

MCAFFEE 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

21505 - Novell eDirectory Multiple Components Vulnerability Prior To 8.8 SP8 Patch 9 HotFix 2

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2017-5186

Description

A Vulnerability is present in some versions of Novell (NetIQ) eDirectory.

Observation

Novell (NetIQ) eDirectory is an X.500 compatible directory service software for centrally managing access to network resources.

A Vulnerability is present in some versions of Novell (NetIQ) eDirectory. The flaw is because of multiple components using embedded certificate over SSL to connect to Sentinel Servers instead of using eDirectory certificates. Successful exploitation could allow a malicious user to cause an unspecified impact.

163322 - Oracle Enterprise Linux ELSA-2017-0893 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10229, CVE-2017-2668

Description

The scan detected that the host is missing the following update:
ELSA-2017-0893

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006824.html>

OEL6

x86_64

389-ds-base-devel-1.2.11.15-91.el6_9

389-ds-base-libs-1.2.11.15-91.el6_9

389-ds-base-1.2.11.15-91.el6_9

i386

389-ds-base-devel-1.2.11.15-91.el6_9

389-ds-base-libs-1.2.11.15-91.el6_9

389-ds-base-1.2.11.15-91.el6_9

21575 - (VMSA-2017-0005) VMware Fusion Out Of Bounds Memory Access Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4901

Description

A vulnerability is present in some versions of VMware Fusion.

Observation

VMware Fusion is a popular virtualization platform.

A vulnerability is present in some versions of VMware Fusion. The flaw lies in the drag-and-drop (DnD) function of this software. Successful exploitation could allow a local attacker to execute arbitrary code in the system that's running VMware Fusion.

141536 - Red Hat Enterprise Linux RHSA-2017-0892 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7910, CVE-2017-2636

Description

The scan detected that the host is missing the following update:
RHSA-2017-0892

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00009.html>

RHEL6D

i386

kernel-headers-2.6.32-696.1.1.el6

perf-debuginfo-2.6.32-696.1.1.el6

kernel-debug-2.6.32-696.1.1.el6

python-perf-2.6.32-696.1.1.el6

kernel-debug-devel-2.6.32-696.1.1.el6

python-perf-debuginfo-2.6.32-696.1.1.el6

kernel-debuginfo-common-i686-2.6.32-696.1.1.el6

kernel-debuginfo-2.6.32-696.1.1.el6

perf-2.6.32-696.1.1.el6

kernel-2.6.32-696.1.1.el6

kernel-devel-2.6.32-696.1.1.el6

kernel-debug-debuginfo-2.6.32-696.1.1.el6

noarch

kernel-firmware-2.6.32-696.1.1.el6

kernel-doc-2.6.32-696.1.1.el6

kernel-abi-whitelists-2.6.32-696.1.1.el6

x86_64

kernel-headers-2.6.32-696.1.1.el6

kernel-debuginfo-common-i686-2.6.32-696.1.1.el6

kernel-debug-debuginfo-2.6.32-696.1.1.el6

perf-2.6.32-696.1.1.el6

kernel-devel-2.6.32-696.1.1.el6
kernel-debuginfo-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6
perf-debuginfo-2.6.32-696.1.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
python-perf-debuginfo-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6

RHEL6S

i386
kernel-headers-2.6.32-696.1.1.el6
perf-debuginfo-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
python-perf-debuginfo-2.6.32-696.1.1.el6
kernel-debuginfo-common-i686-2.6.32-696.1.1.el6
kernel-debuginfo-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
kernel-debug-debuginfo-2.6.32-696.1.1.el6

noarch

kernel-firmware-2.6.32-696.1.1.el6
kernel-doc-2.6.32-696.1.1.el6
kernel-abi-whitelists-2.6.32-696.1.1.el6

x86_64

kernel-headers-2.6.32-696.1.1.el6
kernel-debuginfo-common-i686-2.6.32-696.1.1.el6
kernel-debug-debuginfo-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
kernel-debuginfo-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6
perf-debuginfo-2.6.32-696.1.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
python-perf-debuginfo-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6

RHEL6WS

i386
kernel-headers-2.6.32-696.1.1.el6
perf-debuginfo-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
python-perf-debuginfo-2.6.32-696.1.1.el6
kernel-debuginfo-common-i686-2.6.32-696.1.1.el6
kernel-debuginfo-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
kernel-debug-debuginfo-2.6.32-696.1.1.el6

noarch

kernel-firmware-2.6.32-696.1.1.el6
kernel-doc-2.6.32-696.1.1.el6
kernel-abi-whitelists-2.6.32-696.1.1.el6

x86_64
kernel-headers-2.6.32-696.1.1.el6
perf-debuginfo-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
python-perf-debuginfo-2.6.32-696.1.1.el6
kernel-debuginfo-common-i686-2.6.32-696.1.1.el6
kernel-debuginfo-2.6.32-696.1.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
kernel-debug-debuginfo-2.6.32-696.1.1.el6

145291 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0950-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8540, CVE-2016-10087

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0950-1

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-April/002787.html>

SuSE SLED 12 SP1

x86_64
libpng15-15-1.5.22-9.1
libpng15-15-debuginfo-1.5.22-9.1
libpng15-debugsource-1.5.22-9.1

SuSE SLES 12 SP2

x86_64
libpng15-15-1.5.22-9.1
libpng15-15-debuginfo-1.5.22-9.1
libpng15-debugsource-1.5.22-9.1

SuSE SLED 12 SP2

x86_64
libpng15-15-1.5.22-9.1
libpng15-15-debuginfo-1.5.22-9.1
libpng15-debugsource-1.5.22-9.1

SuSE SLES 12 SP1

x86_64
libpng15-15-1.5.22-9.1
libpng15-15-debuginfo-1.5.22-9.1
libpng15-debugsource-1.5.22-9.1

163323 - Oracle Enterprise Linux ELSA-2017-0892 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7910, CVE-2017-2636

Description

The scan detected that the host is missing the following update:
ELSA-2017-0892

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006826.html>

OEL6

x86_64

kernel-headers-2.6.32-696.1.1.el6
kernel-abi-whitelists-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
kernel-firmware-2.6.32-696.1.1.el6
kernel-doc-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6

i386

kernel-headers-2.6.32-696.1.1.el6
kernel-abi-whitelists-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
kernel-firmware-2.6.32-696.1.1.el6
kernel-doc-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6

175140 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1704-5983)

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

Risk Level: High

CVE: CVE-2016-7910, CVE-2017-2636

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1704-5983)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=5983>

SL6
i386
kernel-headers-2.6.32-696.1.1.el6
perf-debuginfo-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
python-perf-debuginfo-2.6.32-696.1.1.el6
kernel-debuginfo-common-i686-2.6.32-696.1.1.el6
kernel-debuginfo-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
kernel-debug-debuginfo-2.6.32-696.1.1.el6

noarch
kernel-firmware-2.6.32-696.1.1.el6
kernel-doc-2.6.32-696.1.1.el6
kernel-abi-whitelists-2.6.32-696.1.1.el6

x86_64
kernel-headers-2.6.32-696.1.1.el6
kernel-debuginfo-common-i686-2.6.32-696.1.1.el6
kernel-debug-debuginfo-2.6.32-696.1.1.el6
perf-2.6.32-696.1.1.el6
kernel-devel-2.6.32-696.1.1.el6
kernel-debuginfo-2.6.32-696.1.1.el6
kernel-2.6.32-696.1.1.el6
perf-debuginfo-2.6.32-696.1.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.1.1.el6
kernel-debug-devel-2.6.32-696.1.1.el6
python-perf-debuginfo-2.6.32-696.1.1.el6
kernel-debug-2.6.32-696.1.1.el6
python-perf-2.6.32-696.1.1.el6

182325 - FreeBSD id Tech 3 Remote Code Execution Vulnerability (e48355d7-1548-11e7-8611-0090f5f2f347)

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

Risk Level: High

CVE: CVE-2017-6903

Description

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

id Tech 3 -- remote code execution vulnerability (e48355d7-1548-11e7-8611-0090f5f2f347)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/e48355d7-1548-11e7-8611-0090f5f2f347.html>

Affected packages:

ioquake3 < 1.36_16

ioquake3-devel < g2930

iourbanterror < 4.3.2,1

openarena < 0.8.8.s1910_3,1

191925 - Fedora Linux 26 FEDORA-2017-0c4f5fb08e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7413, CVE-2017-7414

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0c4f5fb08e

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/2017/4/?count=200&page=1>

Fedora Core 26

php-horde-Horde-Crypt-2.7.6-1.fc26

21574 - (SA-CORE-2017-001) Drupal Core Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-6377, CVE-2017-6379, CVE-2017-6381

Description

Multiple vulnerabilities are present in some versions of Drupal.

Observation

Drupal is a popular open source content management system.

Multiple vulnerabilities are present in some versions of Drupal. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, execute arbitrary code or make unauthorized modifications on the target system.

141535 - Red Hat Enterprise Linux RHSA-2017-0893 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2668

Description

The scan detected that the host is missing the following update:
RHSA-2017-0893

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00010.html>

RHEL6S
x86_64

389-ds-base-debuginfo-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9
389-ds-base-devel-1.2.11.15-91.el6_9

i386

389-ds-base-debuginfo-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9
389-ds-base-devel-1.2.11.15-91.el6_9

RHEL6WS

x86_64
389-ds-base-debuginfo-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9

i386

389-ds-base-debuginfo-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9

RHEL6D

x86_64
389-ds-base-debuginfo-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9
389-ds-base-devel-1.2.11.15-91.el6_9

i386

389-ds-base-debuginfo-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9
389-ds-base-devel-1.2.11.15-91.el6_9

145288 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0983-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6505, CVE-2017-7228

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0983-1

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-April/002793.html>

SuSE SLED 12 SP2

x86_64
xen-libs-4.7.2_02-36.1
xen-debugsource-4.7.2_02-36.1
xen-libs-debuginfo-32bit-4.7.2_02-36.1
xen-libs-debuginfo-4.7.2_02-36.1
xen-libs-32bit-4.7.2_02-36.1

xen-4.7.2_02-36.1

SuSE SLES 12 SP2

x86_64

xen-tools-domU-4.7.2_02-36.1

xen-libs-4.7.2_02-36.1

xen-tools-debuginfo-4.7.2_02-36.1

xen-debugsource-4.7.2_02-36.1

xen-tools-4.7.2_02-36.1

xen-libs-debuginfo-32bit-4.7.2_02-36.1

xen-libs-debuginfo-4.7.2_02-36.1

xen-libs-32bit-4.7.2_02-36.1

xen-doc-html-4.7.2_02-36.1

xen-4.7.2_02-36.1

xen-tools-domU-debuginfo-4.7.2_02-36.1

145293 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0951-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8637

Description

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

SUSE-SU-2017:0951-1

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-April/002788.html>

SuSE SLED 12 SP2

x86_64

dracut-debugsource-044-108.1

dracut-debuginfo-044-108.1

dracut-044-108.1

SuSE SLES 12 SP2

x86_64

dracut-fips-044-108.1

dracut-debugsource-044-108.1

dracut-debuginfo-044-108.1

dracut-044-108.1

175135 - Scientific Linux Security ERRATA Moderate: gnutls on SL6.x i386/x86_64 (1704-396)

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

Risk Level: High

CVE: CVE-2016-8610, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

Description

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

Security ERRATA Moderate: gnutls on SL6.x i386/x86_64 (1704-396)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=396>

SL6

x86_64

gnutls-debuginfo-2.12.23-21.el6

gnutls-2.12.23-21.el6

gnutls-guile-2.12.23-21.el6

gnutls-devel-2.12.23-21.el6

gnutls-utils-2.12.23-21.el6

i386

gnutls-debuginfo-2.12.23-21.el6

gnutls-2.12.23-21.el6

gnutls-guile-2.12.23-21.el6

gnutls-devel-2.12.23-21.el6

gnutls-utils-2.12.23-21.el6

175141 - Scientific Linux Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1704-2945)

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

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-10142, CVE-2016-2069, CVE-2016-2384, CVE-2016-6480, CVE-2016-7042, CVE-2016-7097, CVE-2016-8399, CVE-2016-9576

Description

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

Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1704-2945)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=2945>

SL6

i386

perf-debuginfo-2.6.32-696.el6

kernel-2.6.32-696.el6

python-perf-2.6.32-696.el6

perf-2.6.32-696.el6

kernel-debug-2.6.32-696.el6

kernel-debuginfo-2.6.32-696.el6

kernel-debuginfo-common-i686-2.6.32-696.el6

python-perf-debuginfo-2.6.32-696.el6

kernel-headers-2.6.32-696.el6

kernel-debug-debuginfo-2.6.32-696.el6

kernel-debug-devel-2.6.32-696.el6

kernel-devel-2.6.32-696.el6

noarch

kernel-firmware-2.6.32-696.el6

kernel-abi-whitelists-2.6.32-696.el6

kernel-doc-2.6.32-696.el6

x86_64

python-perf-2.6.32-696.el6
kernel-debug-2.6.32-696.el6
python-perf-debuginfo-2.6.32-696.el6
perf-2.6.32-696.el6
kernel-debuginfo-common-x86_64-2.6.32-696.el6
kernel-2.6.32-696.el6
kernel-headers-2.6.32-696.el6
kernel-debug-debuginfo-2.6.32-696.el6
kernel-debuginfo-common-i686-2.6.32-696.el6
perf-debuginfo-2.6.32-696.el6
kernel-devel-2.6.32-696.el6
kernel-debug-devel-2.6.32-696.el6
kernel-debuginfo-2.6.32-696.el6

175142 - Scientific Linux Security ERRATA Moderate: bash on SL6.x i386/x86_64 (1704-5255)

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

Risk Level: High

CVE: CVE-2016-0634, CVE-2016-7543, CVE-2016-9401

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: bash on SL6.x i386/x86_64 (1704-5255)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=5255>

SL6
x86_64
bash-doc-4.1.2-48.el6
bash-debuginfo-4.1.2-48.el6
bash-4.1.2-48.el6

i386
bash-doc-4.1.2-48.el6
bash-debuginfo-4.1.2-48.el6
bash-4.1.2-48.el6

175143 - Scientific Linux Security ERRATA Moderate: wireshark on SL6.x i386/x86_64 (1704-2550)

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

Risk Level: High

CVE: CVE-2013-4075, CVE-2015-3811, CVE-2015-3812, CVE-2015-3813

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: wireshark on SL6.x i386/x86_64 (1704-2550)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=2550>

SL6
x86_64
wireshark-debuginfo-1.8.10-25.el6
wireshark-gnome-1.8.10-25.el6
wireshark-devel-1.8.10-25.el6
wireshark-1.8.10-25.el6

i386
wireshark-debuginfo-1.8.10-25.el6
wireshark-gnome-1.8.10-25.el6
wireshark-devel-1.8.10-25.el6
wireshark-1.8.10-25.el6

175144 - Scientific Linux Security ERRATA Important: 389-ds-base on SL6.x i386/x86_64 (1704-6340)

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

Risk Level: High

CVE: CVE-2017-2668

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: 389-ds-base on SL6.x i386/x86_64 (1704-6340)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=6340>

SL6
x86_64
389-ds-base-debuginfo-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9
389-ds-base-devel-1.2.11.15-91.el6_9

i386
389-ds-base-debuginfo-1.2.11.15-91.el6_9
389-ds-base-libs-1.2.11.15-91.el6_9
389-ds-base-1.2.11.15-91.el6_9
389-ds-base-devel-1.2.11.15-91.el6_9

175146 - Scientific Linux Security ERRATA Moderate: openssl on SL6.x i386/x86_64 (1704-1804)

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

Risk Level: High

CVE: CVE-2015-8325

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openssl on SL6.x i386/x86_64 (1704-1804)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=1804>

SL6

x86_64
openssh-5.3p1-122.el6
openssh-debuginfo-5.3p1-122.el6
pam_ssh_agent_auth-0.9.3-122.el6
openssh-server-5.3p1-122.el6
openssh-ldap-5.3p1-122.el6
openssh-clients-5.3p1-122.el6
openssh-askpass-5.3p1-122.el6

i386

openssh-5.3p1-122.el6
openssh-debuginfo-5.3p1-122.el6
pam_ssh_agent_auth-0.9.3-122.el6
openssh-server-5.3p1-122.el6
openssh-ldap-5.3p1-122.el6
openssh-clients-5.3p1-122.el6
openssh-askpass-5.3p1-122.el6

175147 - Scientific Linux Security ERRATA Moderate: glibc on SL6.x i386/x86_64 (1704-3780)

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

Risk Level: High

CVE: CVE-2014-9761, CVE-2015-8776, CVE-2015-8778, CVE-2015-8779

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: glibc on SL6.x i386/x86_64 (1704-3780)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=3780>

SL6

x86_64
glibc-debuginfo-2.12-1.209.el6
glibc-common-2.12-1.209.el6
glibc-2.12-1.209.el6
glibc-static-2.12-1.209.el6
glibc-headers-2.12-1.209.el6
nscd-2.12-1.209.el6
glibc-utils-2.12-1.209.el6
glibc-devel-2.12-1.209.el6
glibc-debuginfo-common-2.12-1.209.el6

i386

glibc-debuginfo-2.12-1.209.el6
glibc-common-2.12-1.209.el6
glibc-2.12-1.209.el6
glibc-static-2.12-1.209.el6
glibc-headers-2.12-1.209.el6
nscd-2.12-1.209.el6
glibc-utils-2.12-1.209.el6

glibc-devel-2.12-1.209.el6
glibc-debuginfo-common-2.12-1.209.el6

175151 - Scientific Linux Security ERRATA Moderate: quagga on SL6.x i386/x86_64 (1704-2144)

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

Risk Level: High

CVE: CVE-2013-2236, CVE-2016-1245, CVE-2016-2342, CVE-2016-4049, CVE-2017-5495

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: quagga on SL6.x i386/x86_64 (1704-2144)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=2144>

SL6
x86_64
quagga-debuginfo-0.99.15-14.el6
quagga-contrib-0.99.15-14.el6
quagga-devel-0.99.15-14.el6
quagga-0.99.15-14.el6

i386
quagga-debuginfo-0.99.15-14.el6
quagga-contrib-0.99.15-14.el6
quagga-devel-0.99.15-14.el6
quagga-0.99.15-14.el6

178420 - Gentoo Linux GLSA-201704-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5407, CVE-2016-7942, CVE-2016-7943, CVE-2016-7944, CVE-2016-7945, CVE-2016-7946, CVE-2016-7947, CVE-2016-7948, CVE-2016-7949, CVE-2016-7950, CVE-2016-7953, CVE-2017-2624, CVE-2017-2625, CVE-2017-2626

Description

The scan detected that the host is missing the following update:
GLSA-201704-03

Observation

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

<https://security.gentoo.org/glsa/201704-03>

Affected packages:
x11-base/xorg-server < 1.19.2
x11-libs/libICE < 1.0.9-r1
x11-libs/libXdmp < 1.1.2-r1
x11-libs/libXrender < 0.9.10
x11-libs/libXi < 1.7.7
x11-libs/libXrandr < 1.5.1

x11-libs/libXfixes < 5.0.3
x11-libs/libXv < 1.0.11

182323 - FreeBSD xen-kernel Broken Check In Memory_exchange () permits PV guest breakout (90becf7c-1acf-11e7-970f-002590263bf5)

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

Risk Level: High

CVE: CVE-2017-7228

Description

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

xen-kernel -- broken check in memory_exchange() permits PV guest breakout (90becf7c-1acf-11e7-970f-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/90becf7c-1acf-11e7-970f-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.2_1

191924 - Fedora Linux 25 FEDORA-2017-054729ab08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7228, CVE-2017-7377

Description

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

FEDORA-2017-054729ab08

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/2017/4/?count=200&page=3>

Fedora Core 25

xen-4.7.2-5.fc25

88857 - Slackware Linux 14.2 SSA:2017-098-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8127, CVE-2015-8665, CVE-2015-8683, CVE-2016-3622, CVE-2016-3623, CVE-2016-3658, CVE-2016-5321, CVE-2016-5323, CVE-2016-5652, CVE-2016-5875, CVE-2016-9273, CVE-2016-9448

Description

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

SSA:2017-098-01

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.395195>

Slackware 14.2
x86_64
libtiff-4.0.7-x86_64-1

i586
libtiff-4.0.7-i586-1

130740 - Debian Linux 8.0 DSA-3827-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10249, CVE-2016-10251, CVE-2016-9591

Description

The scan detected that the host is missing the following update:
DSA-3827-1

Observation

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

<http://www.debian.org/security/2017/dsa-3827>

Debian 8.0
all
libjasper1_1.900.1-debian1-2.4+deb8u3
libjasper-runtime_1.900.1-debian1-2.4+deb8u3
libjasper-dev_1.900.1-debian1-2.4+deb8u3

145292 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0953-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10251, CVE-2016-9583, CVE-2016-9600, CVE-2017-5498, CVE-2017-6850

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0953-1

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-April/002789.html>

SuSE SLED 12 SP1
x86_64
libjasper1-1.900.14-194.1
jasper-debuginfo-1.900.14-194.1

libjasper1-debuginfo-1.900.14-194.1
libjasper1-debuginfo-32bit-1.900.14-194.1
libjasper1-32bit-1.900.14-194.1
jasper-debugsource-1.900.14-194.1

SuSE SLES 12 SP2

x86_64
libjasper1-1.900.14-194.1
jasper-debuginfo-1.900.14-194.1
libjasper1-debuginfo-1.900.14-194.1
libjasper1-debuginfo-32bit-1.900.14-194.1
libjasper1-32bit-1.900.14-194.1
jasper-debugsource-1.900.14-194.1

SuSE SLED 12 SP2

x86_64
libjasper1-1.900.14-194.1
jasper-debuginfo-1.900.14-194.1
libjasper1-debuginfo-1.900.14-194.1
libjasper1-debuginfo-32bit-1.900.14-194.1
libjasper1-32bit-1.900.14-194.1
jasper-debugsource-1.900.14-194.1

SuSE SLES 12 SP1

x86_64
libjasper1-1.900.14-194.1
jasper-debuginfo-1.900.14-194.1
libjasper1-debuginfo-1.900.14-194.1
libjasper1-debuginfo-32bit-1.900.14-194.1
libjasper1-32bit-1.900.14-194.1
jasper-debugsource-1.900.14-194.1

145294 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0940-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7747, CVE-2017-6827, CVE-2017-6828, CVE-2017-6829, CVE-2017-6830, CVE-2017-6831, CVE-2017-6832, CVE-2017-6833, CVE-2017-6834, CVE-2017-6835, CVE-2017-6836, CVE-2017-6837, CVE-2017-6838, CVE-2017-6839

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0940-1

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-April/002783.html>

SuSE SLED 12 SP1

x86_64
audiofile-0.3.6-10.1
libaudiofile1-32bit-0.3.6-10.1
libaudiofile1-debuginfo-32bit-0.3.6-10.1
libaudiofile1-debuginfo-0.3.6-10.1
libaudiofile1-0.3.6-10.1
audiofile-debuginfo-0.3.6-10.1
audiofile-debugsource-0.3.6-10.1

SuSE SLES 12 SP2
x86_64
audiofile-0.3.6-10.1
libaudiofile1-32bit-0.3.6-10.1
libaudiofile1-debuginfo-32bit-0.3.6-10.1
libaudiofile1-debuginfo-0.3.6-10.1
libaudiofile1-0.3.6-10.1
audiofile-debuginfo-0.3.6-10.1
audiofile-debugsource-0.3.6-10.1

SuSE SLED 12 SP2
x86_64
audiofile-0.3.6-10.1
libaudiofile1-32bit-0.3.6-10.1
libaudiofile1-debuginfo-32bit-0.3.6-10.1
libaudiofile1-debuginfo-0.3.6-10.1
libaudiofile1-0.3.6-10.1
audiofile-debuginfo-0.3.6-10.1
audiofile-debugsource-0.3.6-10.1

SuSE SLES 12 SP1
x86_64
audiofile-0.3.6-10.1
libaudiofile1-32bit-0.3.6-10.1
libaudiofile1-debuginfo-32bit-0.3.6-10.1
libaudiofile1-debuginfo-0.3.6-10.1
libaudiofile1-0.3.6-10.1
audiofile-debuginfo-0.3.6-10.1
audiofile-debugsource-0.3.6-10.1

145295 - SuSE SLES 11 SP4 SUSE-SU-2017:0946-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10251, CVE-2016-8654, CVE-2016-9395, CVE-2016-9398, CVE-2016-9560, CVE-2016-9583, CVE-2016-9591, CVE-2016-9600, CVE-2017-5498, CVE-2017-6850

Description

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

SUSE-SU-2017:0946-1

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-April/002785.html>

SuSE SLES 11 SP4
i586
libjasper-1.900.14-134.32.1

x86_64
libjasper-32bit-1.900.14-134.32.1
libjasper-1.900.14-134.32.1

175137 - Scientific Linux Security ERRATA Moderate: ocaml on SL6.x i386/x86_64 (1704-797)

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

Risk Level: Medium

CVE: CVE-2015-8869

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ocaml on SL6.x i386/x86_64 (1704-797)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=797>

SL6

x86_64

ocaml-labltk-3.11.2-5.el6

ocaml-emacs-3.11.2-5.el6

ocaml-ocamldoc-3.11.2-5.el6

ocaml-debuginfo-3.11.2-5.el6

ocaml-x11-3.11.2-5.el6

ocaml-source-3.11.2-5.el6

ocaml-runtime-3.11.2-5.el6

ocaml-3.11.2-5.el6

ocaml-camlp4-3.11.2-5.el6

ocaml-camlp4-devel-3.11.2-5.el6

ocaml-labltk-devel-3.11.2-5.el6

ocaml-docs-3.11.2-5.el6

i386

ocaml-labltk-3.11.2-5.el6

ocaml-emacs-3.11.2-5.el6

ocaml-ocamldoc-3.11.2-5.el6

ocaml-debuginfo-3.11.2-5.el6

ocaml-x11-3.11.2-5.el6

ocaml-source-3.11.2-5.el6

ocaml-runtime-3.11.2-5.el6

ocaml-3.11.2-5.el6

ocaml-camlp4-3.11.2-5.el6

ocaml-camlp4-devel-3.11.2-5.el6

ocaml-labltk-devel-3.11.2-5.el6

ocaml-docs-3.11.2-5.el6

175139 - Scientific Linux Security ERRATA Moderate: libguestfs on SL6.x x86_64 (1704-1463)

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

Risk Level: Medium

CVE: CVE-2015-8869

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libguestfs on SL6.x x86_64 (1704-1463)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=1463>

SL6
x86_64
ocaml-libguestfs-devel-1.20.11-20.el6
libguestfs-java-1.20.11-20.el6
perl-Sys-Guestfs-1.20.11-20.el6
libguestfs-tools-1.20.11-20.el6
libguestfs-devel-1.20.11-20.el6
libguestfs-java-devel-1.20.11-20.el6
python-libguestfs-1.20.11-20.el6
ocaml-libguestfs-1.20.11-20.el6
ruby-libguestfs-1.20.11-20.el6
libguestfs-debuginfo-1.20.11-20.el6
libguestfs-tools-c-1.20.11-20.el6
libguestfs-javadoc-1.20.11-20.el6
libguestfs-1.20.11-20.el6

175145 - Scientific Linux Security ERRATA Moderate: tigervnc on SL6.x i386/x86_64 (1704-5623)

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

Risk Level: Medium

CVE: CVE-2016-10207, CVE-2017-5581

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: tigervnc on SL6.x i386/x86_64 (1704-5623)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=5623>

SL6
i386
tigervnc-server-1.1.0-24.el6
tigervnc-1.1.0-24.el6
tigervnc-debuginfo-1.1.0-24.el6
tigervnc-server-module-1.1.0-24.el6

noarch
tigervnc-server-applet-1.1.0-24.el6

x86_64
tigervnc-server-1.1.0-24.el6
tigervnc-1.1.0-24.el6
tigervnc-debuginfo-1.1.0-24.el6
tigervnc-server-module-1.1.0-24.el6

185662 - Ubuntu Linux 16.04, 16.10 USN-3257-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9642, CVE-2016-9643, CVE-2017-2364, CVE-2017-2367, CVE-2017-2376, CVE-2017-2377, CVE-2017-2386, CVE-2017-2392, CVE-2017-2394, CVE-2017-2395, CVE-2017-2396, CVE-2017-2405, CVE-2017-2415, CVE-2017-2419, CVE-2017-2433, CVE-2017-2442, CVE-2017-2445, CVE-2017-2446, CVE-2017-2447, CVE-2017-2454, CVE-2017-2455, CVE-2017-2457, CVE-2017-

2459, CVE-2017-2460, CVE-2017-2464, CVE-2017-2465, CVE-2017-2466, CVE-2017-2468, CVE-2017-2469, CVE-2017-2470, CVE-2017-2471, CVE-2017-2475, CVE-2017-2476, CVE-2017-2481

Description

The scan detected that the host is missing the following update:
USN-3257-1

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-April/003812.html>

Ubuntu 16.10

libjavascriptcoregtk-4.0-18_2.16.1-0ubuntu0.16.10.1
libwebkit2gtk-4.0-37_2.16.1-0ubuntu0.16.10.1

Ubuntu 16.04

libjavascriptcoregtk-4.0-18_2.16.1-0ubuntu0.16.04.1
libwebkit2gtk-4.0-37_2.16.1-0ubuntu0.16.04.1

191926 - Fedora Linux 26 FEDORA-2017-05b9048fbc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10266, CVE-2016-10267, CVE-2016-10268, CVE-2016-10269, CVE-2016-10270, CVE-2016-10271, CVE-2016-10272

Description

The scan detected that the host is missing the following update:
FEDORA-2017-05b9048fbc

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/2017/4/?count=200&page=2>

Fedora Core 26

libtiff-4.0.7-4.fc26

191928 - Fedora Linux 25 FEDORA-2017-ab3acddd21 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10266, CVE-2016-10267, CVE-2016-10268, CVE-2016-10269, CVE-2016-10270, CVE-2016-10271, CVE-2016-10272

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ab3acddd21

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/2017/4/?count=200&page=1>

Fedora Core 25

libtiff-4.0.7-4.fc25

191934 - Fedora Linux 25 FEDORA-2017-51979161f4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7392, CVE-2017-7393, CVE-2017-7394, CVE-2017-7395, CVE-2017-7396

Description

The scan detected that the host is missing the following update:
FEDORA-2017-51979161f4

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

Fedora Core 25

tigervnc-1.7.1-3.fc25

191936 - Fedora Linux 26 FEDORA-2017-2d0066d567 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7392, CVE-2017-7393, CVE-2017-7394, CVE-2017-7395, CVE-2017-7396

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2d0066d567

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/2017/4/?count=200&page=1>

Fedora Core 26

tigervnc-1.7.1-4.fc26

21632 - (VMSA-2017-0006) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4902, CVE-2017-4903, CVE-2017-4904, CVE-2017-4905

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components. Successful exploitation could allow a local attacker to obtain sensitive information, execute arbitrary code in the context of the host.

21633 - (VMSA-2017-0006) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Pro.

Observation

VMware Workstation is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Pro. The flaws lie in multiple components. Successful exploitation could allow a local attacker to obtain sensitive information, execute arbitrary code in the context of the host.

145286 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0966-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5838

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0966-1

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-April/002791.html>

SuSE SLED 12 SP2

x86_64

gstreamer-debuginfo-32bit-1.8.3-9.5

typelib-1_0-Gst-1_0-1.8.3-9.5

gstreamer-debuginfo-1.8.3-9.5

libgstreamer-1_0-0-32bit-1.8.3-9.5

gstreamer-debugsource-1.8.3-9.5

gstreamer-utils-debuginfo-1.8.3-9.5

gstreamer-1.8.3-9.5

libgstreamer-1_0-0-1.8.3-9.5

libgstreamer-1_0-0-debuginfo-32bit-1.8.3-9.5

libgstreamer-1_0-0-debuginfo-1.8.3-9.5
gstreamer-utils-1.8.3-9.5

noarch
gstreamer-lang-1.8.3-9.5

SuSE SLES 12 SP2
noarch
gstreamer-lang-1.8.3-9.5

x86_64
libgstreamer-1_0-0-debuginfo-1.8.3-9.5
typelib-1_0-Gst-1_0-1.8.3-9.5
gstreamer-debuginfo-1.8.3-9.5
gstreamer-utils-1.8.3-9.5
gstreamer-debugsource-1.8.3-9.5
gstreamer-1.8.3-9.5
libgstreamer-1_0-0-32bit-1.8.3-9.5
libgstreamer-1_0-0-1.8.3-9.5
libgstreamer-1_0-0-debuginfo-32bit-1.8.3-9.5
gstreamer-debuginfo-32bit-1.8.3-9.5
gstreamer-utils-debuginfo-1.8.3-9.5

145289 - SuSE SLED 12 SP2 SUSE-SU-2017:0945-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2007-3126

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0945-1

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-April/002784.html>

SuSE SLED 12 SP2
x86_64
gimp-plugins-python-2.8.18-8.1
libgimp-2_0-0-debuginfo-2.8.18-8.1
gimp-2.8.18-8.1
libgimp-2_0-0-2.8.18-8.1
libgimpui-2_0-0-2.8.18-8.1
gimp-plugins-python-debuginfo-2.8.18-8.1
gimp-debuginfo-2.8.18-8.1
libgimpui-2_0-0-debuginfo-2.8.18-8.1
gimp-debugsource-2.8.18-8.1

noarch
gimp-lang-2.8.18-8.1

145290 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:0967-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2017-5838

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0967-1

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-April/002792.html>

SuSE SLES 12 SP1

noarch
gstreamer-lang-1.2.4-2.3.3

x86_64
gstreamer-1.2.4-2.3.3
libgstreamer-1_0-0-debuginfo-32bit-1.2.4-2.3.3
gstreamer-debuginfo-1.2.4-2.3.3
libgstreamer-1_0-0-32bit-1.2.4-2.3.3
typelib-1_0-Gst-1_0-1.2.4-2.3.3
libgstreamer-1_0-0-debuginfo-1.2.4-2.3.3
gstreamer-utils-debuginfo-1.2.4-2.3.3
gstreamer-utils-1.2.4-2.3.3
gstreamer-debugsource-1.2.4-2.3.3
gstreamer-debuginfo-32bit-1.2.4-2.3.3
libgstreamer-1_0-0-1.2.4-2.3.3

SuSE SLED 12 SP1

x86_64
gstreamer-1.2.4-2.3.3
libgstreamer-1_0-0-debuginfo-32bit-1.2.4-2.3.3
gstreamer-debuginfo-1.2.4-2.3.3
libgstreamer-1_0-0-32bit-1.2.4-2.3.3
typelib-1_0-Gst-1_0-1.2.4-2.3.3
libgstreamer-1_0-0-debuginfo-1.2.4-2.3.3
gstreamer-utils-debuginfo-1.2.4-2.3.3
gstreamer-utils-1.2.4-2.3.3
gstreamer-debugsource-1.2.4-2.3.3
gstreamer-debuginfo-32bit-1.2.4-2.3.3
libgstreamer-1_0-0-1.2.4-2.3.3

noarch
gstreamer-lang-1.2.4-2.3.3

145296 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0962-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5843, CVE-2017-5848

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0962-1

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-April/002790.html>

SuSE SLED 12 SP2

x86_64

libgstbadvideo-1_0-0-debuginfo-1.8.3-17.2
libgstadaptivedemux-1_0-0-debuginfo-1.8.3-17.2
libgstcodecparsers-1_0-0-debuginfo-1.8.3-17.2
libgstphotography-1_0-0-debuginfo-1.8.3-17.2
libgstbadaudio-1_0-0-debuginfo-1.8.3-17.2
gststreamer-plugins-bad-debugsource-1.8.3-17.2
libgstgl-1_0-0-1.8.3-17.2
gststreamer-plugins-bad-1.8.3-17.2
libgstmpegts-1_0-0-debuginfo-1.8.3-17.2
gststreamer-plugins-bad-debuginfo-1.8.3-17.2
libgstbadvideo-1_0-0-1.8.3-17.2
libgstbasecamerabinsrc-1_0-0-1.8.3-17.2
libgstcodecparsers-1_0-0-1.8.3-17.2
libgstadaptivedemux-1_0-0-1.8.3-17.2
libgstphotography-1_0-0-1.8.3-17.2
libgstgl-1_0-0-debuginfo-1.8.3-17.2
libgstbadbase-1_0-0-debuginfo-1.8.3-17.2
libgstbadaudio-1_0-0-1.8.3-17.2
libgsturidownloader-1_0-0-1.8.3-17.2
libgstbasecamerabinsrc-1_0-0-debuginfo-1.8.3-17.2
libgsturidownloader-1_0-0-debuginfo-1.8.3-17.2
libgstmpegts-1_0-0-1.8.3-17.2
libgstbadbase-1_0-0-1.8.3-17.2

noarch

gststreamer-plugins-bad-lang-1.8.3-17.2

SuSE SLES 12 SP2

noarch

gststreamer-plugins-bad-lang-1.8.3-17.2

x86_64

libgstbadvideo-1_0-0-debuginfo-1.8.3-17.2
libgstadaptivedemux-1_0-0-debuginfo-1.8.3-17.2
libgstcodecparsers-1_0-0-debuginfo-1.8.3-17.2
libgstphotography-1_0-0-debuginfo-1.8.3-17.2
libgstbadaudio-1_0-0-debuginfo-1.8.3-17.2
gststreamer-plugins-bad-debugsource-1.8.3-17.2
libgstgl-1_0-0-1.8.3-17.2
gststreamer-plugins-bad-1.8.3-17.2
libgstmpegts-1_0-0-debuginfo-1.8.3-17.2
gststreamer-plugins-bad-debuginfo-1.8.3-17.2
libgstbadvideo-1_0-0-1.8.3-17.2
libgstbasecamerabinsrc-1_0-0-1.8.3-17.2
libgstcodecparsers-1_0-0-1.8.3-17.2
libgstadaptivedemux-1_0-0-1.8.3-17.2
libgstphotography-1_0-0-1.8.3-17.2
libgstgl-1_0-0-debuginfo-1.8.3-17.2
libgstbadbase-1_0-0-debuginfo-1.8.3-17.2
libgstbadaudio-1_0-0-1.8.3-17.2
libgsturidownloader-1_0-0-1.8.3-17.2
libgstbasecamerabinsrc-1_0-0-debuginfo-1.8.3-17.2

libgstridownloader-1_0-0-debuginfo-1.8.3-17.2
libgstmpegts-1_0-0-1.8.3-17.2
libgstbadbase-1_0-0-1.8.3-17.2

175134 - Scientific Linux Security ERRATA Moderate: samba4 on SL6.x i386/x86_64 (1704-4167)

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

Risk Level: Medium

CVE: CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: samba4 on SL6.x i386/x86_64 (1704-4167)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=4167>

SL6

x86_64
samba4-dc-libs-4.2.10-9.el6
samba4-test-4.2.10-9.el6
samba4-devel-4.2.10-9.el6
samba4-winbind-krb5-locator-4.2.10-9.el6
samba4-common-4.2.10-9.el6
samba4-winbind-4.2.10-9.el6
samba4-client-4.2.10-9.el6
samba4-winbind-clients-4.2.10-9.el6
samba4-dc-4.2.10-9.el6
samba4-pidl-4.2.10-9.el6
samba4-libs-4.2.10-9.el6
samba4-debuginfo-4.2.10-9.el6
samba4-python-4.2.10-9.el6
samba4-4.2.10-9.el6

i386

samba4-dc-libs-4.2.10-9.el6
samba4-test-4.2.10-9.el6
samba4-devel-4.2.10-9.el6
samba4-winbind-krb5-locator-4.2.10-9.el6
samba4-common-4.2.10-9.el6
samba4-winbind-4.2.10-9.el6
samba4-client-4.2.10-9.el6
samba4-winbind-clients-4.2.10-9.el6
samba4-dc-4.2.10-9.el6
samba4-pidl-4.2.10-9.el6
samba4-libs-4.2.10-9.el6
samba4-debuginfo-4.2.10-9.el6
samba4-python-4.2.10-9.el6
samba4-4.2.10-9.el6

175136 - Scientific Linux Security ERRATA Moderate: coreutils on SL6.x i386/x86_64 (1704-3436)

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

Risk Level: Medium

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: coreutils on SL6.x i386/x86_64 (1704-3436)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=3436>

SL6
x86_64
coreutils-libs-8.4-46.el6
coreutils-8.4-46.el6
coreutils-debuginfo-8.4-46.el6

i386
coreutils-libs-8.4-46.el6
coreutils-8.4-46.el6
coreutils-debuginfo-8.4-46.el6

175148 - Scientific Linux Security ERRATA Moderate: subscription-manager on SL6.x i386/x86_64 (1704-4522)

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

Risk Level: Medium

CVE: CVE-2016-4455

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: subscription-manager on SL6.x i386/x86_64 (1704-4522)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=4522>

SL6
i386
python-rhsm-certificates-1.18.6-1.el6
subscription-manager-firstboot-1.18.10-1.el6
python-rhsm-1.18.6-1.el6
subscription-manager-migration-1.18.10-1.el6
subscription-manager-1.18.10-1.el6
subscription-manager-plugin-container-1.18.10-1.el6
subscription-manager-debuginfo-1.18.10-1.el6
subscription-manager-gui-1.18.10-1.el6
python-rhsm-debuginfo-1.18.6-1.el6

noarch
subscription-manager-migration-data-2.0.34-1.el6

x86_64
python-rhsm-certificates-1.18.6-1.el6
subscription-manager-firstboot-1.18.10-1.el6

python-rhsm-1.18.6-1.el6
subscription-manager-migration-1.18.10-1.el6
subscription-manager-1.18.10-1.el6
subscription-manager-plugin-container-1.18.10-1.el6
subscription-manager-debuginfo-1.18.10-1.el6
subscription-manager-gui-1.18.10-1.el6
python-rhsm-debuginfo-1.18.6-1.el6

175149 - Scientific Linux Security ERRATA Moderate: curl on SL6.x i386/x86_64 (1704-76)

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

Risk Level: Medium

CVE: CVE-2015-3148, CVE-2017-2628

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: curl on SL6.x i386/x86_64 (1704-76)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=76>

SL6
x86_64
curl-7.19.7-53.el6_9
curl-debuginfo-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

i386
curl-7.19.7-53.el6_9
curl-debuginfo-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

175150 - Scientific Linux Security ERRATA Moderate: samba on SL6.x i386/x86_64 (1704-4902)

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

Risk Level: Medium

CVE: CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: samba on SL6.x i386/x86_64 (1704-4902)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=4902>

SL6
x86_64
samba-winbind-clients-3.6.23-41.el6

samba-glusterfs-3.6.23-41.el6
libsmbclient-3.6.23-41.el6
samba-swat-3.6.23-41.el6
samba-winbind-3.6.23-41.el6
samba-winbind-krb5-locator-3.6.23-41.el6
libsmbclient-devel-3.6.23-41.el6
samba-common-3.6.23-41.el6
samba-doc-3.6.23-41.el6
samba-debuginfo-3.6.23-41.el6
samba-winbind-devel-3.6.23-41.el6
samba-client-3.6.23-41.el6
samba-domainjoin-gui-3.6.23-41.el6
samba-3.6.23-41.el6

i386

samba-winbind-clients-3.6.23-41.el6
libsmbclient-3.6.23-41.el6
samba-swat-3.6.23-41.el6
samba-winbind-3.6.23-41.el6
samba-winbind-krb5-locator-3.6.23-41.el6
libsmbclient-devel-3.6.23-41.el6
samba-common-3.6.23-41.el6
samba-doc-3.6.23-41.el6
samba-debuginfo-3.6.23-41.el6
samba-winbind-devel-3.6.23-41.el6
samba-client-3.6.23-41.el6
samba-domainjoin-gui-3.6.23-41.el6
samba-3.6.23-41.el6

178421 - Gentoo Linux GLSA-201704-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Description

The scan detected that the host is missing the following update:
GLSA-201704-02

Observation

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

<https://security.gentoo.org/glsa/201704-02>

Affected packages:

www-client/chromium < 57.0.2987.133

178422 - Gentoo Linux GLSA-201704-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9602, CVE-2017-2620, CVE-2017-2630, CVE-2017-5973, CVE-2017-5987, CVE-2017-6058, CVE-2017-6505

Description

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

GLSA-201704-01

Observation

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

<https://security.gentoo.org/glsa/201704-01>

Affected packages:

app-emulation/qemu < 2.8.0-r9

191937 - Fedora Linux 26 FEDORA-2017-1d305fa070 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10087

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1d305fa070

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/2017/4/?count=200&page=1>

Fedora Core 26

libpng12-1.2.57-1.fc26

145287 - SuSE SLES 11 SP4 SUSE-SU-2017:0948-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1855, CVE-2015-7551

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0948-1

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-April/002786.html>

SuSE SLES 11 SP4

i586

ruby-1.8.7.p357-0.9.19.1

ruby-tk-1.8.7.p357-0.9.19.1

ruby-doc-html-1.8.7.p357-0.9.19.1

x86_64

ruby-1.8.7.p357-0.9.19.1

ruby-tk-1.8.7.p357-0.9.19.1
ruby-doc-html-1.8.7.p357-0.9.19.1

191929 - Fedora Linux 26 FEDORA-2017-628b627eac Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7207

Description

The scan detected that the host is missing the following update:
FEDORA-2017-628b627eac

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/2017/4/?count=200&page=1>

Fedora Core 26

ghostscript-9.20-8.fc26

191932 - Fedora Linux 25 FEDORA-2017-047cffb598 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7207

Description

The scan detected that the host is missing the following update:
FEDORA-2017-047cffb598

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/2017/4/?count=200&page=2>

Fedora Core 25

ghostscript-9.20-7.fc25

21518 - (K45427159) F5 BIG-IP NTP Authentication Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> F5
Risk Level: Low
CVE: CVE-2016-1551

Description

A spoofing 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 spoofing vulnerability is present in some versions of F5 BIG-IP systems. The flaw is due to a bad IPv4 bogon packet filtering done by the ntpd process. Successful exploitation could allow a malicious user to conduct spoofing attacks against the target system.

Please refer to our Documentation Standards file:

<http://2010.corp.mcafee.com/sites/fs/Infrastructure/Training/Foundstone%20Threat%20Documentation%20Standard.docx>

Script is working as expected.

88856 - Slackware Linux 14.0, 14.1 SSA:2017-100-01 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:2017-100-01

Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.403724>

Slackware 14.1

x86_64

vim-7.4.399-x86_64-1

vim-gvim-7.4.399-x86_64-1

Slackware 14.0

x86_64

vim-7.4.399-x86_64-1

vim-gvim-7.4.399-x86_64-1

130741 - Debian Linux 8.0 DSA-3828-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2669

Description

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

DSA-3828-1

Observation

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

For more information see:

<http://www.debian.org/security/2017/dsa-3828>

Debian 8.0

all

dovecot-mysql_1:2.2.13-12~deb8u2

dovecot-managesieved_1:2.2.13-12~deb8u2
dovecot-dev_1:2.2.13-12~deb8u2
dovecot-core_1:2.2.13-12~deb8u2
dovecot-imapd_1:2.2.13-12~deb8u2
dovecot-gssapi_1:2.2.13-12~deb8u2
dovecot-pgsql_1:2.2.13-12~deb8u2
dovecot-lucene_1:2.2.13-12~deb8u2
dovecot-pop3d_1:2.2.13-12~deb8u2
dovecot-sqlite_1:2.2.13-12~deb8u2
dovecot-dbg_1:2.2.13-12~deb8u2
dovecot-solr_1:2.2.13-12~deb8u2
dovecot-sieve_1:2.2.13-12~deb8u2
dovecot-lmtpd_1:2.2.13-12~deb8u2
dovecot-ldap_1:2.2.13-12~deb8u2

185661 - Ubuntu Linux 16.04, 16.10 USN-3258-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2669

Description

The scan detected that the host is missing the following update:
USN-3258-2

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-April/003814.html>

Ubuntu 16.10

dovecot-core_2.2.24-1ubuntu1.3

Ubuntu 16.04

dovecot-core_2.2.22-1ubuntu2.4

185663 - Ubuntu Linux 16.04, 16.10 USN-3258-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2669

Description

The scan detected that the host is missing the following update:
USN-3258-1

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-April/003813.html>

Ubuntu 16.10

dovecot-core_2.2.24-1ubuntu1.2

Ubuntu 16.04

dovecot-core_2.2.22-1ubuntu2.3

191927 - Fedora Linux 26 FEDORA-2017-fb9ed95cf3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fb9ed95cf3

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

Fedora Core 26

samba-4.6.2-0.fc26

191930 - Fedora Linux 24 FEDORA-2017-712a186f5f 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-2017-712a186f5f

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

Fedora Core 24

icecat-52.0.1-5.fc24

191931 - Fedora Linux 25 FEDORA-2017-7e5b5201e7 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-2017-7e5b5201e7

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/2017/4/?count=200&page=5>

Fedora Core 25

xen-4.7.2-4.fc25

191933 - Fedora Linux 24 FEDORA-2017-174cb400d7 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-2017-174cb400d7

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/2017/4/?count=200&page=1>

Fedora Core 24

flatpak-0.8.5-1.fc24

191935 - Fedora Linux 25 FEDORA-2017-674d306f51 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-2017-674d306f51

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/2017/4/?count=200&page=3>

Fedora Core 25

icecat-52.0.1-5.fc25

175138 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL6.x i386/x86_64 (1704-1121)

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

Risk Level: Low

CVE: CVE-2016-3712

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: qemu-kvm on SL6.x i386/x86_64 (1704-1121)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=1121>

SL6

x86_64

qemu-kvm-tools-0.12.1.2-2.503.el6

qemu-guest-agent-0.12.1.2-2.503.el6

qemu-img-0.12.1.2-2.503.el6

qemu-kvm-0.12.1.2-2.503.el6

qemu-kvm-debuginfo-0.12.1.2-2.503.el6

i386

qemu-guest-agent-0.12.1.2-2.503.el6

qemu-kvm-debuginfo-0.12.1.2-2.503.el6

182324 - FreeBSD cURL Out Of Buffer Read (04f29189-1a05-11e7-bc6e-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-7407

Description

The scan detected that the host is missing the following update:
cURL -- out of buffer read (04f29189-1a05-11e7-bc6e-b499baebfeaf)

Observation

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

<http://www.vuxml.org/freebsd/04f29189-1a05-11e7-bc6e-b499baebfeaf.html>

Affected packages:

6.5 <= curl < 7.53.1_1

191923 - Fedora Linux 25 FEDORA-2017-b38b98727e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7407

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b38b98727e

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/2017/4/?count=200&page=2>

Fedora Core 25

curl-7.51.0-6.fc25

191938 - Fedora Linux 26 FEDORA-2017-e396614cd0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7407

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e396614cd0

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/2017/4/?count=200&page=1>

Fedora Core 26

curl-7.53.1-4.fc26

21640 - Microsoft Office 2016 Click-To-Run April 2017 Updates

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run.

Observation

Microsoft Office 2016 Click-to-Run is an alternative to the Windows Installer-based (MSI) installation method of the popular office suite.

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run. The flaws are present in multiple components. Such defects could lead the product to software vulnerabilities, malfunction or unexpected behavior in some of its affected components.

ENHANCED CHECKS

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

21141 - IBM WebSphere MQ JMS Client Deserialization RCE Vulnerability

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

Risk Level: High

CVE: CVE-2016-0360

[Update Details](#)

FASLScript is updated

21538 - ACTi Cameras Information Exposure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2017-3185

[Update Details](#)

Recommendation is updated

21537 - ACTi Cameras Missing Authentication for Critical Function Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2017-3184

[Update Details](#)

Recommendation is updated

21539 - ACTi Cameras Weak Password Requirements Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2017-3186

[Update Details](#)

Recommendation is updated

21593 - (MSPT-Apr2017) Microsoft Edge Security Bypass (CVE-2017-0203)

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

Risk Level: High

CVE: CVE-2017-0203

[Update Details](#)

Name is updated

21594 - (MSPT-Apr2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-0205)

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

Risk Level: High

CVE: CVE-2017-0205

[Update Details](#)

Name is updated

21603 - (MSPT-Apr2017) Microsoft .NET Remote Code Execution (CVE-2017-0160)

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

Risk Level: High

CVE: CVE-2017-0160

[Update Details](#)

Name is updated

21604 - (MSPT-Apr2017) Microsoft Internet Explorer Memory Corruption Remote Code Execution (CVE-2017-0202)

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

Risk Level: High

CVE: CVE-2017-0202

[Update Details](#)

Name is updated

21617 - (MSPT-Apr2017) Microsoft Hyper-V Remote Code Execution (CVE-2017-0162)

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

Risk Level: High

CVE: CVE-2017-0162

[Update Details](#)

Name is updated

21618 - (MSPT-Apr2017) Microsoft Hyper-V Remote Code Execution (CVE-2017-0163)

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

Risk Level: High

CVE: CVE-2017-0163

[Update Details](#)

Name is updated

21620 - (MSPT-Apr2017) Microsoft Windows Hyper-V Remote Code Execution (CVE-2017-0181)

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

Risk Level: High

CVE: CVE-2017-0181

[Update Details](#)

Name is updated

21627 - (MSPT-Apr2017) Microsoft Internet Explorer Privilege Escalation (CVE-2017-0210)

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Name is updated

21514 - D-link Dir-850l Web Admin Interface Stack-based Buffer Overflow Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: High

CVE: CVE-2017-3193

[Update Details](#)

Recommendation is updated

21584 - (MSPT-Apr2017) Microsoft Outlook Parsing Remote Code Execution (CVE-2017-0106)

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

Risk Level: High

CVE: CVE-2017-0106

[Update Details](#)

Name is updated

21587 - (MSPT-Apr2017) Microsoft Office DLL Loading Remote Code Execution (CVE-2017-0197)

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

Risk Level: High

CVE: CVE-2017-0197

[Update Details](#)

Name is updated

21588 - (MSPT-Apr2017) Microsoft Outlook Parsing Remote Code Execution (CVE-2017-0199)

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

Risk Level: High

CVE: CVE-2017-0199

[Update Details](#)

Name is updated

21592 - (MSPT-Apr2017) Microsoft Windows Memory Handling Denial of Service (CVE-2017-0191)

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

Risk Level: High

CVE: CVE-2017-0191

Update Details

Name is updated

21595 - (MSPT-Apr2017) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2017-0093)

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

Risk Level: High

CVE: CVE-2017-0093

Update Details

Name is updated

21596 - (MSPT-Apr2017) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2017-0200)

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

Risk Level: High

CVE: CVE-2017-0200

Update Details

Name is updated

21605 - (MSPT-Apr2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-0201)

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

Risk Level: High

CVE: CVE-2017-0201

Update Details

Name is updated

21606 - (MSPT-Apr2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-0158)

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

Risk Level: High

CVE: CVE-2017-0158

Update Details

Name is updated

21619 - (MSPT-Apr2017) Microsoft Windows Hyper-V Remote Code Execution (CVE-2017-0180)

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

Risk Level: High

CVE: CVE-2017-0180

Update Details

Name is updated

21498 - DotCMS Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-3187, CVE-2017-3188, CVE-2017-3189

Update Details

Recommendation is updated

21583 - (MSPT-Apr2017) Microsoft Office Spoofing (CVE-2017-0207)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-0207

Update Details

Name is updated

21585 - (MSPT-Apr2017) Microsoft Office Memory Corruption Information Disclosure (CVE-2017-0194)

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

Risk Level: Medium

CVE: CVE-2017-0194

Update Details

Name is updated

21586 - (MSPT-Apr2017) Microsoft Office Cross Site Scripting Privilege Escalation (CVE-2017-0195)

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

Risk Level: Medium

CVE: CVE-2017-0195

Update Details

Name is updated FASLScript is updated

21589 - (MSPT-Apr2017) Microsoft Office File Parsing Security Bypass (CVE-2017-0204)

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

Risk Level: Medium

CVE: CVE-2017-0204

Update Details

Name is updated

21590 - (MSPT-Apr2017) Microsoft Active Directory Denial of Service (CVE-2017-0164)

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

Risk Level: Medium

CVE: CVE-2017-0164

Update Details

Name is updated

21591 - (MSPT-Apr2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-0167)

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

Risk Level: Medium

CVE: CVE-2017-0167

Update Details

Name is updated

21597 - (MSPT-Apr2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-0058)

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

Risk Level: Medium

CVE: CVE-2017-0058

Update Details

Name is updated

21598 - (MSPT-Apr2017) Microsoft Windows Kernel Privilege Escalation (CVE-2017-0189)

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

Risk Level: Medium

CVE: CVE-2017-0189

Update Details

Name is updated

21599 - (MSPT-Apr2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-0188)

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

Risk Level: Medium

CVE: CVE-2017-0188

[Update Details](#)

Name is updated

21600 - (MSPT-Apr2017) Microsoft ATMFd.dll Information Disclosure (CVE-2017-0192)

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

Risk Level: Medium

CVE: CVE-2017-0192

[Update Details](#)

Name is updated

21601 - (MSPT-Apr2017) Microsoft Windows Graphics Privilege Escalation (CVE-2017-0155)

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

Risk Level: Medium

CVE: CVE-2017-0155

[Update Details](#)

Name is updated

21602 - (MSPT-Apr2017) Microsoft Windows Handle Sanitization Privilege Escalation (CVE-2017-0165)

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

Risk Level: Medium

CVE: CVE-2017-0165

[Update Details](#)

Name is updated

21607 - (MSPT-Apr2017) Microsoft Edge Scripting Engine Information Disclosure (CVE-2017-0208)

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

Risk Level: Medium

CVE: CVE-2017-0208

[Update Details](#)

Name is updated

21608 - (MSPT-Apr2017) Microsoft Hyper-V Denial of Service (CVE-2017-0178)

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

Risk Level: Medium

CVE: CVE-2017-0178

[Update Details](#)

Name is updated

21609 - (MSPT-Apr2017) Microsoft Hyper-V Denial of Service (CVE-2017-0179)

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

Risk Level: Medium

CVE: CVE-2017-0179

Update Details

Name is updated

21610 - (MSPT-Apr2017) Microsoft Hyper-V Denial of Service (CVE-2017-0182)

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

Risk Level: Medium

CVE: CVE-2017-0182

Update Details

Name is updated

21611 - (MSPT-Apr2017) Microsoft Hyper-V Denial of Service (CVE-2017-0183)

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

Risk Level: Medium

CVE: CVE-2017-0183

Update Details

Name is updated

21612 - (MSPT-Apr2017) Microsoft Hyper-V Denial of Service (CVE-2017-0184)

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

Risk Level: Medium

CVE: CVE-2017-0184

Update Details

Name is updated

21613 - (MSPT-Apr2017) Microsoft Hyper-V Denial of Service (CVE-2017-0185)

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

Risk Level: Medium

CVE: CVE-2017-0185

Update Details

Name is updated

21614 - (MSPT-Apr2017) Microsoft Hyper-V Denial of Service (CVE-2017-0186)

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

Risk Level: Medium

CVE: CVE-2017-0186

Update Details

Name is updated

21615 - (MSPT-Apr2017) Microsoft Hyper-V Information Disclosure (CVE-2017-0168)

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

Risk Level: Medium

CVE: CVE-2017-0168

Update Details

Name is updated

21616 - (MSPT-Apr2017) Microsoft Hyper-V Information Disclosure (CVE-2017-0169)

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

Risk Level: Medium

CVE: CVE-2017-0169

Update Details

Name is updated

21621 - (MSPT-Apr2017) Microsoft Windows libjpeg Information Disclosure (CVE-2013-6629)

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

Risk Level: Medium

CVE: CVE-2013-6629

Update Details

Name is updated

21622 - (MSPT-Apr2017) Microsoft LDAP Privilege Escalation (CVE-2017-0166)

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

Risk Level: Medium

CVE: CVE-2017-0166

Update Details

Name is updated

21623 - (MSPT-Apr2017) Microsoft ADFS Security Bypass (CVE-2017-0159)

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

Risk Level: Medium

CVE: CVE-2017-0159

Update Details

Name is updated

21626 - (MSPT-Apr2017) Microsoft Windows OLE Privilege Escalation (CVE-2017-0211)

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

Risk Level: Medium

CVE: CVE-2017-0211

Update Details

Name is updated

21628 - (MSPT-Apr2017) Microsoft Windows Graphics Privilege Escalation (CVE-2017-0156)

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

Risk Level: Medium

CVE: CVE-2017-0156

Update Details

Name is updated

19579 - (SOL22843911) F5 BIG-IP F5 Path MTU Discovery Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7759

Update Details

FASLScript is updated

33285 - Oracle Solaris 151074-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3956

Update Details

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

33286 - Oracle Solaris 151075-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3956

Update Details

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

70074 - mcafee.fasI3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70131 - f5.fasI3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFFEE 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.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2017 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates