2016-JUL-07
FSL version 7.5.832

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

144719 - SuSE Linux 13.2 openSUSE-SU-2016:1725-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0749, CVE-2016-2150

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1725-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-07/msg00003.html

SuSE Linux 13.2
x86_64
libspice-server-devel-0.12.4-4.12.1
spice-client-debuginfo-0.12.4-4.12.1
libspice-server1-debuginfo-0.12.4-4.12.1
spice-debugsource-0.12.4-4.12.1
spice-client-0.12.4-4.12.1
libspice-server1-0.12.4-4.12.1

i586
libspice-server-devel-0.12.4-4.12.1
spice-client-debuginfo-0.12.4-4.12.1
libspice-server1-debuginfo-0.12.4-4.12.1
spice-debugsource-0.12.4-4.12.1
spice-client-0.12.4-4.12.1
libspice-server1-0.12.4-4.12.1

144725 - SuSE Linux 13.2 openSUSE-SU-2016:1744-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2099

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1744-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-07/msg00016.html

SuSE Linux 13.2
x86_64
libxerces-c-3_1-debuginfo-3.1.1-13.6.1
xerces-c-3.1.1-13.6.1
xerces-c-debugsource-3.1.1-13.6.1
libxerces-c-3_1-3.1.1-13.6.1
libxerces-c-3_1-32bit-3.1.1-13.6.1
libxerces-c-devel-3.1.1-13.6.1
xerces-c-debuginfo-3.1.1-13.6.1
libxerces-c-3_1-debuginfo-32bit-3.1.1-13.6.1

i586
libxerces-c-3_1-debuginfo-3.1.1-13.6.1
xerces-c-3.1.1-13.6.1
xerces-c-debugsource-3.1.1-13.6.1
libxerces-c-3_1-3.1.1-13.6.1
libxerces-c-devel-3.1.1-13.6.1
xerces-c-debuginfo-3.1.1-13.6.1

144723 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1703-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5745, CVE-2015-7549, CVE-2015-8504, CVE-2015-8558, CVE-2015-8567, CVE-2015-8568, CVE-2015-8613, CVE-2015-8619, CVE-2015-8743, CVE-2015-8744, CVE-2015-8745, CVE-2015-8817, CVE-2015-8818, CVE-2016-1568, CVE-2016-1714, CVE-2016-1922, CVE-2016-1981, CVE-2016-2197, CVE-2016-2198, CVE-2016-2538, CVE-2016-2841, CVE-2016-2857, CVE-2016-2858, CVE-2016-3710, CVE-2016-3712, CVE-2016-4001, CVE-2016-4002, CVE-2016-4020, CVE-2016-4037, CVE-2016-4439, CVE-2016-4441, CVE-2016-4952

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1703-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002141.html

SuSE SLES 12 SP1
noarch
qemu-vgabios-1.8.1-14.1
qemu-seabios-1.8.1-14.1
qemu-ipxe-1.0.0-14.1
qemu-sgabios-8-14.1

x86_64
qemu-block-curl-2.3.1-14.1
qemu-tools-debuginfo-2.3.1-14.1
qemu-guest-agent-debuginfo-2.3.1-14.1
qemu-kvm-2.3.1-14.1
qemu-x86-2.3.1-14.1
qemu-block-rbd-2.3.1-14.1

qemu-block-rbd-debuginfo-2.3.1-14.1
qemu-guest-agent-2.3.1-14.1
qemu-lang-2.3.1-14.1
qemu-debugsource-2.3.1-14.1
qemu-block-curl-debuginfo-2.3.1-14.1
qemu-2.3.1-14.1
qemu-tools-2.3.1-14.1

SuSE SLED 12 SP1
x86_64
qemu-kvm-2.3.1-14.1
qemu-debugsource-2.3.1-14.1
qemu-x86-2.3.1-14.1
qemu-tools-2.3.1-14.1
qemu-block-curl-debuginfo-2.3.1-14.1
qemu-tools-debuginfo-2.3.1-14.1
qemu-block-curl-2.3.1-14.1
qemu-2.3.1-14.1

noarch
qemu-vgabios-1.8.1-14.1
qemu-seabios-1.8.1-14.1
qemu-ipxe-1.0.0-14.1
qemu-sgabios-8-14.1

144729 - SuSE SLED 12, 12 SP1 SUSE-SU-2016:1728-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0794, CVE-2016-0795

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1728-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-July/002146.html

SuSE SLED 12
x86_64
libboost_date_time1_54_0-1.54.0-15.1
hunspell-1.3.2-18.1
libboost_iostreams1_54_0-debuginfo-1.54.0-15.1
libboost_regex1_54_0-1.54.0-15.1
libreoffice-impress-5.1.3.2-22.9
libvisio-0_1-1-0.1.5-7.1
libwps-0_4-4-debuginfo-0.4.2-6.1
libhyphen0-debuginfo-2.8.8-12.1
libreoffice-calc-extensions-5.1.3.2-22.9
libreoffice-officebean-debuginfo-5.1.3.2-22.9
libOpenCOLLADA0-1_3335ac1-2.1
libboost_atomic1_54_0-1.54.0-15.1
libreoffice-impress-debuginfo-5.1.3.2-22.9
liborcus-debugsource-0.11.0-6.1
myspell-lightproof-ru_RU-20160511-11.1

libreoffice-math-5.1.3.2-22.9
libreoffice-pyuno-debuginfo-5.1.3.2-22.9
liborcus-0_11-0-debuginfo-0.11.0-6.1
libetonyek-debugsource-0.1.6-6.3
libixion-debugsource-0.11.0-6.2
libcmis-0_5-5-0.5.1-8.2
hunspell-tools-debuginfo-1.3.2-18.1
cmis-client-debuginfo-0.5.1-8.2
libboost_filesystem1_54_0-debuginfo-1.54.0-15.1
libcmis-0_5-5-debuginfo-0.5.1-8.2
libreoffice-pyuno-5.1.3.2-22.9
hunspell-debugsource-1.3.2-18.1
myspell-dictionaries-20160511-11.1
libvisio-0_1-1-debuginfo-0.1.5-7.1
cmis-client-debugsource-0.5.1-8.2
libboost_system1_54_0-debuginfo-1.54.0-15.1
libreoffice-draw-debuginfo-5.1.3.2-22.9
libwps-debugsource-0.4.2-6.1
libboost_filesystem1_54_0-1.54.0-15.1
libreoffice-base-drivers-postgresql-debuginfo-5.1.3.2-22.9
myspell-lightproof-en-20160511-11.1
libreoffice-5.1.3.2-22.9
libboost_program_options1_54_0-debuginfo-1.54.0-15.1
libboost_atomic1_54_0-debuginfo-1.54.0-15.1
myspell-lightproof-hu_HU-20160511-11.1
libhyphen0-2.8.8-12.1
libvisio-debugsource-0.1.5-7.1
libreoffice-debuginfo-5.1.3.2-22.9
hunspell-debuginfo-1.3.2-18.1
hunspell-tools-1.3.2-18.1
libboost_iostreams1_54_0-1.54.0-15.1
hunspell-debuginfo-32bit-1.3.2-18.1
hyphen-debugsource-2.8.8-12.1
libreoffice-writer-5.1.3.2-22.9
libetonyek-0_1-1-debuginfo-0.1.6-6.3
libboost_thread1_54_0-1.54.0-15.1
libboost_thread1_54_0-debuginfo-1.54.0-15.1
libreoffice-base-drivers-mysql-debuginfo-5.1.3.2-22.9
myspell-lightproof-pt_BR-20160511-11.1
libOpenCOLLADA0-debuginfo-1_3335ac1-2.1
libreoffice-gnome-debuginfo-5.1.3.2-22.9
libreoffice-calc-5.1.3.2-22.9
libboost_system1_54_0-1.54.0-15.1
libreoffice-mailmerge-5.1.3.2-22.9
libreoffice-gnome-5.1.3.2-22.9
libreoffice-base-drivers-mysql-5.1.3.2-22.9
libreoffice-filters-optional-5.1.3.2-22.9
libreoffice-base-5.1.3.2-22.9
libreoffice-calc-debuginfo-5.1.3.2-22.9
libboost_date_time1_54_0-debuginfo-1.54.0-15.1
liborcus-0_11-0-0.11.0-6.1
libboost_program_options1_54_0-1.54.0-15.1
libboost_regex1_54_0-debuginfo-1.54.0-15.1
libreoffice-writer-extensions-5.1.3.2-22.9
libreoffice-math-debuginfo-5.1.3.2-22.9
libboost_signals1_54_0-debuginfo-1.54.0-15.1
libreoffice-base-debuginfo-5.1.3.2-22.9
libreoffice-writer-debuginfo-5.1.3.2-22.9
libwps-0_4-4-0.4.2-6.1
libreoffice-draw-5.1.3.2-22.9

libixion-0_11-0-0.11.0-6.2
libreoffice-debugsource-5.1.3.2-22.9
libboost_signals1_54_0-1.54.0-15.1
hunspell-32bit-1.3.2-18.1
libixion-0_11-0-debuginfo-0.11.0-6.2
libreoffice-base-drivers-postgresql-5.1.3.2-22.9
libetonyek-0_1-1-0.1.6-6.3
libreoffice-officebean-5.1.3.2-22.9

noarch
myspell-ar_EG-20160511-11.1
myspell-ar_IQ-20160511-11.1
myspell-sv_FI-20160511-11.1
myspell-ro_RO-20160511-11.1
myspell-en_NA-20160511-11.1
libreoffice-l10n-pt-BR-5.1.3.2-22.9
myspell-el_GR-20160511-11.1
myspell-ar_SA-20160511-11.1
myspell-af_ZA-20160511-11.1
libreoffice-l10n-en-5.1.3.2-22.9
libreoffice-l10n-sv-5.1.3.2-22.9
libreoffice-l10n-hi-5.1.3.2-22.9
myspell-af_NA-20160511-11.1
myspell-ar_LB-20160511-11.1
myspell-et_EE-20160511-11.1
myspell-pl_PL-20160511-11.1
myspell-en_IE-20160511-11.1
myspell-ca_IT-20160511-11.1
myspell-en-20160511-11.1
myspell-ar_OM-20160511-11.1
myspell-hi_IN-20160511-11.1
libreoffice-l10n-pl-5.1.3.2-22.9
myspell-es_CR-20160511-11.1
myspell-en_TT-20160511-11.1
myspell-es_PA-20160511-11.1
myspell-es_AR-20160511-11.1
myspell-en_PH-20160511-11.1
myspell-en_MW-20160511-11.1
myspell-th_TH-20160511-11.1
libreoffice-l10n-nn-5.1.3.2-22.9
libreoffice-l10n-zh-Hant-5.1.3.2-22.9
myspell-nl_BE-20160511-11.1
myspell-en_BS-20160511-11.1
myspell-cs_CZ-20160511-11.1
myspell-zu_ZA-20160511-11.1
myspell-de_DE-20160511-11.1
myspell-ar_YE-20160511-11.1
myspell-es_VE-20160511-11.1
myspell-en_ZA-20160511-11.1
myspell-vi-20160511-11.1
libreoffice-l10n-da-5.1.3.2-22.9
myspell-es_EC-20160511-11.1
myspell-en_IN-20160511-11.1
myspell-es_NI-20160511-11.1
myspell-ar_SD-20160511-11.1
myspell-ar-20160511-11.1
myspell-en_US-20160511-11.1
myspell-he_IL-20160511-11.1
libreoffice-l10n-af-5.1.3.2-22.9
myspell-hu_HU-20160511-11.1

myspell-es_MX-20160511-11.1
myspell-sr_CS-20160511-11.1
myspell-fr_BE-20160511-11.1
myspell-sr-20160511-11.1
myspell-sl_SI-20160511-11.1
myspell-bn_BD-20160511-11.1
myspell-ar_BH-20160511-11.1
libreoffice-l10n-gu-5.1.3.2-22.9
libreoffice-l10n-nb-5.1.3.2-22.9
myspell-ru_RU-20160511-11.1
myspell-ca_ES_valencia-20160511-11.1
myspell-es_UY-20160511-11.1
myspell-es_DO-20160511-11.1
myspell-te-20160511-11.1
myspell-hr_HR-20160511-11.1
myspell-sr_Latn_CS-20160511-11.1
libreoffice-l10n-it-5.1.3.2-22.9
myspell-en_BZ-20160511-11.1
myspell-ar_LY-20160511-11.1
myspell-es-20160511-11.1
libreoffice-l10n-ar-5.1.3.2-22.9
myspell-fr_FR-20160511-11.1
myspell-ar_SY-20160511-11.1
myspell-bs-20160511-11.1
myspell-bn_IN-20160511-11.1
myspell-fr_CA-20160511-11.1
libreoffice-l10n-zh-Hans-5.1.3.2-22.9
myspell-en_NZ-20160511-11.1
libreoffice-l10n-fi-5.1.3.2-22.9
myspell-en_GB-20160511-11.1
myspell-de_CH-20160511-11.1
myspell-es_CO-20160511-11.1
myspell-es_CL-20160511-11.1
myspell-bs_BA-20160511-11.1
myspell-es_GT-20160511-11.1
libreoffice-l10n-es-5.1.3.2-22.9
myspell-es_BO-20160511-11.1
myspell-sr_Latn_RS-20160511-11.1
myspell-bg_BG-20160511-11.1
myspell-es_PY-20160511-11.1
libreoffice-l10n-sk-5.1.3.2-22.9
libreoffice-l10n-nl-5.1.3.2-22.9
myspell-ca-20160511-11.1
myspell-da_DK-20160511-11.1
myspell-en_ZW-20160511-11.1
myspell-pt_AO-20160511-11.1
libreoffice-l10n-zu-5.1.3.2-22.9
myspell-ar_DZ-20160511-11.1
myspell-sk_SK-20160511-11.1
myspell-nl_NL-20160511-11.1
myspell-no-20160511-11.1
libreoffice-icon-theme-galaxy-5.1.3.2-22.9
myspell-fr_LU-20160511-11.1
myspell-es_HN-20160511-11.1
myspell-en_JM-20160511-11.1
libreoffice-l10n-hu-5.1.3.2-22.9
myspell-lv_LV-20160511-11.1
myspell-gu_IN-20160511-11.1
myspell-de-20160511-11.1
myspell-sv_SE-20160511-11.1

myspell-nn_NO-20160511-11.1
myspell-ar_QA-20160511-11.1
libreoffice-l10n-ru-5.1.3.2-22.9
libreoffice-l10n-ja-5.1.3.2-22.9
libreoffice-l10n-ca-5.1.3.2-22.9
myspell-pt_PT-20160511-11.1
myspell-fr_CH-20160511-11.1
myspell-te_IN-20160511-11.1
myspell-en_GH-20160511-11.1
myspell-es_PR-20160511-11.1
libreoffice-l10n-cs-5.1.3.2-22.9
myspell-en_AU-20160511-11.1
myspell-fr_MC-20160511-11.1
libreoffice-icon-theme-tango-5.1.3.2-22.9
libreoffice-l10n-xh-5.1.3.2-22.9
myspell-nb_NO-20160511-11.1
myspell-ar_TN-20160511-11.1
myspell-ca_FR-20160511-11.1
myspell-ca_AD-20160511-11.1

SuSE SLED 12 SP1
x86_64
libboost_date_time1_54_0-1.54.0-15.1

20250 - IBM WebSphere Application Server Liberty Profile Apache Standard Taglibs XML External Entity Injection Vulnerability (swg2197849

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

Risk Level: High

CVE: CVE-2015-0254

Description

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

Observation

IBM WebSphere Application Server Liberty Profile is a Java EE application server.

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

144720 - SuSE Linux 13.2 openSUSE-SU-2016:1724-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9805, CVE-2014-9807, CVE-2014-9808, CVE-2014-9809, CVE-2014-9810, CVE-2014-9811, CVE-2014-9813, CVE-2014-9814, CVE-2014-9815, CVE-2014-9816, CVE-2014-9817, CVE-2014-9818, CVE-2014-9819, CVE-2014-9820, CVE-2014-9828, CVE-2014-9829, CVE-2014-9830, CVE-2014-9831, CVE-2014-9834, CVE-2014-9835, CVE-2014-9837, CVE-2014-9839, CVE-2014-9840, CVE-2014-9844, CVE-2014-9845, CVE-2014-9846, CVE-2014-9847, CVE-2014-9853, CVE-2015-8894, CVE-2015-8896, CVE-2015-8901, CVE-2015-8903, CVE-2016-2317, CVE-2016-2318, CVE-2016-5240, CVE-2016-5241, CVE-2016-5688

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1724-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-07/msg00002.html

SuSE Linux 13.2
x86_64
libGraphicsMagick-Q16-3-debuginfo-1.3.20-9.1
GraphicsMagick-debugsource-1.3.20-9.1
GraphicsMagick-devel-1.3.20-9.1
perl-GraphicsMagick-1.3.20-9.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-9.1
libGraphicsMagick3-config-1.3.20-9.1
libGraphicsMagick++-Q16-3-1.3.20-9.1
libGraphicsMagick-Q16-3-1.3.20-9.1
perl-GraphicsMagick-debuginfo-1.3.20-9.1
libGraphicsMagick++-devel-1.3.20-9.1
GraphicsMagick-1.3.20-9.1
libGraphicsMagickWand-Q16-2-1.3.20-9.1
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-9.1
GraphicsMagick-debuginfo-1.3.20-9.1

i586
libGraphicsMagick-Q16-3-debuginfo-1.3.20-9.1
GraphicsMagick-debugsource-1.3.20-9.1
GraphicsMagick-devel-1.3.20-9.1
perl-GraphicsMagick-1.3.20-9.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-9.1
libGraphicsMagick3-config-1.3.20-9.1
libGraphicsMagick++-Q16-3-1.3.20-9.1
libGraphicsMagick-Q16-3-1.3.20-9.1
perl-GraphicsMagick-debuginfo-1.3.20-9.1
libGraphicsMagick++-devel-1.3.20-9.1
GraphicsMagick-1.3.20-9.1
libGraphicsMagickWand-Q16-2-1.3.20-9.1
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-9.1
GraphicsMagick-debuginfo-1.3.20-9.1

144721 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1721-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1234, CVE-2016-3075, CVE-2016-3706, CVE-2016-4429

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1721-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002145.html

SuSE SLED 12
x86_64
nscd-2.19-22.16.2
glibc-devel-debuginfo-2.19-22.16.2

glibc-locale-32bit-2.19-22.16.2
glibc-2.19-22.16.2
glibc-devel-2.19-22.16.2
glibc-debuginfo-2.19-22.16.2
glibc-locale-2.19-22.16.2
glibc-devel-32bit-2.19-22.16.2
nscd-debuginfo-2.19-22.16.2
glibc-locale-debuginfo-2.19-22.16.2
glibc-32bit-2.19-22.16.2
glibc-devel-debuginfo-32bit-2.19-22.16.2
glibc-debuginfo-32bit-2.19-22.16.2
glibc-locale-debuginfo-32bit-2.19-22.16.2
glibc-debugsource-2.19-22.16.2

noarch
glibc-i18ndata-2.19-22.16.2

SuSE SLES 12
noarch
glibc-i18ndata-2.19-22.16.2
glibc-html-2.19-22.16.2
glibc-info-2.19-22.16.2

x86_64
nscd-2.19-22.16.2
glibc-devel-debuginfo-2.19-22.16.2
glibc-profile-32bit-2.19-22.16.2
nscd-debuginfo-2.19-22.16.2
glibc-2.19-22.16.2
glibc-devel-2.19-22.16.2
glibc-debuginfo-2.19-22.16.2
glibc-locale-2.19-22.16.2
glibc-locale-32bit-2.19-22.16.2
glibc-profile-2.19-22.16.2
glibc-locale-debuginfo-2.19-22.16.2
glibc-32bit-2.19-22.16.2
glibc-devel-debuginfo-32bit-2.19-22.16.2
glibc-debuginfo-32bit-2.19-22.16.2
glibc-locale-debuginfo-32bit-2.19-22.16.2
glibc-debugsource-2.19-22.16.2
glibc-devel-32bit-2.19-22.16.2

144722 - SuSE Linux 13.2 openSUSE-SU-2016:1723-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3100

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1723-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-07/msg00001.html

SuSE Linux 13.2
i586
kinit-debugsource-5.11.0-27.1
kinit-devel-5.11.0-27.1
kinit-debuginfo-5.11.0-27.1
kinit-5.11.0-27.1

noarch
kinit-lang-5.11.0-27.1

x86_64
kinit-debuginfo-5.11.0-27.1
kinit-devel-5.11.0-27.1
kinit-debuginfo-32bit-5.11.0-27.1
kinit-32bit-5.11.0-27.1
kinit-debugsource-5.11.0-27.1
kinit-5.11.0-27.1

144724 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1710-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4997, CVE-2016-4998

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1710-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002144.html

SuSE SLED 12
x86_64
kernel-xen-debugsource-3.12.60-52.54.2
kernel-default-debugsource-3.12.60-52.54.2
kernel-default-devel-3.12.60-52.54.2
kernel-xen-debuginfo-3.12.60-52.54.2
kernel-default-debuginfo-3.12.60-52.54.2
kernel-default-3.12.60-52.54.2
kernel-xen-devel-3.12.60-52.54.2
kernel-default-extra-3.12.60-52.54.2
kernel-syms-3.12.60-52.54.1
kernel-xen-3.12.60-52.54.2
kernel-default-extra-debuginfo-3.12.60-52.54.2

noarch
kernel-devel-3.12.60-52.54.1
kernel-macros-3.12.60-52.54.1
kernel-source-3.12.60-52.54.1

SuSE SLES 12
noarch
kernel-devel-3.12.60-52.54.1
kernel-macros-3.12.60-52.54.1
kernel-source-3.12.60-52.54.1

x86_64
kernel-xen-debuginfo-3.12.60-52.54.2
kernel-xen-base-debuginfo-3.12.60-52.54.2
kernel-xen-devel-3.12.60-52.54.2
kernel-xen-3.12.60-52.54.2
kernel-default-debuginfo-3.12.60-52.54.2
kernel-default-devel-3.12.60-52.54.2
kernel-default-debugsource-3.12.60-52.54.2
kernel-default-3.12.60-52.54.2
kernel-default-base-debuginfo-3.12.60-52.54.2
kernel-syms-3.12.60-52.54.1
kernel-xen-base-3.12.60-52.54.2
kernel-xen-debugsource-3.12.60-52.54.2
kernel-default-base-3.12.60-52.54.2

144726 - SuSE Linux 13.2 openSUSE-SU-2016:1737-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1737-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-07/msg00009.html

SuSE Linux 13.2
x86_64
libircclient1-1.6-8.3.1
libircclient-devel-1.6-8.3.1
libircclient-doc-1.6-8.3.1

i586
libircclient1-1.6-8.3.1
libircclient-devel-1.6-8.3.1
libircclient-doc-1.6-8.3.1

144727 - SuSE Linux 13.2 openSUSE-SU-2016:1741-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3992

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1741-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-07/msg00013.html

SuSE Linux 13.2
noarch
cronic-3-3.1

144728 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1733-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1234, CVE-2016-3075, CVE-2016-3706, CVE-2016-4429

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1733-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-July/002147.html

SuSE SLES 12 SP1
noarch
glibc-i18ndata-2.19-38.2
glibc-html-2.19-38.2
glibc-info-2.19-38.2

x86_64
glibc-profile-32bit-2.19-38.2
glibc-locale-debuginfo-32bit-2.19-38.2
nscd-2.19-38.2
glibc-debuginfo-32bit-2.19-38.2
glibc-debugsource-2.19-38.2
glibc-devel-debuginfo-2.19-38.2
glibc-devel-debuginfo-32bit-2.19-38.2
glibc-profile-2.19-38.2
glibc-2.19-38.2
glibc-locale-2.19-38.2
glibc-locale-debuginfo-2.19-38.2
glibc-devel-2.19-38.2
glibc-locale-32bit-2.19-38.2
nscd-debuginfo-2.19-38.2
glibc-debuginfo-2.19-38.2
glibc-devel-32bit-2.19-38.2
glibc-32bit-2.19-38.2

SuSE SLED 12 SP1
x86_64
glibc-locale-debuginfo-32bit-2.19-38.2
nscd-2.19-38.2
glibc-debuginfo-32bit-2.19-38.2
glibc-debugsource-2.19-38.2
glibc-devel-debuginfo-2.19-38.2
glibc-devel-debuginfo-32bit-2.19-38.2
glibc-2.19-38.2
glibc-locale-2.19-38.2
glibc-locale-debuginfo-2.19-38.2

glibc-devel-2.19-38.2
nscd-debuginfo-2.19-38.2
glibc-locale-32bit-2.19-38.2
glibc-debuginfo-2.19-38.2
glibc-devel-32bit-2.19-38.2
glibc-32bit-2.19-38.2

noarch
glibc-i18ndata-2.19-38.2

144730 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1709-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4997, CVE-2016-4998

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1709-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002143.html

SuSE SLES 12 SP1
noarch
kernel-devel-3.12.59-60.45.1
kernel-macros-3.12.59-60.45.1
kernel-source-3.12.59-60.45.1

x86_64
kernel-xen-debuginfo-3.12.59-60.45.2
kernel-default-base-debuginfo-3.12.59-60.45.2
kernel-default-debuginfo-3.12.59-60.45.2
kernel-xen-debugsource-3.12.59-60.45.2
kernel-default-base-3.12.59-60.45.2
kernel-xen-base-debuginfo-3.12.59-60.45.2
kernel-xen-3.12.59-60.45.2
kernel-default-3.12.59-60.45.2
kernel-xen-base-3.12.59-60.45.2
kernel-default-debugsource-3.12.59-60.45.2
kernel-syms-3.12.59-60.45.1
kernel-xen-devel-3.12.59-60.45.2
kernel-default-devel-3.12.59-60.45.2

SuSE SLED 12 SP1
x86_64
kernel-xen-debuginfo-3.12.59-60.45.2
kernel-xen-debugsource-3.12.59-60.45.2
kernel-xen-3.12.59-60.45.2
kernel-default-devel-3.12.59-60.45.2
kernel-xen-devel-3.12.59-60.45.2
kernel-default-debugsource-3.12.59-60.45.2
kernel-default-extra-3.12.59-60.45.2
kernel-default-3.12.59-60.45.2
kernel-default-debuginfo-3.12.59-60.45.2

kernel-syms-3.12.59-60.45.1
kernel-default-extra-debuginfo-3.12.59-60.45.2

noarch
kernel-devel-3.12.59-60.45.1
kernel-macros-3.12.59-60.45.1
kernel-source-3.12.59-60.45.1

144731 - SuSE SLES 11 SP4 SUSE-SU-2016:1707-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1339, CVE-2015-7566, CVE-2015-8551, CVE-2015-8552, CVE-2015-8816, CVE-2016-2143, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-2782, CVE-2016-2847, CVE-2016-3137, CVE-2016-3138, CVE-2016-3139, CVE-2016-3140, CVE-2016-3156

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1707-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-June/002142.html

SuSE SLES 11 SP4
x86_64
kernel-rt_trace-devel-3.0.101.rt130-54.1
kernel-rt-devel-3.0.101.rt130-54.1
kernel-rt_trace-base-3.0.101.rt130-54.1
kernel-rt-3.0.101.rt130-54.1
kernel-rt-base-3.0.101.rt130-54.1
kernel-syms-rt-3.0.101.rt130-54.1
kernel-source-rt-3.0.101.rt130-54.1
kernel-rt_trace-3.0.101.rt130-54.1

144732 - SuSE Linux 13.2 openSUSE-SU-2016:1727-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4994

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1727-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-07/msg00005.html

SuSE Linux 13.2
i586
gimp-debugsource-2.8.16-3.1

gimp-debuginfo-2.8.16-3.1
libgimpui-2_0-0-2.8.16-3.1
gimp-plugin-aa-debuginfo-2.8.16-3.1
gimp-help-browser-debuginfo-2.8.16-3.1
libgimpui-2_0-0-debuginfo-2.8.16-3.1
libgimp-2_0-0-debuginfo-2.8.16-3.1
gimp-2.8.16-3.1
gimp-devel-2.8.16-3.1
gimp-plugins-python-2.8.16-3.1
libgimp-2_0-0-2.8.16-3.1
gimp-plugins-python-debuginfo-2.8.16-3.1
gimp-help-browser-2.8.16-3.1
gimp-devel-debuginfo-2.8.16-3.1
gimp-plugin-aa-2.8.16-3.1

noarch
gimp-lang-2.8.16-3.1

x86_64
libgimpui-2_0-0-debuginfo-32bit-2.8.16-3.1
gimp-debugsource-2.8.16-3.1
gimp-debuginfo-2.8.16-3.1
libgimp-2_0-0-debuginfo-32bit-2.8.16-3.1
libgimpui-2_0-0-2.8.16-3.1
gimp-plugin-aa-debuginfo-2.8.16-3.1
gimp-help-browser-debuginfo-2.8.16-3.1
libgimpui-2_0-0-debuginfo-2.8.16-3.1
libgimp-2_0-0-debuginfo-2.8.16-3.1
libgimp-2_0-0-32bit-2.8.16-3.1
gimp-2.8.16-3.1
libgimpui-2_0-0-32bit-2.8.16-3.1
gimp-devel-2.8.16-3.1
gimp-plugins-python-2.8.16-3.1
libgimp-2_0-0-2.8.16-3.1
gimp-plugins-python-debuginfo-2.8.16-3.1
gimp-help-browser-2.8.16-3.1
gimp-devel-debuginfo-2.8.16-3.1
gimp-plugin-aa-2.8.16-3.1

181995 - FreeBSD openssl Denial Of Service (0ca24682-3f03-11e6-b3c8-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2016-2177

Description

The scan detected that the host is missing the following update:
openssl -- denial of service (0ca24682-3f03-11e6-b3c8-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/0ca24682-3f03-11e6-b3c8-14dae9d210b8.html

Affected packages:
openssl < 1.0.2_14

181996 - FreeBSD xen-tools QEMU: Banked Access To VGA Memory (VBE) uses inconsistent bounds checks (e6ce6f50-4212-11e6-942d-bc5ff45d0f28)

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

Risk Level: High

CVE: CVE-2016-3710, CVE-2016-3712

Description

The scan detected that the host is missing the following update:
xen-tools -- QEMU: Banked access to VGA memory (VBE) uses inconsistent bounds checks (e6ce6f50-4212-11e6-942d-bc5ff45d0f28)

Observation

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

http://www.vuxml.org/freebsd/e6ce6f50-4212-11e6-942d-bc5ff45d0f28.html

Affected packages:
xen-tools < 4.7.0_2

181997 - FreeBSD hive Authorization Logic Vulnerability (a5c204b5-4153-11e6-8dfe-002590263bf5)

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

Risk Level: High

CVE: CVE-2015-7521

Description

The scan detected that the host is missing the following update:
hive -- authorization logic vulnerability (a5c204b5-4153-11e6-8dfe-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/a5c204b5-4153-11e6-8dfe-002590263bf5.html

Affected packages:
hive < 2.0.0

181998 - FreeBSD xen-kernel X86 Shadow Pagetables: Address Width Overflow (d51ced72-4212-11e6-942d-bc5ff45d0f28)

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

Risk Level: High

CVE: CVE-2016-3960

Description

The scan detected that the host is missing the following update:
xen-kernel -- x86 shadow pagetables: address width overflow (d51ced72-4212-11e6-942d-bc5ff45d0f28)

Observation

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

http://www.vuxml.org/freebsd/d51ced72-4212-11e6-942d-bc5ff45d0f28.html

Affected packages:
3.4 <= xen-kernel < 4.7.0

182005 - FreeBSD xen-kernel X86 Software Guest Page Walk PS Bit Handling Flaw (e43b210a-4212-11e6-942d-bc5ff45d0f28)

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

Risk Level: High

CVE: CVE-2016-4480

Description

The scan detected that the host is missing the following update:
xen-kernel -- x86 software guest page walk PS bit handling flaw (e43b210a-4212-11e6-942d-bc5ff45d0f28)

Observation

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

http://www.vuxml.org/freebsd/e43b210a-4212-11e6-942d-bc5ff45d0f28.html

Affected packages:
xen-kernel < 4.7.0

130530 - Debian Linux 8.0 DSA-3609-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5174, CVE-2015-5345, CVE-2015-5346, CVE-2015-5351, CVE-2016-0706, CVE-2016-0714, CVE-2016-0763, CVE-2016-3092

Description

The scan detected that the host is missing the following update:
DSA-3609-1

Observation

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

http://www.debian.org/security/2016/dsa-3609

Debian 8.0
all
tomcat8_8.0.14-1+deb8u2

182001 - FreeBSD xen-tools Unsanitised Guest Input In Libxl Device Handling Code (e2fca11b-4212-11e6-942d-bc5ff45d0f28)

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

Risk Level: Medium

CVE: CVE-2016-4962

Description

The scan detected that the host is missing the following update:
xen-tools -- Unsanitised guest input in libxl device handling code (e2fca11b-4212-11e6-942d-bc5ff45d0f28)

Observation

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

http://www.vuxml.org/freebsd/e2fca11b-4212-11e6-942d-bc5ff45d0f28.html

Affected packages:
xen-tools < 4.7.0_1

185342 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-3024-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5174, CVE-2015-5345, CVE-2015-5346, CVE-2015-5351, CVE-2016-0706, CVE-2016-0714, CVE-2016-0763, CVE-2016-3092

Description

The scan detected that the host is missing the following update:
USN-3024-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-July/003487.html

Ubuntu 12.04

libtomcat6-java_6.0.35-1ubuntu3.7

Ubuntu 16.04

libtomcat7-java_7.0.68-1ubuntu0.1

Ubuntu 15.10

libtomcat7-java_7.0.64-1ubuntu0.3

Ubuntu 14.04

libtomcat7-java_7.0.52-1ubuntu0.6

20246 - LibreOffice RTF File Processing Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-4324

Description

A denial of service vulnerability is present in some versions of LibreOffice.

Observation

LibreOffice is an open source office suite.

A denial of service vulnerability is present in some versions of LibreOffice. The flaw occurs due to dereference of an invalid STL iterator when processing and RTF file. Successful exploitation could allow an attacker to cause a denial of service condition.

141218 - Red Hat Enterprise Linux RHSA-2016-1380 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7191

Description

The scan detected that the host is missing the following update:
RHSA-2016-1380

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-July/msg00002.html

RHEL6_6S
noarch
nodejs010-nodejs-qs-0.6.5-5.el6
nodejs010-node-gyp-3.2.0-3.el6

RHEL6S
noarch
nodejs010-nodejs-qs-0.6.5-5.el6
nodejs010-node-gyp-3.2.0-3.el6

RHEL6WS
noarch
nodejs010-nodejs-qs-0.6.5-5.el6
nodejs010-node-gyp-3.2.0-3.el6

RHEL7S
noarch
nodejs010-node-gyp-3.2.0-3.el7
nodejs010-nodejs-qs-0.6.5-5.el7

RHEL7WS
noarch
nodejs010-node-gyp-3.2.0-3.el7
nodejs010-nodejs-qs-0.6.5-5.el7

185344 - Ubuntu Linux 14.04, 15.10, 16.04 USN-3026-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5104

Description

The scan detected that the host is missing the following update:
USN-3026-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-July/003489.html

Ubuntu 16.04

libimobiledevice6_1.2.0+dfsg-3~ubuntu0.2

Ubuntu 15.10

libimobiledevice4_1.1.6+dfsg-3.1ubuntu0.1

Ubuntu 14.04

libimobiledevice4_1.1.5+git20140313.bafe6a9e-0ubuntu1.1

185345 - Ubuntu Linux 15.10, 16.04 USN-3026-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5104

Description

The scan detected that the host is missing the following update:
USN-3026-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-July/003490.html

Ubuntu 15.10

libusbmuxd2_1.0.9-1ubuntu0.1

Ubuntu 16.04

libusbmuxd4_1.0.10-2ubuntu0.1

88788 - Slackware Linux 14.1, 14.2 SSA:2016-187-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2016-187-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.405271

Slackware 14.1
x86_64
mozilla-thunderbird-45.2.0-x86_64-1

Slackware 14.2
x86_64
mozilla-thunderbird-45.2.0-x86_64-1

i586
mozilla-thunderbird-45.2.0-i586-1

130525 - Debian Linux 8.0 DSA-3612-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4994

Description

The scan detected that the host is missing the following update:
DSA-3612-1

Observation

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

http://www.debian.org/security/2016/dsa-3612

Debian 8.0
all
gimp_2.8.14-1+deb8u1

130526 - Debian Linux 8.0 DSA-3615-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5350, CVE-2016-5351, CVE-2016-5353, CVE-2016-5354, CVE-2016-5355, CVE-2016-5356, CVE-2016-5357, CVE-2016-5359

Description

The scan detected that the host is missing the following update:
DSA-3615-1

Observation

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

http://www.debian.org/security/2016/dsa-3615

Debian 8.0
all
wireshark_1.12.1+g01b65bf-4+deb8u7

130527 - Debian Linux 8.0 DSA-3611-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3092

Description

The scan detected that the host is missing the following update:
DSA-3611-1

Observation

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

http://www.debian.org/security/2016/dsa-3611

Debian 8.0
all
libcommons-fileupload-java_1.3.1-1+deb8u1

130528 - Debian Linux 8.0 DSA-3614-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3092

Description

The scan detected that the host is missing the following update:
DSA-3614-1

Observation

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

http://www.debian.org/security/2016/dsa-3614

Debian 8.0
all
tomcat7_7.0.56-3+deb8u3

130529 - Debian Linux 8.0 DSA-3610-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4463

Description

The scan detected that the host is missing the following update:
DSA-3610-1

Observation

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

http://www.debian.org/security/2016/dsa-3610

Debian 8.0
all
libxerces-c-doc_3.1.1-5.1+deb8u3
libxerces-c-samples_3.1.1-5.1+deb8u3
libxerces-c-dev_3.1.1-5.1+deb8u3
libxerces-c3.1_3.1.1-5.1+deb8u3

130531 - Debian Linux 8.0 DSA-3613-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5008

Description

The scan detected that the host is missing the following update:
DSA-3613-1

Observation

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

http://www.debian.org/security/2016/dsa-3613

Debian 8.0
all
libvirt-clients_1.2.9-9+deb8u3
libvirt-sanlock_1.2.9-9+deb8u3
libvirt0_1.2.9-9+deb8u3
libvirt-doc_1.2.9-9+deb8u3
libvirt-daemon-system_1.2.9-9+deb8u3
libvirt-bin_1.2.9-9+deb8u3
libvirt-daemon_1.2.9-9+deb8u3
libvirt0-dbg_1.2.9-9+deb8u3
libvirt-dev_1.2.9-9+deb8u3

130532 - Debian Linux 8.0 DSA-3616-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-9904, CVE-2016-5728, CVE-2016-5828, CVE-2016-5829, CVE-2016-6130

Description

The scan detected that the host is missing the following update:
DSA-3616-1

Observation

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

http://www.debian.org/security/2016/dsa-3616

Debian 8.0
all
crypto-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3

kernel-image-3.16.0-4-octeon-di_3.16.7-ckt25-2+deb8u3
hfs-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
squashfs-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
speakup-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
sound-modules-3.16.0-4-octeon-di_3.16.7-ckt25-2+deb8u3
zlib-modules-3.16.0-4-versatile-di_3.16.7-ckt25-2+deb8u3
udf-modules-3.16.0-4-orion5x-di_3.16.7-ckt25-2+deb8u3
sata-modules-3.16.0-4-octeon-di_3.16.7-ckt25-2+deb8u3
squashfs-modules-3.16.0-4-orion5x-di_3.16.7-ckt25-2+deb8u3
fat-modules-3.16.0-4-586-di_3.16.7-ckt25-2+deb8u3
udf-modules-3.16.0-4-armmp-di_3.16.7-ckt25-2+deb8u3
nic-shared-modules-3.16.0-4-armmp-di_3.16.7-ckt25-2+deb8u3
crypto-modules-3.16.0-4-powerpc-di_3.16.7-ckt25-2+deb8u3
nic-pcmcia-modules-3.16.0-4-powerpc64-di_3.16.7-ckt25-2+deb8u3
linux-headers-3.16.0-4-powerpc_3.16.7-ckt25-2+deb8u3
mtd-modules-3.16.0-4-armmp-di_3.16.7-ckt25-2+deb8u3
uinput-modules-3.16.0-4-armmp-di_3.16.7-ckt25-2+deb8u3
scsi-modules-3.16.0-4-amd64-di_3.16.7-ckt25-2+deb8u3
fat-modules-3.16.0-4-amd64-di_3.16.7-ckt25-2+deb8u3
pcmcia-storage-modules-3.16.0-4-powerpc64-di_3.16.7-ckt25-2+deb8u3
nic-modules-3.16.0-4-kirkwood-di_3.16.7-ckt25-2+deb8u3
scsi-core-modules-3.16.0-4-686-pae-di_3.16.7-ckt25-2+deb8u3
zlib-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
nic-shared-modules-3.16.0-4-versatile-di_3.16.7-ckt25-2+deb8u3
udf-modules-3.16.0-4-amd64-di_3.16.7-ckt25-2+deb8u3
core-modules-3.16.0-4-amd64-di_3.16.7-ckt25-2+deb8u3
sata-modules-3.16.0-4-powerpc64-di_3.16.7-ckt25-2+deb8u3
input-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt25-2+deb8u3
isofs-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
usb-storage-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
nic-shared-modules-3.16.0-4-r4k-ip22-di_3.16.7-ckt25-2+deb8u3
input-modules-3.16.0-4-686-pae-di_3.16.7-ckt25-2+deb8u3
hfs-modules-3.16.0-4-loongson-3-di_3.16.7-ckt25-2+deb8u3
kernel-image-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
uinput-modules-3.16.0-4-powerpc64-di_3.16.7-ckt25-2+deb8u3
usb-serial-modules-3.16.0-4-orion5x-di_3.16.7-ckt25-2+deb8u3
linux-headers-3.16.0-4-powerpc64le_3.16.7-ckt25-2+deb8u3
scsi-core-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt25-2+deb8u3
scsi-common-modules-3.16.0-4-powerpc-di_3.16.7-ckt25-2+deb8u3
usb-modules-3.16.0-4-powerpc-di_3.16.7-ckt25-2+deb8u3
nic-shared-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
xfs-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3
jfs-modules-3.16.0-4-octeon-di_3.16.7-ckt25-2+deb8u3
pata-modules-3.16.0-4-powerpc64-di_3.16.7-ckt25-2+deb8u3
event-modules-3.16.0-4-amd64-di_3.16.7-ckt25-2+deb8u3
fat-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
multipath-modules-3.16.0-4-686-pae-di_3.16.7-ckt25-2+deb8u3
nic-usb-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
ppp-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt25-2+deb8u3
linux-image-3.16.0-4-orion5x_3.16.7-ckt25-2+deb8u3
crc-modules-3.16.0-4-powerpc-di_3.16.7-ckt25-2+deb8u3
loop-modules-3.16.0-4-versatile-di_3.16.7-ckt25-2+deb8u3
loop-modules-3.16.0-4-kirkwood-di_3.16.7-ckt25-2+deb8u3
firewire-core-modules-3.16.0-4-powerpc64-di_3.16.7-ckt25-2+deb8u3
squashfs-modules-3.16.0-4-armmp-di_3.16.7-ckt25-2+deb8u3
scsi-core-modules-3.16.0-4-loongson-3-di_3.16.7-ckt25-2+deb8u3
usb-serial-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
loop-modules-3.16.0-4-amd64-di_3.16.7-ckt25-2+deb8u3
crypto-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
md-modules-3.16.0-4-r5k-ip32-di_3.16.7-ckt25-2+deb8u3

sata-modules-3.16.0-4-versatile-di_3.16.7-ckt25-2+deb8u3
usb-storage-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3
crypto-dm-modules-3.16.0-4-octeon-di_3.16.7-ckt25-2+deb8u3
core-modules-3.16.0-4-arm64-di_3.16.7-ckt25-2+deb8u3
scsi-modules-3.16.0-4-powerpc-di_3.16.7-ckt25-2+deb8u3
linux-headers-3.16.0-4-586_3.16.7-ckt25-2+deb8u3
scsi-modules-3.16.0-4-loongson-3-di_3.16.7-ckt25-2+deb8u3
virtio-modules-3.16.0-4-powerpc-di_3.16.7-ckt25-2+deb8u3
usb-modules-3.16.0-4-686-pae-di_3.16.7-ckt25-2+deb8u3
fuse-modules-3.16.0-4-r5k-ip32-di_3.16.7-ckt25-2+deb8u3
crc-modules-3.16.0-4-r5k-ip32-di_3.16.7-ckt25-2+deb8u3
input-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3
usb-storage-modules-3.16.0-4-orion5x-di_3.16.7-ckt25-2+deb8u3
loop-modules-3.16.0-4-armmp-di_3.16.7-ckt25-2+deb8u3
sata-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt25-2+deb8u3
nbd-modules-3.16.0-4-loongson-3-di_3.16.7-ckt25-2+deb8u3
event-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt25-2+deb8u3
pata-modules-3.16.0-4-586-di_3.16.7-ckt25-2+deb8u3
scsi-extra-modules-3.16.0-4-586-di_3.16.7-ckt25-2+deb8u3
sata-modules-3.16.0-4-armmp-di_3.16.7-ckt25-2+deb8u3
crypto-dm-modules-3.16.0-4-kirkwood-di_3.16.7-ckt25-2+deb8u3
md-modules-3.16.0-4-armmp-di_3.16.7-ckt25-2+deb8u3
linux-headers-3.16.0-4-versatile_3.16.7-ckt25-2+deb8u3
crc-modules-3.16.0-4-powerpc64-di_3.16.7-ckt25-2+deb8u3
crypto-dm-modules-3.16.0-4-loongson-3-di_3.16.7-ckt25-2+deb8u3
scsi-common-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3
md-modules-3.16.0-4-s390x-di_3.16.7-ckt25-2+deb8u3
mouse-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
usb-serial-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
scsi-core-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
usb-storage-modules-3.16.0-4-octeon-di_3.16.7-ckt25-2+deb8u3
isofs-modules-3.16.0-4-586-di_3.16.7-ckt25-2+deb8u3
xfs-modules-3.16.0-4-octeon-di_3.16.7-ckt25-2+deb8u3
crc-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3
scsi-common-modules-3.16.0-4-586-di_3.16.7-ckt25-2+deb8u3
linux-headers-3.16.0-4-powerpc64_3.16.7-ckt25-2+deb8u3
dasd-extra-modules-3.16.0-4-s390x-di_3.16.7-ckt25-2+deb8u3
virtio-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3
nic-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt25-2+deb8u3
btrfs-modules-3.16.0-4-loongson-3-di_3.16.7-ckt25-2+deb8u3
nic-shared-modules-3.16.0-4-octeon-di_3.16.7-ckt25-2+deb8u3
minix-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3
linux-image-3.16.0-4-amd64-dbg_3.16.7-ckt25-2+deb8u3
linux-image-3.16.0-4-r5k-ip32_3.16.7-ckt25-2+deb8u3
event-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
squashfs-modules-3.16.0-4-versatile-di_3.16.7-ckt25-2+deb8u3
nic-modules-3.16.0-4-586-di_3.16.7-ckt25-2+deb8u3
nic-modules-3.16.0-4-s390x-di_3.16.7-ckt25-2+deb8u3
crypto-modules-3.16.0-4-r4k-ip22-di_3.16.7-ckt25-2+deb8u3
virtio-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt25-2+deb8u3
md-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt25-2+deb8u3
md-modules-3.16.0-4-loongson-3-di_3.16.7-ckt25-2+deb8u3
linux-headers-3.16.0-4-all-armel_3.16.7-ckt25-2+deb8u3
nic-modules-3.16.0-4-amd64-di_3.16.7-ckt25-2+deb8u3
zlib-modules-3.16.0-4-r4k-ip22-di_3.16.7-ckt25-2+deb8u3
ata-modules-3.16.0-4-arm64-di_3.16.7-ckt25-2+deb8u3
virtio-modules-3.16.0-4-loongson-3-di_3.16.7-ckt25-2+deb8u3
scsi-modules-3.16.0-4-586-di_3.16.7-ckt25-2+deb8u3
ata-modules-3.16.0-4-586-di_3.16.7-ckt25-2+deb8u3

130533 - Debian Linux 8.0 DSA-3608-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4324

Description

The scan detected that the host is missing the following update:
DSA-3608-1

Observation

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

http://www.debian.org/security/2016/dsa-3608

Debian 8.0
all
libreoffice_1:4.3.3-2+deb8u5

181989 - FreeBSD apache24 X509 Client Certificate Based Authentication Can Be Bypassed When HTTP/2 Is Used (e9d1e040-42c9-11e6-9608-20cf3

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

Risk Level: Low

CVE: CVE-2016-4979

Description

The scan detected that the host is missing the following update:
apache24 -- X509 Client certificate based authentication can be bypassed when HTTP/2 is used (e9d1e040-42c9-11e6-9608-20cf30e32f6d)

Observation

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

http://www.vuxml.org/freebsd/e9d1e040-42c9-11e6-9608-20cf30e32f6d.html

Affected packages:
2.4.18 <= apache24 < 2.4.23

181990 - FreeBSD phpMyAdmin Multiple Vulnerabilities (e7028e1d-3f9b-11e6-81f9-6805ca0b3d42)

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

Risk Level: Low

CVE: CVE-2016-5701, CVE-2016-5702, CVE-2016-5703, CVE-2016-5704, CVE-2016-5705, CVE-2016-5706, CVE-2016-5730, CVE-2016-5731, CVE-2016-5732, CVE-2016-5733, CVE-2016-5734, CVE-2016-5739

Description

The scan detected that the host is missing the following update:
phpMyAdmin -- multiple vulnerabilities (e7028e1d-3f9b-11e6-81f9-6805ca0b3d42)

Observation

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

For more information see:

http://www.vuxml.org/freebsd/e7028e1d-3f9b-11e6-81f9-6805ca0b3d42.html

Affected packages:
4.6.0 <= phpmyadmin < 4.6.3

181991 - FreeBSD wireshark Multiple Vulnerabilities (313e9557-41e8-11e6-ab34-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-5350, CVE-2016-5351, CVE-2016-5352, CVE-2016-5353, CVE-2016-5354, CVE-2016-5355, CVE-2016-5356, CVE-2016-5357, CVE-2016-5358

Description

The scan detected that the host is missing the following update:
wireshark -- multiple vulnerabilities (313e9557-41e8-11e6-ab34-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/313e9557-41e8-11e6-ab34-002590263bf5.html

Affected packages:
wireshark < 2.0.4
wireshark-lite < 2.0.4
wireshark-qt5 < 2.0.4
tshark < 2.0.4
tshark-lite < 2.0.4

181992 - FreeBSD libtorrent-rasterbar Denial Of Service (093584f2-3f14-11e6-b3c8-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-5301

Description

The scan detected that the host is missing the following update:
libtorrent-rasterbar -- denial of service (093584f2-3f14-11e6-b3c8-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/093584f2-3f14-11e6-b3c8-14dae9d210b8.html

Affected packages:
libtorrent-rasterbar < 1.1.1

181993 - FreeBSD haproxy Denial Of Service (f1c219ba-3f14-11e6-b3c8-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-5360

Description

The scan detected that the host is missing the following update:
haproxy -- denial of service (f1c219ba-3f14-11e6-b3c8-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/f1c219ba-3f14-11e6-b3c8-14dae9d210b8.html

Affected packages:
1.6.0 <= haproxy < 1.6.5_1

181994 - FreeBSD icingaweb2 Remote Code Execution (ad9b77f6-4163-11e6-b05b-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
icingaweb2 -- remote code execution (ad9b77f6-4163-11e6-b05b-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/ad9b77f6-4163-11e6-b05b-14dae9d210b8.html

Affected packages:
icingaweb2 < 2.3.4

181999 - FreeBSD dnsmasq Denial Of Service (875e4cf8-3f0e-11e6-b3c8-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-8899

Description

The scan detected that the host is missing the following update:
dnsmasq -- denial of service (875e4cf8-3f0e-11e6-b3c8-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/875e4cf8-3f0e-11e6-b3c8-14dae9d210b8.html

Affected packages:
dnsmasq < 2.76,1
dnsmasq-devel < 2.76.0test1

182000 - FreeBSD SQLite3 Tempdir Selection Vulnerability (546deeea-3fc6-11e6-a671-60a44ce6887b)

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

Risk Level: Low

CVE: CVE-2016-6153

Description

The scan detected that the host is missing the following update:
SQLite3 -- Tempdir Selection Vulnerability (546deeea-3fc6-11e6-a671-60a44ce6887b)

Observation

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

http://www.vuxml.org/freebsd/546deeea-3fc6-11e6-a671-60a44ce6887b.html

Affected packages:
sqlite3 < 3.13.0

182003 - FreeBSD moodle Multiple Vulnerabilities (8656cf5f-4170-11e6-8dfe-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-3729, CVE-2016-3731, CVE-2016-3732, CVE-2016-3733, CVE-2016-3734

Description

The scan detected that the host is missing the following update:
moodle -- multiple vulnerabilities (8656cf5f-4170-11e6-8dfe-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/8656cf5f-4170-11e6-8dfe-002590263bf5.html

Affected packages:
moodle28 < 2.8.12
moodle29 < 2.9.6
moodle30 < 3.0.4

182004 - FreeBSD Python HTTP Header Injection In Python Urllib (a61374fc-3a4d-11e6-a671-60a44ce6887b)

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

Risk Level: Low

CVE: CVE-2016-5699

Description

The scan detected that the host is missing the following update:
Python -- HTTP Header Injection in Python urllib (a61374fc-3a4d-11e6-a671-60a44ce6887b)

Observation

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

http://www.vuxml.org/freebsd/a61374fc-3a4d-11e6-a671-60a44ce6887b.html

Affected packages:
python27 < 2.7.10
python34 < 3.4.4
python35 < 3.5.0

182007 - FreeBSD expat2 Denial Of Service (ff76f0e0-3f11-11e6-b3c8-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-4472

Description

The scan detected that the host is missing the following update:
expat2 -- denial of service (ff76f0e0-3f11-11e6-b3c8-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/ff76f0e0-3f11-11e6-b3c8-14dae9d210b8.html

Affected packages:
expat2 < 2.1.1_2

182008 - FreeBSD Python 2.7 Smtplib StartTLS Stripping Vulnerability (8d5368ef-40fe-11e6-b2ec-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2016-0772

Description

The scan detected that the host is missing the following update:
Python 2.7 -- smtplib StartTLS stripping vulnerability (8d5368ef-40fe-11e6-b2ec-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/8d5368ef-40fe-11e6-b2ec-b499baebfeaf.html

Affected packages:
python27 < 2.7.12
python34 < 3.4.5
python35 < 3.5.2

185343 - Ubuntu Linux 12.04, 15.10, 16.04 USN-3022-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4324

Description

The scan detected that the host is missing the following update:
USN-3022-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-June/003485.html

Ubuntu 12.04

libreoffice-core_3.5.7-0ubuntu11

Ubuntu 16.04

libreoffice-core_5.1.4-0ubuntu1

Ubuntu 15.10

libreoffice-core_5.0.6-0ubuntu1

185346 - Ubuntu Linux 12.04, 14.04, 15.10 USN-3025-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4994

Description

The scan detected that the host is missing the following update:
USN-3025-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-July/003488.html

Ubuntu 12.04

gimp_2.6.12-1ubuntu1.4

Ubuntu 15.10

gimp_2.8.14-1ubuntu2.1

Ubuntu 14.04

gimp_2.8.10-0ubuntu1.1

185347 - Ubuntu Linux 14.04, 15.10, 16.04 USN-3015-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1704

Description

The scan detected that the host is missing the following update:
USN-3015-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-June/003486.html

Ubuntu 16.04

liboxideqtcore0_1.15.8-0ubuntu0.16.04.1

Ubuntu 15.10

liboxideqtcore0_1.15.8-0ubuntu0.15.10.1

Ubuntu 14.04

liboxideqtcore0_1.15.8-0ubuntu0.14.04.1

182002 - FreeBSD xen-tools Unrestricted Qemu Logging (e800cd4b-4212-11e6-942d-bc5ff45d0f28)

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

Risk Level: Low

CVE: CVE-2014-3672

Description

The scan detected that the host is missing the following update:
xen-tools -- Unrestricted qemu logging (e800cd4b-4212-11e6-942d-bc5ff45d0f28)

Observation

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

http://www.vuxml.org/freebsd/e800cd4b-4212-11e6-942d-bc5ff45d0f28.html

Affected packages:
xen-tools < 4.7.0_2

182006 - FreeBSD xen-tools Unsanitised Driver Domain Input In Libxl Device Handling (e589ae90-4212-11e6-942d-bc5ff45d0f28)

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

Risk Level: Low

CVE: CVE-2016-4963

Description

The scan detected that the host is missing the following update:
xen-tools -- Unsanitised driver domain input in libxl device handling (e589ae90-4212-11e6-942d-bc5ff45d0f28)

Observation

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

http://www.vuxml.org/freebsd/e589ae90-4212-11e6-942d-bc5ff45d0f28.html

Affected packages:

xen-tools < 4.7.0_1

ENHANCED CHECKS

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

18907 - (SOL17173) F5 BIG-IP OpenJDK Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-4760

Update Details

Recommendation is updated

18874 - (SOL17113) F5 BIG-IP OpenSSH Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-5600

Update Details

Documentation is updated

18725 - (SOL16993) F5 BIG-IP PHP Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-4025, CVE-2015-4026

Update Details

Documentation is updated

20230 - IBM WebSphere Application Server Apache Standard Taglibs XML External Entity Injection Vulnerability

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

Risk Level: High

CVE: CVE-2015-0254

Update Details

Description is updated Observation is updated

181868 - FreeBSD wireshark Multiple Vulnerabilities (45117749-df55-11e5-b2bd-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-2522, CVE-2016-2523, CVE-2016-2524, CVE-2016-2525, CVE-2016-2526, CVE-2016-2527, CVE-2016-2528, CVE-2016-2529, CVE-2016-2530, CVE-2016-2531, CVE-2016-2532, CVE-2016-4415, CVE-2016-4416, CVE-2016-4417, CVE-2016-4418, CVE-2016-4419, CVE-2016-4420, CVE-2016-4421

Update Details

CVE is updated

18354 - (SOL16472) F5 BIG-IP glibc getaddrinfo function Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-7424

Update Details

Documentation is updated

18415 - (SOL16707) F5 BIG-IP cURL and libcurl vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-3148

Update Details

Recommendation is updated

18492 - (SOL16704) F5 BIG-IP cURL and libcurl Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-3143

Update Details

Recommendation is updated

19055 - (SOL17251) F5 BIG-IP Apache HTTP Request Smuggling Attack Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-3183

Update Details

Recommendation is updated

19123 - (SOL17235) F5 BIG-IP PCRE Library Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-3210

Update Details

Recommendation is updated

9410 - Microsoft Internet Explorer CSS 'expression' Remote Denial of Service Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated FASLScript is updated

181934 - FreeBSD wireshark Multiple Vulnerabilities (7e36c369-10c0-11e6-94fa-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-4006, CVE-2016-4076, CVE-2016-4077, CVE-2016-4078, CVE-2016-4079, CVE-2016-4080, CVE-2016-4081, CVE-2016-4082, CVE-2016-4083, CVE-2016-4084

Update Details

CVE is updated

181953 - FreeBSD openvswitch MPLS Buffer Overflow (b53bbf58-257f-11e6-9f4d-20cf30e32f6d)

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

Risk Level: Low

CVE: CVE-2016-2074

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.