-7762, CVE-2017-7763, CVE-2017-7764, CVE-2017-7765, CVE-2017-7766, CVE-2017-7767, CVE-2017-7768, CVE-2017-7778

Update Details

FASLScript is updated

14462 - openSUSE Obsolete Version Detection

Category: SSH Module -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

45001 - ShellInitialize.fasl3

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.