

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

21035 - (APSB16-41) Vulnerability In Adobe DNG Converter

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-7856

Description

A memory corruption vulnerability is present in some versions of Adobe DNG Converter.

Observation

Adobe DNG Converter is a software used to convert image to DNG format.

A memory corruption vulnerability is present in some versions of Adobe DNG Converter. The flaw lies in unspecified component. Successful exploitation could allow an attacker to execute arbitrary code.

The update provided by Adobe bulletin APSB16-41 resolves this issue. The target system appears to be missing this update.

21036 - (HT207422) Apple iOS Multiple Vulnerabilities Prior To 10.2

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2016-4689, CVE-2016-4690, CVE-2016-4691, CVE-2016-4692, CVE-2016-4693, CVE-2016-4743, CVE-2016-4781, CVE-2016-7586, CVE-2016-7587, CVE-2016-7588, CVE-2016-7589, CVE-2016-7591, CVE-2016-7592, CVE-2016-7594, CVE-2016-7595, CVE-2016-7597, CVE-2016-7598, CVE-2016-7599, CVE-2016-7601, CVE-2016-7606, CVE-2016-7607, CVE-2016-7610, CVE-2016-7611, CVE-2016-7612, CVE-2016-7615, CVE-2016-7616, CVE-2016-7619, CVE-2016-7621, CVE-2016-7623, CVE-2016-7626, CVE-2016-7627, CVE-2016-7632, CVE-2016-7634, CVE-2016-7635, CVE-2016-7636, CVE-2016-7637, CVE-2016-7638, CVE-2016-7639, CVE-2016-7640, CVE-2016-7641, CVE-2016-7642, CVE-2016-7643, CVE-2016-7644, CVE-2016-7645, CVE-2016-7646, CVE-2016-7648, CVE-2016-7649, CVE-2016-7650, CVE-2016-7651, CVE-2016-7652, CVE-2016-7653, CVE-2016-7654, CVE-2016-7655, CVE-2016-7656, CVE-2016-7657, CVE-2016-7658, CVE-2016-7659, CVE-2016-7660, CVE-2016-7661, CVE-2016-7662, CVE-2016-7663, CVE-2016-7664, CVE-2016-7665, CVE-2016-7667

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

Apple iOS is the operating system used by Apple iPhone, iPad and iPod touch.

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or execute arbitrary code.

21037 - (K14338030) F5 BIG-IP Libxml2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-1762

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the xmlNextChar function in libxml2. Successful exploitation could allow an attacker to cause a denial of service condition.

141383 - Red Hat Enterprise Linux RHSA-2016-2962 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

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

RHSA-2016-2962

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2962.html>

RHEL5D

i386

kernel-debug-devel-2.6.18-417.el5

kernel-xen-debuginfo-2.6.18-417.el5

kernel-debug-debuginfo-2.6.18-417.el5

kernel-devel-2.6.18-417.el5

kernel-2.6.18-417.el5

kernel-debuginfo-2.6.18-417.el5

kernel-PAE-2.6.18-417.el5

kernel-xen-devel-2.6.18-417.el5

kernel-headers-2.6.18-417.el5

kernel-debuginfo-common-2.6.18-417.el5

kernel-xen-2.6.18-417.el5

kernel-PAE-devel-2.6.18-417.el5

kernel-PAE-debuginfo-2.6.18-417.el5

kernel-debug-2.6.18-417.el5

noarch

kernel-doc-2.6.18-417.el5

x86_64

kernel-xen-debuginfo-2.6.18-417.el5

kernel-debug-debuginfo-2.6.18-417.el5

kernel-debuginfo-common-2.6.18-417.el5

kernel-xen-devel-2.6.18-417.el5

kernel-debug-2.6.18-417.el5

kernel-devel-2.6.18-417.el5

kernel-debug-devel-2.6.18-417.el5
kernel-2.6.18-417.el5
kernel-xen-2.6.18-417.el5
kernel-debuginfo-2.6.18-417.el5
kernel-headers-2.6.18-417.el5

RHEL5S
noarch
kernel-doc-2.6.18-417.el5

x86_64
kernel-xen-debuginfo-2.6.18-417.el5
kernel-debug-debuginfo-2.6.18-417.el5
kernel-debuginfo-common-2.6.18-417.el5
kernel-xen-devel-2.6.18-417.el5
kernel-debug-2.6.18-417.el5
kernel-devel-2.6.18-417.el5
kernel-debug-devel-2.6.18-417.el5
kernel-2.6.18-417.el5
kernel-xen-2.6.18-417.el5
kernel-debuginfo-2.6.18-417.el5
kernel-headers-2.6.18-417.el5

i386
kernel-debug-devel-2.6.18-417.el5
kernel-xen-debuginfo-2.6.18-417.el5
kernel-debug-debuginfo-2.6.18-417.el5
kernel-devel-2.6.18-417.el5
kernel-2.6.18-417.el5
kernel-debuginfo-2.6.18-417.el5
kernel-PAE-2.6.18-417.el5
kernel-xen-devel-2.6.18-417.el5
kernel-headers-2.6.18-417.el5
kernel-debuginfo-common-2.6.18-417.el5
kernel-xen-2.6.18-417.el5
kernel-PAE-devel-2.6.18-417.el5
kernel-PAE-debuginfo-2.6.18-417.el5
kernel-debug-2.6.18-417.el5

141385 - Red Hat Enterprise Linux RHSA-2016-2947 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7867, CVE-2016-7868, CVE-2016-7869, CVE-2016-7870, CVE-2016-7871, CVE-2016-7872, CVE-2016-7873, CVE-2016-7874, CVE-2016-7875, CVE-2016-7876, CVE-2016-7877, CVE-2016-7878, CVE-2016-7879, CVE-2016-7880, CVE-2016-7881, CVE-2016-7890, CVE-2016-7892

Description

The scan detected that the host is missing the following update:
RHSA-2016-2947

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2947.html>

RHEL6D

x86_64
flash-plugin-24.0.0.186-1.el6_8

i386
flash-plugin-24.0.0.186-1.el6_8

RHEL6S
x86_64
flash-plugin-24.0.0.186-1.el6_8

i386
flash-plugin-24.0.0.186-1.el6_8

RHEL6WS
x86_64
flash-plugin-24.0.0.186-1.el6_8

i386
flash-plugin-24.0.0.186-1.el6_8

145086 - SuSE SLED 12 SP1 SUSE-SU-2016:3148-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7867, CVE-2016-7868, CVE-2016-7869, CVE-2016-7870, CVE-2016-7871, CVE-2016-7872, CVE-2016-7873, CVE-2016-7874, CVE-2016-7875, CVE-2016-7876, CVE-2016-7877, CVE-2016-7878, CVE-2016-7879, CVE-2016-7880, CVE-2016-7881, CVE-2016-7890, CVE-2016-7892

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3148-1

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-December/002486.html>

SuSE SLED 12 SP1
x86_64
flash-player-24.0.0.186-152.1
flash-player-gnome-24.0.0.186-152.1

160179 - CentOS 5 CESA-2016-2962 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

The scan detected that the host is missing the following update:
CESA-2016-2962

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-December/022182.html>

CentOS 5
i386
kernel-headers-2.6.18-417.el5

i686
kernel-PAE-2.6.18-417.el5
kernel-xen-devel-2.6.18-417.el5
kernel-debug-2.6.18-417.el5
kernel-PAE-devel-2.6.18-417.el5
kernel-devel-2.6.18-417.el5
kernel-debug-devel-2.6.18-417.el5
kernel-2.6.18-417.el5
kernel-xen-2.6.18-417.el5

noarch
kernel-doc-2.6.18-417.el5

x86_64
kernel-xen-devel-2.6.18-417.el5
kernel-debug-2.6.18-417.el5
kernel-devel-2.6.18-417.el5
kernel-debug-devel-2.6.18-417.el5
kernel-2.6.18-417.el5
kernel-xen-2.6.18-417.el5
kernel-headers-2.6.18-417.el5

175049 - Scientific Linux Security ERRATA Important: mariadb on SL7.x x86_64 (1612-6698)

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: mariadb on SL7.x x86_64 (1612-6698)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=6698>

SL7
x86_64
mariadb-debuginfo-5.5.52-1.el7
mariadb-server-5.5.52-1.el7
mariadb-test-5.5.52-1.el7
mariadb-embedded-devel-5.5.52-1.el7
mariadb-embedded-5.5.52-1.el7
mariadb-devel-5.5.52-1.el7
mariadb-5.5.52-1.el7
mariadb-bench-5.5.52-1.el7
mariadb-libs-5.5.52-1.el7

175052 - Scientific Linux Security ERRATA Low: python on SL7.x x86_64 (1612-7169)

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

Risk Level: High

CVE: CVE-2016-5636

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: python on SL7.x x86_64 (1612-7169)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=7169>

SL7
x86_64
python-tools-2.7.5-48.el7
python-2.7.5-48.el7
tkinter-2.7.5-48.el7
python-test-2.7.5-48.el7
python-devel-2.7.5-48.el7
python-debug-2.7.5-48.el7
python-debuginfo-2.7.5-48.el7
python-libs-2.7.5-48.el7

175057 - Scientific Linux Security ERRATA Important: kernel on SL5.x i386/x86_64 (1612-17134)

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

Risk Level: High

CVE: CVE-2016-7117

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL5.x i386/x86_64 (1612-17134)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=17134>

SL5
i386
kernel-debug-devel-2.6.18-417.el5
kernel-xen-debuginfo-2.6.18-417.el5
kernel-debug-debuginfo-2.6.18-417.el5
kernel-devel-2.6.18-417.el5
kernel-2.6.18-417.el5
kernel-debuginfo-2.6.18-417.el5
kernel-PAE-2.6.18-417.el5
kernel-xen-devel-2.6.18-417.el5
kernel-headers-2.6.18-417.el5
kernel-debuginfo-common-2.6.18-417.el5
kernel-xen-2.6.18-417.el5

kernel-PAE-devel-2.6.18-417.el5
kernel-PAE-debuginfo-2.6.18-417.el5
kernel-debug-2.6.18-417.el5

noarch
kernel-doc-2.6.18-417.el5

x86_64
kernel-xen-debuginfo-2.6.18-417.el5
kernel-debug-debuginfo-2.6.18-417.el5
kernel-debuginfo-common-2.6.18-417.el5
kernel-xen-devel-2.6.18-417.el5
kernel-debug-2.6.18-417.el5
kernel-devel-2.6.18-417.el5
kernel-debug-devel-2.6.18-417.el5
kernel-2.6.18-417.el5
kernel-xen-2.6.18-417.el5
kernel-debuginfo-2.6.18-417.el5
kernel-headers-2.6.18-417.el5

175069 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1612-12735)

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2015-8956, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-3841, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1612-12735)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=12735>

SL7
x86_64
python-perf-debuginfo-3.10.0-514.el7
python-perf-3.10.0-514.el7
kernel-debuginfo-common-x86_64-3.10.0-514.el7
kernel-debug-debuginfo-3.10.0-514.el7
kernel-debug-devel-3.10.0-514.el7
perf-3.10.0-514.el7
kernel-tools-debuginfo-3.10.0-514.el7
kernel-headers-3.10.0-514.el7
kernel-devel-3.10.0-514.el7
kernel-tools-libs-devel-3.10.0-514.el7
kernel-debuginfo-3.10.0-514.el7
kernel-debug-3.10.0-514.el7
perf-debuginfo-3.10.0-514.el7
kernel-tools-3.10.0-514.el7
kernel-tools-libs-3.10.0-514.el7
kernel-3.10.0-514.el7

noarch
kernel-abi-whitelists-3.10.0-514.el7
kernel-doc-3.10.0-514.el7

185524 - Ubuntu Linux 16.04 USN-3161-4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8964, CVE-2016-4568, CVE-2016-6213, CVE-2016-7097, CVE-2016-7425, CVE-2016-8630, CVE-2016-8633, CVE-2016-8645, CVE-2016-8658, CVE-2016-9555, CVE-2016-9644

Description

The scan detected that the host is missing the following update:
USN-3161-4

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-December/003681.html>

Ubuntu 16.04

linux-image-snapdragon_4.4.0.1042.34
linux-image-4.4.0-1042-snapdragon_4.4.0-1042.46

185527 - Ubuntu Linux 16.10 USN-3162-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6213, CVE-2016-7097, CVE-2016-7425, CVE-2016-8630, CVE-2016-8633, CVE-2016-8645, CVE-2016-9313, CVE-2016-9555

Description

The scan detected that the host is missing the following update:
USN-3162-2

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-December/003683.html>

Ubuntu 16.10

linux-image-4.8.0-1021-raspi2_4.8.0-1021.24
linux-image-raspi2_4.8.0.1021.24

185528 - Ubuntu Linux 16.04 USN-3161-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8964, CVE-2016-4568, CVE-2016-6213, CVE-2016-8630, CVE-2016-8633, CVE-2016-8645, CVE-2016-9555

Description

The scan detected that the host is missing the following update:
USN-3161-1

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-December/003678.html>

Ubuntu 16.04

linux-image-generic-lpae_4.4.0.57.60
linux-image-4.4.0-57-generic-lpae_4.4.0-57.78
linux-image-powerpc64-emb_4.4.0.57.60
linux-image-powerpc-smp_4.4.0.57.60
linux-image-powerpc64-smp_4.4.0.57.60
linux-image-4.4.0-57-powerpc-e500mc_4.4.0-57.78
linux-image-4.4.0-57-lowlatency_4.4.0-57.78
linux-image-4.4.0-57-powerpc-smp_4.4.0-57.78
linux-image-4.4.0-57-powerpc64-smp_4.4.0-57.78
linux-image-generic_4.4.0.57.60
linux-image-lowlatency_4.4.0.57.60
linux-image-4.4.0-57-generic_4.4.0-57.78
linux-image-4.4.0-57-powerpc64-emb_4.4.0-57.78
linux-image-powerpc-e500mc_4.4.0.57.60

185530 - Ubuntu Linux 16.10 USN-3162-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6213, CVE-2016-8630, CVE-2016-8633, CVE-2016-8645, CVE-2016-9313, CVE-2016-9555

Description

The scan detected that the host is missing the following update:
USN-3162-1

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-December/003682.html>

Ubuntu 16.10

linux-image-powerpc-smp_4.8.0.32.41
linux-image-generic_4.8.0.32.41
linux-image-4.8.0-32-lowlatency_4.8.0-32.34
linux-image-4.8.0-32-powerpc-e500mc_4.8.0-32.34
linux-image-4.8.0-32-generic-lpae_4.8.0-32.34
linux-image-4.8.0-32-powerpc64-emb_4.8.0-32.34
linux-image-powerpc64-emb_4.8.0.32.41
linux-image-powerpc-e500mc_4.8.0.32.41
linux-image-lowlatency_4.8.0.32.41
linux-image-generic-lpae_4.8.0.32.41
linux-image-4.8.0-32-powerpc-smp_4.8.0-32.34
linux-image-4.8.0-32-generic_4.8.0-32.34

185531 - Ubuntu Linux 14.04 USN-3161-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8964, CVE-2016-4568, CVE-2016-6213, CVE-2016-8630, CVE-2016-8633, CVE-2016-8645, CVE-2016-9555

Description

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

USN-3161-2

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-December/003679.html>

Ubuntu 14.04

linux-image-generic-lpae-lts-xenial_4.4.0.57.44
linux-image-4.4.0-57-powerpc64-emb_4.4.0-57.78~14.04.1
linux-image-4.4.0-57-generic-lpae_4.4.0-57.78~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.57.44
linux-image-4.4.0-57-powerpc64-smp_4.4.0-57.78~14.04.1
linux-image-powerpc-smp-lts-xenial_4.4.0.57.44
linux-image-4.4.0-57-powerpc-smp_4.4.0-57.78~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.57.44
linux-image-generic-lts-xenial_4.4.0.57.44
linux-image-powerpc-e500mc-lts-xenial_4.4.0.57.44
linux-image-powerpc64-emb-lts-xenial_4.4.0.57.44
linux-image-4.4.0-57-powerpc-e500mc_4.4.0-57.78~14.04.1
linux-image-4.4.0-57-generic_4.4.0-57.78~14.04.1
linux-image-4.4.0-57-lowlatency_4.4.0-57.78~14.04.1

185534 - Ubuntu Linux 16.04 USN-3161-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8964, CVE-2016-4568, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-7425, CVE-2016-8630, CVE-2016-8633, CVE-2016-8645, CVE-2016-8658, CVE-2016-9178, CVE-2016-9555

Description

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

USN-3161-3

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-December/003680.html>

Ubuntu 16.04

linux-image-raspi2_4.4.0.1038.37
linux-image-4.4.0-1038-raspi2_4.4.0-1038.45

20951 - Mozilla Thunderbird SVG Animation Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-9079

Description

A use-after-free vulnerability is present in some versions of Mozilla Thunderbird.

Observation

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

A use-after-free vulnerability is present in some versions of Mozilla Thunderbird. The flaw lies in SVG Animation. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

20952 - Mozilla Thunderbird SVG Animation Remote Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-9079

Description

A use-after-free vulnerability is present in some versions of Mozilla Thunderbird.

Observation

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

A use-after-free vulnerability is present in some versions of Mozilla Thunderbird. The flaw lies in SVG Animation. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

21042 - (APSB16-43) Vulnerability In Adobe InDesign

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-7886

Description

A memory corruption vulnerability is present in some versions of Adobe InDesign.

Observation

Adobe InDesign is a page layout application.

A memory corruption vulnerability is present in some versions of Adobe InDesign. The flaw occurs due to a memory issue. Successful exploitation could allow an attacker to execute arbitrary code.

The update provided by Adobe bulletin APSB16-43 resolves the issue. The target system is missing this update.

21048 - (APSB16-43) Vulnerability In Adobe InDesign

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7886

Description

A memory corruption vulnerability is present in some versions of Adobe InDesign.

Observation

Adobe InDesign is a page layout application.

A memory corruption vulnerability is present in some versions of Adobe InDesign. The flaw occurs due to a memory issue. Successful exploitation could allow an attacker to execute arbitrary code.

The update provided by Adobe bulletin APSPB16-43 resolves the issue. The target system is missing this update.

141384 - Red Hat Enterprise Linux RHSA-2016-2946 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
RHSA-2016-2946

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2946.html>

RHEL5S

i386

firefox-debuginfo-45.6.0-1.el5_11

firefox-45.6.0-1.el5_11

x86_64

firefox-debuginfo-45.6.0-1.el5_11

firefox-45.6.0-1.el5_11

RHEL7S

x86_64

firefox-debuginfo-45.6.0-1.el7_3

firefox-45.6.0-1.el7_3

RHEL6S

i386

firefox-debuginfo-45.6.0-1.el6_8

firefox-45.6.0-1.el6_8

x86_64

firefox-debuginfo-45.6.0-1.el6_8

firefox-45.6.0-1.el6_8

RHEL6WS

x86_64

firefox-debuginfo-45.6.0-1.el6_8

firefox-45.6.0-1.el6_8

i386
firefox-debuginfo-45.6.0-1.el6_8
firefox-45.6.0-1.el6_8

RHEL5D
x86_64
firefox-debuginfo-45.6.0-1.el5_11
firefox-45.6.0-1.el5_11

i386
firefox-debuginfo-45.6.0-1.el5_11
firefox-45.6.0-1.el5_11

RHEL7D
x86_64
firefox-debuginfo-45.6.0-1.el7_3
firefox-45.6.0-1.el7_3

RHEL6D
x86_64
firefox-debuginfo-45.6.0-1.el6_8
firefox-45.6.0-1.el6_8

i386
firefox-debuginfo-45.6.0-1.el6_8
firefox-45.6.0-1.el6_8

RHEL7WS
x86_64
firefox-debuginfo-45.6.0-1.el7_3
firefox-45.6.0-1.el7_3

145096 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3161-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8964, CVE-2015-2325, CVE-2015-2327, CVE-2015-2328, CVE-2015-3210, CVE-2015-3217, CVE-2015-5073, CVE-2015-8380, CVE-2015-8381, CVE-2015-8382, CVE-2015-8383, CVE-2015-8384, CVE-2015-8385, CVE-2015-8386, CVE-2015-8387, CVE-2015-8388, CVE-2015-8389, CVE-2015-8390, CVE-2015-8391, CVE-2015-8392, CVE-2015-8393, CVE-2015-8394, CVE-2015-8395, CVE-2016-1283, CVE-2016-3191

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3161-1

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-December/002488.html>

SuSE SLED 12 SP2
x86_64
libpcrecpp0-debuginfo-32bit-8.39-7.1
libpcrecpp0-8.39-7.1
libpcrecpp0-32bit-8.39-7.1
libpcrecpp0-debuginfo-8.39-7.1

libpcre16-0-debuginfo-8.39-7.1
pcre-debugsource-8.39-7.1
libpcre1-debuginfo-32bit-8.39-7.1
libpcre1-8.39-7.1
libpcre16-0-8.39-7.1
libpcre1-32bit-8.39-7.1
libpcre1-debuginfo-8.39-7.1

SuSE SLES 12 SP2

x86_64
libpcre1-8.39-7.1
libpcre1-32bit-8.39-7.1
libpcre16-0-debuginfo-8.39-7.1
pcre-debugsource-8.39-7.1
libpcre1-debuginfo-32bit-8.39-7.1
libpcre16-0-8.39-7.1
libpcre1-debuginfo-8.39-7.1

SuSE SLES 12 SP1

x86_64
libpcre1-8.39-7.1
libpcre1-32bit-8.39-7.1
libpcre16-0-debuginfo-8.39-7.1
pcre-debugsource-8.39-7.1
libpcre1-debuginfo-32bit-8.39-7.1
libpcre16-0-8.39-7.1
libpcre1-debuginfo-8.39-7.1

SuSE SLED 12 SP1

x86_64
libpcrecpp0-debuginfo-32bit-8.39-7.1
libpcrecpp0-8.39-7.1
libpcrecpp0-32bit-8.39-7.1
libpcrecpp0-debuginfo-8.39-7.1
libpcre16-0-debuginfo-8.39-7.1
pcre-debugsource-8.39-7.1
libpcre1-debuginfo-32bit-8.39-7.1
libpcre1-8.39-7.1
libpcre16-0-8.39-7.1
libpcre1-32bit-8.39-7.1
libpcre1-debuginfo-8.39-7.1

160181 - CentOS 5, 6, 7 CESA-2016-2946 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
CESA-2016-2946

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-December/022180.html>

<http://lists.centos.org/pipermail/centos-announce/2016-December/022179.html>
<http://lists.centos.org/pipermail/centos-announce/2016-December/022178.html>

CentOS 6
x86_64
firefox-45.6.0-1.el6.centos

i686
firefox-45.6.0-1.el6.centos

CentOS 7
x86_64
firefox-45.6.0-1.el7.centos

i686
firefox-45.6.0-1.el7.centos

CentOS 5
x86_64
firefox-45.6.0-1.el5.centos

i386
firefox-45.6.0-1.el5.centos

163239 - Oracle Enterprise Linux ELSA-2016-2946 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
ELSA-2016-2946

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006585.html>
<http://oss.oracle.com/pipermail/el-errata/2016-December/006586.html>
<http://oss.oracle.com/pipermail/el-errata/2016-December/006584.html>

OEL6
x86_64
firefox-45.6.0-1.0.1.el6_8

i386
firefox-45.6.0-1.0.1.el6_8

OEL5
x86_64
firefox-45.6.0-1.0.1.el5_11

i386
firefox-45.6.0-1.0.1.el5_11

OEL7

x86_64
firefox-45.6.0-1.0.1.el7_3

170752 - Amazon Linux AMI ALAS-2016-774 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2834, CVE-2016-5285, CVE-2016-8635

Description

The scan detected that the host is missing the following update:
ALAS-2016-774

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-774.html>

Amazon Linux AMI

x86_64
nss-softokn-debuginfo-3.16.2.3-14.4.39.amzn1
nss-util-3.21.3-1.1.51.amzn1
nss-util-devel-3.21.3-1.1.51.amzn1
nss-softokn-3.16.2.3-14.4.39.amzn1
nss-util-debuginfo-3.21.3-1.1.51.amzn1
nss-softokn-freebl-devel-3.16.2.3-14.4.39.amzn1
nss-softokn-devel-3.16.2.3-14.4.39.amzn1
nss-pkcs11-devel-3.21.3-2.77.amzn1
nss-softokn-freebl-3.16.2.3-14.4.39.amzn1
nss-devel-3.21.3-2.77.amzn1
nss-3.21.3-2.77.amzn1
nss-tools-3.21.3-2.77.amzn1
nss-sysinit-3.21.3-2.77.amzn1
nss-debuginfo-3.21.3-2.77.amzn1

i686
nss-softokn-debuginfo-3.16.2.3-14.4.39.amzn1
nss-pkcs11-devel-3.21.3-2.77.amzn1
nss-util-3.21.3-1.1.51.amzn1
nss-util-devel-3.21.3-1.1.51.amzn1
nss-softokn-3.16.2.3-14.4.39.amzn1
nss-util-debuginfo-3.21.3-1.1.51.amzn1
nss-softokn-freebl-devel-3.16.2.3-14.4.39.amzn1
nss-softokn-devel-3.16.2.3-14.4.39.amzn1
nss-3.21.3-2.77.amzn1
nss-softokn-freebl-3.16.2.3-14.4.39.amzn1
nss-devel-3.21.3-2.77.amzn1
nss-tools-3.21.3-2.77.amzn1
nss-sysinit-3.21.3-2.77.amzn1
nss-debuginfo-3.21.3-2.77.amzn1

175058 - Scientific Linux Security ERRATA Moderate: poppler on SL7.x x86_64 (1612-10803)

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

Risk Level: High

CVE: CVE-2015-8868

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: poppler on SL7.x x86_64 (1612-10803)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=10803>

SL7
x86_64
poppler-qt-devel-0.26.5-16.el7
poppler-cpp-0.26.5-16.el7
poppler-0.26.5-16.el7
poppler-devel-0.26.5-16.el7
poppler-cpp-devel-0.26.5-16.el7
poppler-glib-devel-0.26.5-16.el7
poppler-demos-0.26.5-16.el7
poppler-qt-0.26.5-16.el7
poppler-utils-0.26.5-16.el7
poppler-debuginfo-0.26.5-16.el7
poppler-glib-0.26.5-16.el7

175059 - Scientific Linux Security ERRATA Moderate: libreoffice on SL7.x x86_64 (1612-7832)

Category: SSH Module -> NonIntrusive -> Scientific Linux 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:
Security ERRATA Moderate: libreoffice on SL7.x x86_64 (1612-7832)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=7832>

SL7
x86_64
libreoffice-langpack-ta-5.0.6.2-3.el7
libreoffice-xsltfilter-5.0.6.2-3.el7
libreoffice-langpack-th-5.0.6.2-3.el7
libcmis-devel-0.5.1-2.el7
libreoffice-langpack-de-5.0.6.2-3.el7
libreoffice-langpack-mai-5.0.6.2-3.el7
libreoffice-langpack-ts-5.0.6.2-3.el7
libreoffice-langpack-fi-5.0.6.2-3.el7
libreoffice-langpack-pl-5.0.6.2-3.el7
libpagemaker-tools-0.0.3-1.el7
libreoffice-rhino-5.0.6.2-3.el7
libreoffice-langpack-sl-5.0.6.2-3.el7
libreoffice-langpack-si-5.0.6.2-3.el7
libreoffice-gdb-debug-support-5.0.6.2-3.el7

libreoffice-langpack-sr-5.0.6.2-3.el7
libreoffice-langpack-ve-5.0.6.2-3.el7
libreoffice-langpack-zh-Hans-5.0.6.2-3.el7
libreoffice-calc-5.0.6.2-3.el7
libreoffice-emailmerge-5.0.6.2-3.el7
libreoffice-langpack-gu-5.0.6.2-3.el7
libreoffice-langpack-tr-5.0.6.2-3.el7
libreoffice-langpack-ar-5.0.6.2-3.el7
libreoffice-langpack-nb-5.0.6.2-3.el7
libreoffice-filters-5.0.6.2-3.el7
libreoffice-debuginfo-5.0.6.2-3.el7
libreoffice-langpack-kn-5.0.6.2-3.el7
libreoffice-langpack-kk-5.0.6.2-3.el7
libreoffice-langpack-nn-5.0.6.2-3.el7
libreoffice-langpack-lt-5.0.6.2-3.el7
libreoffice-writer-5.0.6.2-3.el7
libreoffice-langpack-en-5.0.6.2-3.el7
libreoffice-langpack-nl-5.0.6.2-3.el7
libreoffice-officebean-5.0.6.2-3.el7
libreoffice-langpack-nr-5.0.6.2-3.el7
libreoffice-langpack-el-5.0.6.2-3.el7
libreoffice-langpack-it-5.0.6.2-3.el7
libreoffice-langpack-ro-5.0.6.2-3.el7
libreoffice-langpack-ca-5.0.6.2-3.el7
libreoffice-langpack-he-5.0.6.2-3.el7
libreoffice-langpack-fa-5.0.6.2-3.el7
libreoffice-langpack-pt-PT-5.0.6.2-3.el7
libreoffice-langpack-te-5.0.6.2-3.el7
libreoffice-langpack-bn-5.0.6.2-3.el7
libreoffice-langpack-dz-5.0.6.2-3.el7
libreoffice-langpack-cs-5.0.6.2-3.el7
libpagemaker-debuginfo-0.0.3-1.el7
libreoffice-bsh-5.0.6.2-3.el7
libreoffice-sdk-5.0.6.2-3.el7
libreoffice-langpack-or-5.0.6.2-3.el7
libreoffice-pdfimport-5.0.6.2-3.el7
libreoffice-langpack-br-5.0.6.2-3.el7
libreoffice-graphicsfilter-5.0.6.2-3.el7
libreoffice-langpack-af-5.0.6.2-3.el7
libreoffice-langpack-hi-5.0.6.2-3.el7
libreoffice-langpack-ga-5.0.6.2-3.el7
libreoffice-langpack-hr-5.0.6.2-3.el7
libreoffice-postgresql-5.0.6.2-3.el7
libreoffice-math-5.0.6.2-3.el7
libreoffice-core-5.0.6.2-3.el7
libpagemaker-devel-0.0.3-1.el7
libreoffice-pyuno-5.0.6.2-3.el7
libreoffice-langpack-bg-5.0.6.2-3.el7
libreoffice-langpack-es-5.0.6.2-3.el7
libreoffice-langpack-sk-5.0.6.2-3.el7
libreoffice-impress-5.0.6.2-3.el7
libreoffice-langpack-ru-5.0.6.2-3.el7
libreoffice-langpack-eu-5.0.6.2-3.el7
libreoffice-langpack-pt-BR-5.0.6.2-3.el7
libreoffice-langpack-uk-5.0.6.2-3.el7
libreoffice-ogltrans-5.0.6.2-3.el7
libreoffice-ure-5.0.6.2-3.el7
libreoffice-langpack-zh-Hant-5.0.6.2-3.el7
libreoffice-nlpsolver-5.0.6.2-3.el7
libreoffice-wiki-publisher-5.0.6.2-3.el7

libreoffice-langpack-xh-5.0.6.2-3.el7
libreoffice-langpack-da-5.0.6.2-3.el7
libreoffice-base-5.0.6.2-3.el7
libreoffice-langpack-ja-5.0.6.2-3.el7
libpagemaker-0.0.3-1.el7
libreoffice-librelogo-5.0.6.2-3.el7
libreoffice-langpack-hu-5.0.6.2-3.el7
libreoffice-langpack-zu-5.0.6.2-3.el7
libreoffice-langpack-ss-5.0.6.2-3.el7
libreoffice-draw-5.0.6.2-3.el7
libreoffice-langpack-st-5.0.6.2-3.el7
libreoffice-langpack-as-5.0.6.2-3.el7
libreoffice-langpack-ml-5.0.6.2-3.el7
libreoffice-langpack-fr-5.0.6.2-3.el7
libreoffice-langpack-mr-5.0.6.2-3.el7
libreoffice-langpack-ko-5.0.6.2-3.el7
libcmis-tools-0.5.1-2.el7
libcmis-debuginfo-0.5.1-2.el7
libreoffice-langpack-pa-5.0.6.2-3.el7
libcmis-0.5.1-2.el7
libreoffice-langpack-cy-5.0.6.2-3.el7
libreoffice-glade-5.0.6.2-3.el7
libreoffice-langpack-gl-5.0.6.2-3.el7
libreoffice-langpack-tn-5.0.6.2-3.el7
libreoffice-langpack-nso-5.0.6.2-3.el7
libreoffice-5.0.6.2-3.el7
libreoffice-langpack-et-5.0.6.2-3.el7
libreoffice-langpack-sv-5.0.6.2-3.el7
libreoffice-sdk-doc-5.0.6.2-3.el7
libreoffice-langpack-lv-5.0.6.2-3.el7

noarch

autocorr-ca-5.0.6.2-3.el7
autocorr-da-5.0.6.2-3.el7
autocorr-en-5.0.6.2-3.el7
autocorr-de-5.0.6.2-3.el7
autocorr-ro-5.0.6.2-3.el7
autocorr-ja-5.0.6.2-3.el7
autocorr-is-5.0.6.2-3.el7
autocorr-af-5.0.6.2-3.el7
autocorr-ru-5.0.6.2-3.el7
autocorr-zh-5.0.6.2-3.el7
autocorr-hu-5.0.6.2-3.el7
autocorr-sl-5.0.6.2-3.el7
mdds-devel-0.12.1-1.el7
autocorr-sk-5.0.6.2-3.el7
libreoffice-opensymbol-fonts-5.0.6.2-3.el7
autocorr-lb-5.0.6.2-3.el7
autocorr-sr-5.0.6.2-3.el7
autocorr-fa-5.0.6.2-3.el7
autocorr-pl-5.0.6.2-3.el7
autocorr-cs-5.0.6.2-3.el7
autocorr-fr-5.0.6.2-3.el7
autocorr-es-5.0.6.2-3.el7
libpagemaker-doc-0.0.3-1.el7
autocorr-fi-5.0.6.2-3.el7
autocorr-pt-5.0.6.2-3.el7
autocorr-sv-5.0.6.2-3.el7
autocorr-ga-5.0.6.2-3.el7
autocorr-mn-5.0.6.2-3.el7

autocorr-bg-5.0.6.2-3.el7
autocorr-ko-5.0.6.2-3.el7
autocorr-vi-5.0.6.2-3.el7
autocorr-It-5.0.6.2-3.el7
autocorr-tr-5.0.6.2-3.el7
autocorr-nl-5.0.6.2-3.el7
autocorr-it-5.0.6.2-3.el7
autocorr-hr-5.0.6.2-3.el7

175063 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-16640)

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

Description

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

Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-16640)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=16640>

SL5

x86_64

firefox-debuginfo-45.6.0-1.el5_11

firefox-45.6.0-1.el5_11

i386

firefox-debuginfo-45.6.0-1.el5_11

firefox-45.6.0-1.el5_11

SL7

x86_64

firefox-debuginfo-45.6.0-1.el7_3

firefox-45.6.0-1.el7_3

SL6

x86_64

firefox-debuginfo-45.6.0-1.el6_8

firefox-45.6.0-1.el6_8

i386

firefox-debuginfo-45.6.0-1.el6_8

firefox-45.6.0-1.el6_8

175066 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-15603)

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

Risk Level: High

CVE: CVE-2016-9079

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-15603)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=15603>

SL5
x86_64
firefox-45.5.1-1.el5_11
firefox-debuginfo-45.5.1-1.el5_11

i386
firefox-45.5.1-1.el5_11
firefox-debuginfo-45.5.1-1.el5_11

SL7
x86_64
firefox-45.5.1-1.el7_3
firefox-debuginfo-45.5.1-1.el7_3

SL6
x86_64
firefox-45.5.1-1.el6_8
firefox-debuginfo-45.5.1-1.el6_8

i386
firefox-45.5.1-1.el6_8
firefox-debuginfo-45.5.1-1.el6_8

185529 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3157-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9949, CVE-2016-9950, CVE-2016-9951

Description

The scan detected that the host is missing the following update:
USN-3157-1

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-December/003671.html>

Ubuntu 12.04

python-apport_2.0.1-0ubuntu17.15
apport-kde_2.0.1-0ubuntu17.15
apport-gtk_2.0.1-0ubuntu17.15
apport_2.0.1-0ubuntu17.15

Ubuntu 16.04

apport_2.20.1-0ubuntu2.4
python3-apport_2.20.1-0ubuntu2.4
python-apport_2.20.1-0ubuntu2.4
apport-gtk_2.20.1-0ubuntu2.4
apport-kde_2.20.1-0ubuntu2.4

Ubuntu 14.04

apport_2.14.1-0ubuntu3.23
python3-apport_2.14.1-0ubuntu3.23
apport-gtk_2.14.1-0ubuntu3.23
python-apport_2.14.1-0ubuntu3.23
apport-kde_2.14.1-0ubuntu3.23

Ubuntu 16.10

apport_2.20.3-0ubuntu8.2
python3-apport_2.20.3-0ubuntu8.2
apport-gtk_2.20.3-0ubuntu8.2
apport-kde_2.20.3-0ubuntu8.2
python-apport_2.20.3-0ubuntu8.2

21029 - (SB10175) McAfee Application Control Privilege Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2016-8009

Description

A privilege escalation vulnerability exists in some versions of McAfee Application Control.

Observation

McAfee Application Control is a security manager software that prevents execution of unwanted programs.

A privilege escalation vulnerability exists in some versions of McAfee Application Control. The affected software allows an unauthorized use of the Input/Output Control (IOCTL) system call. Successful exploitation of this vulnerability could allow a malicious user to escalate privileges, cause a denial-of-service condition, produce unexpected behavior in the system, or potentially execute unauthorized code.

21030 - Cisco AnyConnect Secure Mobility Client Local Privilege Escalation Vulnerability I

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

Risk Level: High

CVE: CVE-2016-9192

Description

A privilege escalation vulnerability is present in some versions of Cisco AnyConnect Secure Mobility Client.

Observation

Cisco AnyConnect Secure Mobility Client is a VPN client.

A privilege escalation vulnerability is present in some versions of Cisco AnyConnect Secure Mobility Client. The flaw is due to incorrect permissions on a system directory at installation. Successful exploitation could allow a local attacker to execute commands with elevated privilege.

21044 - Joomla Shell Upload Vulnerability (20161202)

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

Risk Level: High

CVE: CVE-2016-9836

Description

An improper access control vulnerability exists in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

An improper access control vulnerability exists in some versions of Joomla! CMS. The flaw lies in the file scanning mechanism, which allows the upload and execution of PHP files that use alternate file extensions (.php6, .php7, .phtml and .phpt). Successful exploitation of this vulnerability could allow a malicious user to affect integrity, confidentiality or availability of the system.

132315 - Oracle VM OVMSA-2016-0176 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0176

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000603.html>

OVM3.4
x86_64
xen-4.4.4-105.0.4.el6
xen-tools-4.4.4-105.0.4.el6

132316 - Oracle VM OVMSA-2016-0177 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0177

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000604.html>

OVM3.3
x86_64
xen-tools-4.3.0-55.el6.119.63
xen-4.3.0-55.el6.119.63

132317 - Oracle VM OVMSA-2016-0178 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0178

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000605.html>

OVM3.2
x86_64
xen-devel-4.1.3-25.el5.223.46
xen-tools-4.1.3-25.el5.223.46
xen-4.1.3-25.el5.223.46

141382 - Red Hat Enterprise Linux RHSA-2016-2963 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9637

Description

The scan detected that the host is missing the following update:
RHSA-2016-2963

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2963.html>

RHEL5D
x86_64
xen-libs-3.0.3-148.el5_11
xen-debuginfo-3.0.3-148.el5_11

i386
xen-libs-3.0.3-148.el5_11
xen-debuginfo-3.0.3-148.el5_11

RHEL5S
i386
xen-libs-3.0.3-148.el5_11
xen-debuginfo-3.0.3-148.el5_11

x86_64
xen-libs-3.0.3-148.el5_11
xen-debuginfo-3.0.3-148.el5_11

145087 - SuSE SLES 11 SP4 SUSE-SU-2016:3193-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5219, CVE-2015-8139, CVE-2015-8140, CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3193-1

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-December/002496.html>

SuSE SLES 11 SP4
i586
ntp-doc-4.2.8p9-57.2
ntp-4.2.8p9-57.2

x86_64
ntp-doc-4.2.8p9-57.2
ntp-4.2.8p9-57.2

145088 - SuSE Linux 13.2 openSUSE-SU-2016:3177-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9427

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3177-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00115.html>

SuSE Linux 13.2
x86_64
libgc1-debuginfo-7.2d-4.3.1
gc-devel-7.2d-4.3.1
gc-debugsource-7.2d-4.3.1
libgc1-7.2d-4.3.1

i586
libgc1-debuginfo-7.2d-4.3.1

gc-devel-7.2d-4.3.1
gc-debugsource-7.2d-4.3.1
libgc1-7.2d-4.3.1

145089 - SuSE Linux 13.2 openSUSE-SU-2016:3179-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8649

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3179-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00117.html>

SuSE Linux 13.2
x86_64
lxc-devel-1.0.6-12.1
lxc-debuginfo-1.0.6-12.1
lxc-debugsource-1.0.6-12.1
lxc-1.0.6-12.1

i586
lxc-devel-1.0.6-12.1
lxc-debuginfo-1.0.6-12.1
lxc-debugsource-1.0.6-12.1
lxc-1.0.6-12.1

145090 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3195-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5219, CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3195-1

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-December/002497.html>

SuSE SLED 12 SP1
x86_64
ntp-debuginfo-4.2.8p9-55.1
ntp-debugsource-4.2.8p9-55.1
ntp-4.2.8p9-55.1
ntp-doc-4.2.8p9-55.1

SuSE SLES 12 SP2
x86_64
ntp-debuginfo-4.2.8p9-55.1
ntp-debugsource-4.2.8p9-55.1
ntp-4.2.8p9-55.1
ntp-doc-4.2.8p9-55.1

SuSE SLED 12 SP2
x86_64
ntp-debuginfo-4.2.8p9-55.1
ntp-debugsource-4.2.8p9-55.1
ntp-4.2.8p9-55.1
ntp-doc-4.2.8p9-55.1

SuSE SLES 12 SP1
x86_64
ntp-debuginfo-4.2.8p9-55.1
ntp-debugsource-4.2.8p9-55.1
ntp-4.2.8p9-55.1
ntp-doc-4.2.8p9-55.1

145091 - SuSE SLES 11 SP4 SUSE-SU-2016:3162-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7035, CVE-2016-7797

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3162-1

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-December/002489.html>

SuSE SLES 11 SP4
i586
libpacemaker-devel-1.1.12-18.1
pacemaker-1.1.12-18.1
pacemaker-remote-1.1.12-18.1
libpacemaker3-1.1.12-18.1
pacemaker-cli-1.1.12-18.1

x86_64
libpacemaker-devel-1.1.12-18.1
pacemaker-1.1.12-18.1
pacemaker-remote-1.1.12-18.1
libpacemaker3-1.1.12-18.1
pacemaker-cli-1.1.12-18.1

145092 - SuSE Linux 13.2 openSUSE-SU-2016:3184-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9080, CVE-2016-9893, CVE-2016-9894, CVE-2016-9895, CVE-2016-9896, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9903, CVE-2016-9904

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3184-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00121.html>

SuSE Linux 13.2

x86_64

MozillaFirefox-debuginfo-50.1.0-94.1

MozillaFirefox-translations-common-50.1.0-94.1

MozillaFirefox-translations-other-50.1.0-94.1

MozillaFirefox-debugsource-50.1.0-94.1

MozillaFirefox-devel-50.1.0-94.1

MozillaFirefox-50.1.0-94.1

MozillaFirefox-branding-upstream-50.1.0-94.1

MozillaFirefox-buildsymbols-50.1.0-94.1

i586

MozillaFirefox-debuginfo-50.1.0-94.1

MozillaFirefox-translations-common-50.1.0-94.1

MozillaFirefox-translations-other-50.1.0-94.1

MozillaFirefox-debugsource-50.1.0-94.1

MozillaFirefox-devel-50.1.0-94.1

MozillaFirefox-50.1.0-94.1

MozillaFirefox-branding-upstream-50.1.0-94.1

MozillaFirefox-buildsymbols-50.1.0-94.1

145093 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:3146-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9576, CVE-2016-9794

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3146-1

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-December/002485.html>

SuSE SLED 12 SP2

x86_64

kernel-default-debugsource-4.4.21-90.1

kernel-syms-4.4.21-90.1

kernel-default-4.4.21-90.1

kernel-default-devel-4.4.21-90.1

kernel-default-debuginfo-4.4.21-90.1

kernel-default-extra-debuginfo-4.4.21-90.1
kernel-default-extra-4.4.21-90.1

noarch
kernel-source-4.4.21-90.1
kernel-macros-4.4.21-90.1
kernel-devel-4.4.21-90.1

SuSE SLES 12 SP2
noarch
kernel-source-4.4.21-90.1
kernel-macros-4.4.21-90.1
kernel-devel-4.4.21-90.1

x86_64
kernel-default-4.4.21-90.1
kernel-syms-4.4.21-90.1
kernel-default-base-debuginfo-4.4.21-90.1
kernel-default-base-4.4.21-90.1
kernel-default-devel-4.4.21-90.1
kernel-default-debuginfo-4.4.21-90.1
kernel-default-debugsource-4.4.21-90.1

145094 - SuSE Linux 13.2 openSUSE-SU-2016:3147-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9445, CVE-2016-9446

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3147-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00109.html>

SuSE Linux 13.2

i586
libgstsignalprocessor-0_10-23-debuginfo-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-debuginfo-0.10.23-15.3.1
libgstvdp-0_10-23-0.10.23-15.3.1
libgstbasecamerabinsrc-0_10-23-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-debugsource-0.10.23-15.3.1
libgstsignalprocessor-0_10-23-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-0.10.23-15.3.1
libgstphotography-0_10-23-debuginfo-0.10.23-15.3.1
libgstvdp-0_10-23-debuginfo-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-doc-0.10.23-15.3.1
libgstcodecparsers-0_10-23-debuginfo-0.10.23-15.3.1
libgstphotography-0_10-23-0.10.23-15.3.1
libgstbasecamerabinsrc-0_10-23-debuginfo-0.10.23-15.3.1
libgstcodecparsers-0_10-23-0.10.23-15.3.1
libgstbasevideo-0_10-23-0.10.23-15.3.1
libgstbasevideo-0_10-23-debuginfo-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-devel-0.10.23-15.3.1

noarch
gstreamer-0_10-plugins-bad-lang-0.10.23-15.3.1

x86_64
libgstphotography-0_10-23-debuginfo-32bit-0.10.23-15.3.1
libgstvdp-0_10-23-32bit-0.10.23-15.3.1
libgstcodecparsers-0_10-23-debuginfo-32bit-0.10.23-15.3.1
libgstsignalprocessor-0_10-23-debuginfo-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-debuginfo-32bit-0.10.23-15.3.1
libgstsignalprocessor-0_10-23-debuginfo-32bit-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-32bit-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-debugsource-0.10.23-15.3.1
libgstcodecparsers-0_10-23-32bit-0.10.23-15.3.1
libgstsignalprocessor-0_10-23-0.10.23-15.3.1
libgstbasecamerabinsrc-0_10-23-32bit-0.10.23-15.3.1
libgstbasevideo-0_10-23-32bit-0.10.23-15.3.1
libgstbasevideo-0_10-23-debuginfo-0.10.23-15.3.1
libgstbasevideo-0_10-23-debuginfo-32bit-0.10.23-15.3.1
libgstvdp-0_10-23-debuginfo-0.10.23-15.3.1
libgstphotography-0_10-23-32bit-0.10.23-15.3.1
libgstcodecparsers-0_10-23-debuginfo-0.10.23-15.3.1
libgstvdp-0_10-23-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-devel-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-debuginfo-0.10.23-15.3.1
libgstbasecamerabinsrc-0_10-23-debuginfo-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-doc-0.10.23-15.3.1
libgstsignalprocessor-0_10-23-32bit-0.10.23-15.3.1
libgstphotography-0_10-23-debuginfo-0.10.23-15.3.1
libgstphotography-0_10-23-0.10.23-15.3.1
gstreamer-0_10-plugins-bad-0.10.23-15.3.1
libgstbasecamerabinsrc-0_10-23-0.10.23-15.3.1
libgstbasecamerabinsrc-0_10-23-debuginfo-32bit-0.10.23-15.3.1
libgstvdp-0_10-23-debuginfo-32bit-0.10.23-15.3.1
libgstbasevideo-0_10-23-0.10.23-15.3.1
libgstcodecparsers-0_10-23-0.10.23-15.3.1

145095 - SuSE Linux 13.2 openSUSE-SU-2016:3202-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3202-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00127.html>

SuSE Linux 13.2

x86_64

libz1-debuginfo-1.2.8-5.8.1

zlib-devel-static-32bit-1.2.8-5.8.1

libz1-debuginfo-32bit-1.2.8-5.8.1

libminizip1-debuginfo-1.2.8-5.8.1

libz1-32bit-1.2.8-5.8.1
zlib-devel-static-1.2.8-5.8.1
zlib-debugsource-1.2.8-5.8.1
libminizip1-1.2.8-5.8.1
zlib-devel-32bit-1.2.8-5.8.1
libz1-1.2.8-5.8.1
minizip-devel-1.2.8-5.8.1
zlib-devel-1.2.8-5.8.1

i586
libz1-debuginfo-1.2.8-5.8.1
libminizip1-debuginfo-1.2.8-5.8.1
zlib-devel-static-1.2.8-5.8.1
zlib-debugsource-1.2.8-5.8.1
libminizip1-1.2.8-5.8.1
libz1-1.2.8-5.8.1
minizip-devel-1.2.8-5.8.1
zlib-devel-1.2.8-5.8.1

145097 - SuSE SLES 11 SP4 SUSE-SU-2016:3172-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7944

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3172-1

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-December/002491.html>

SuSE SLES 11 SP4
i586
xorg-x11-libXfixes-7.4-1.20.1

x86_64
xorg-x11-libXfixes-32bit-7.4-1.20.1
xorg-x11-libXfixes-7.4-1.20.1

145098 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:3188-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9576, CVE-2016-9794

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3188-1

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-December/002494.html>

SuSE SLES 12 SP1

noarch
kernel-source-3.12.67-60.64.24.1
kernel-devel-3.12.67-60.64.24.1
kernel-macros-3.12.67-60.64.24.1

x86_64

kernel-default-debugsource-3.12.67-60.64.24.1
kernel-default-3.12.67-60.64.24.1
kernel-default-devel-3.12.67-60.64.24.1
kernel-default-base-3.12.67-60.64.24.1
kernel-xen-debuginfo-3.12.67-60.64.24.1
kernel-default-base-debuginfo-3.12.67-60.64.24.1
kernel-default-debuginfo-3.12.67-60.64.24.1
kernel-xen-debugsource-3.12.67-60.64.24.1
kernel-xen-base-3.12.67-60.64.24.1
kernel-xen-devel-3.12.67-60.64.24.1
kernel-xen-base-debuginfo-3.12.67-60.64.24.1
kernel-xen-3.12.67-60.64.24.1
kernel-syms-3.12.67-60.64.24.1

SuSE SLED 12 SP1

x86_64
kernel-default-extra-3.12.67-60.64.24.1
kernel-xen-devel-3.12.67-60.64.24.1
kernel-syms-3.12.67-60.64.24.1
kernel-default-3.12.67-60.64.24.1
kernel-default-extra-debuginfo-3.12.67-60.64.24.1
kernel-default-debuginfo-3.12.67-60.64.24.1
kernel-default-debugsource-3.12.67-60.64.24.1
kernel-xen-3.12.67-60.64.24.1
kernel-xen-debuginfo-3.12.67-60.64.24.1
kernel-xen-debugsource-3.12.67-60.64.24.1
kernel-default-devel-3.12.67-60.64.24.1

noarch

kernel-source-3.12.67-60.64.24.1
kernel-devel-3.12.67-60.64.24.1
kernel-macros-3.12.67-60.64.24.1

145099 - SuSE SLES 11 SP4 SUSE-SU-2016:3189-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7945, CVE-2016-7946, CVE-2016-7947, CVE-2016-7948, CVE-2016-7951, CVE-2016-7952, CVE-2016-7953

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3189-1

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-December/002495.html>

SuSE SLES 11 SP4
i586
xorg-x11-libs-7.4-8.26.49.1

x86_64
xorg-x11-libs-32bit-7.4-8.26.49.1
xorg-x11-libs-7.4-8.26.49.1

145100 - SuSE Linux 13.2 openSUSE-SU-2016:3158-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9445, CVE-2016-9446

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3158-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00111.html>

SuSE Linux 13.2
i586
libgstphotography-1_0-0-1.4.3-3.1
libgstbadvideo-1_0-0-debuginfo-1.4.3-3.1
libgstgl-1_0-0-1.4.3-3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-1.4.3-3.1
libgstphotography-1_0-0-debuginfo-1.4.3-3.1
libgstinsertbin-1_0-0-debuginfo-1.4.3-3.1
libgstmpegts-1_0-0-debuginfo-1.4.3-3.1
gstreamer-plugins-bad-debuginfo-1.4.3-3.1
libgstbadvideo-1_0-0-1.4.3-3.1
libgstbadbase-1_0-0-debuginfo-1.4.3-3.1
libgstbasecamerabinsrc-1_0-0-1.4.3-3.1
libgsturidownloader-1_0-0-debuginfo-1.4.3-3.1
libgsturidownloader-1_0-0-1.4.3-3.1
gstreamer-plugins-bad-doc-1.4.3-3.1
libgstcodecparsers-1_0-0-debuginfo-1.4.3-3.1
libgstmpegts-1_0-0-1.4.3-3.1
gstreamer-plugins-bad-devel-1.4.3-3.1
libgstcodecparsers-1_0-0-1.4.3-3.1
gstreamer-plugins-bad-debugsource-1.4.3-3.1
libgstgl-1_0-0-debuginfo-1.4.3-3.1
gstreamer-plugins-bad-1.4.3-3.1
libgstinsertbin-1_0-0-1.4.3-3.1
libgstbadbase-1_0-0-1.4.3-3.1

noarch
gstreamer-plugins-bad-lang-1.4.3-3.1

x86_64
libgstbadbase-1_0-0-debuginfo-1.4.3-3.1
libgstphotography-1_0-0-1.4.3-3.1
gstreamer-plugins-bad-devel-1.4.3-3.1
libgsturidownloader-1_0-0-debuginfo-1.4.3-3.1

libgstgl-1_0-0-32bit-1.4.3-3.1
libgstbadbase-1_0-0-1.4.3-3.1
libgstinsertbin-1_0-0-debuginfo-32bit-1.4.3-3.1
libgstgl-1_0-0-debuginfo-1.4.3-3.1
libgsturidownloader-1_0-0-1.4.3-3.1
libgstphotography-1_0-0-debuginfo-32bit-1.4.3-3.1
libgstgl-1_0-0-1.4.3-3.1
libgstbadvideo-1_0-0-32bit-1.4.3-3.1
libgstbasecamerabinsrc-1_0-0-32bit-1.4.3-3.1
libgsturidownloader-1_0-0-32bit-1.4.3-3.1
libgstinsertbin-1_0-0-debuginfo-1.4.3-3.1
libgstbadvideo-1_0-0-debuginfo-1.4.3-3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-32bit-1.4.3-3.1
gstreamer-plugins-bad-debugsource-1.4.3-3.1
libgstcodecparsers-1_0-0-1.4.3-3.1
libgstcodecparsers-1_0-0-debuginfo-1.4.3-3.1
libgstinsertbin-1_0-0-32bit-1.4.3-3.1
libgstbasecamerabinsrc-1_0-0-1.4.3-3.1
libgstphotography-1_0-0-32bit-1.4.3-3.1
libgstmpegts-1_0-0-debuginfo-32bit-1.4.3-3.1
libgstmpegts-1_0-0-32bit-1.4.3-3.1
libgstmpegts-1_0-0-1.4.3-3.1
libgstbadvideo-1_0-0-1.4.3-3.1
libgstgl-1_0-0-debuginfo-32bit-1.4.3-3.1
libgstcodecparsers-1_0-0-32bit-1.4.3-3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-1.4.3-3.1
gstreamer-plugins-bad-doc-1.4.3-3.1
libgstmpegts-1_0-0-debuginfo-1.4.3-3.1
libgstbadvideo-1_0-0-debuginfo-32bit-1.4.3-3.1
libgstbadbase-1_0-0-32bit-1.4.3-3.1
libgstbadbase-1_0-0-debuginfo-32bit-1.4.3-3.1
gstreamer-plugins-bad-debuginfo-32bit-1.4.3-3.1
gstreamer-plugins-bad-debuginfo-1.4.3-3.1
libgstcodecparsers-1_0-0-debuginfo-32bit-1.4.3-3.1
gstreamer-plugins-bad-32bit-1.4.3-3.1
libgstphotography-1_0-0-debuginfo-1.4.3-3.1
libgsturidownloader-1_0-0-debuginfo-32bit-1.4.3-3.1
libgstinsertbin-1_0-0-1.4.3-3.1
gstreamer-plugins-bad-1.4.3-3.1

145102 - SuSE SLES 11 SP4 SUSE-SU-2016:3203-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9576, CVE-2016-9794

Description

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

SUSE-SU-2016:3203-1

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-December/002501.html>

SuSE SLES 11 SP4

i586

kernel-xen-base-3.0.101-91.1
kernel-pae-devel-3.0.101-91.1
kernel-xen-3.0.101-91.1
kernel-xen-devel-3.0.101-91.1
kernel-ec2-base-3.0.101-91.1
kernel-source-3.0.101-91.1
kernel-syms-3.0.101-91.1
kernel-default-base-3.0.101-91.1
kernel-default-3.0.101-91.1
kernel-trace-devel-3.0.101-91.1
kernel-pae-base-3.0.101-91.1
kernel-ec2-3.0.101-91.1
kernel-ec2-devel-3.0.101-91.1
kernel-pae-3.0.101-91.1
kernel-trace-base-3.0.101-91.1
kernel-default-devel-3.0.101-91.1
kernel-trace-3.0.101-91.1

x86_64

kernel-xen-base-3.0.101-91.1
kernel-xen-3.0.101-91.1
kernel-xen-devel-3.0.101-91.1
kernel-ec2-base-3.0.101-91.1
kernel-source-3.0.101-91.1
kernel-syms-3.0.101-91.1
kernel-default-base-3.0.101-91.1
kernel-default-3.0.101-91.1
kernel-trace-devel-3.0.101-91.1
kernel-ec2-3.0.101-91.1
kernel-ec2-devel-3.0.101-91.1
kernel-trace-base-3.0.101-91.1
kernel-default-devel-3.0.101-91.1
kernel-trace-3.0.101-91.1

160180 - CentOS 5 CESA-2016-2963 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9637

Description

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

CESA-2016-2963

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-December/022181.html>

CentOS 5

x86_64

xen-libs-3.0.3-148.el5_11

xen-devel-3.0.3-148.el5_11

xen-3.0.3-148.el5_11

i386

xen-libs-3.0.3-148.el5_11

xen-devel-3.0.3-148.el5_11
xen-3.0.3-148.el5_11

170750 - Amazon Linux AMI ALAS-2016-776 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6816, CVE-2016-8735

Description

The scan detected that the host is missing the following update:
ALAS-2016-776

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-776.html>

Amazon Linux AMI

noarch

tomcat6-docs-webapp-6.0.48-1.8.amzn1

tomcat6-servlet-2.5-api-6.0.48-1.8.amzn1

tomcat6-admin-webapps-6.0.48-1.8.amzn1

tomcat6-6.0.48-1.8.amzn1

tomcat6-jsp-2.1-api-6.0.48-1.8.amzn1

tomcat6-javadoc-6.0.48-1.8.amzn1

tomcat6-el-2.1-api-6.0.48-1.8.amzn1

tomcat6-webapps-6.0.48-1.8.amzn1

tomcat6-lib-6.0.48-1.8.amzn1

170751 - Amazon Linux AMI ALAS-2016-777 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6816, CVE-2016-8735

Description

The scan detected that the host is missing the following update:
ALAS-2016-777

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-777.html>

Amazon Linux AMI

noarch

tomcat7-lib-7.0.73-1.23.amzn1

tomcat7-servlet-3.0-api-7.0.73-1.23.amzn1

tomcat7-admin-webapps-7.0.73-1.23.amzn1

tomcat7-7.0.73-1.23.amzn1

tomcat7-el-2.2-api-7.0.73-1.23.amzn1

tomcat7-docs-webapp-7.0.73-1.23.amzn1

tomcat7-javadoc-7.0.73-1.23.amzn1

tomcat7-jsp-2.2-api-7.0.73-1.23.amzn1
tomcat7-log4j-7.0.73-1.23.amzn1
tomcat7-webapps-7.0.73-1.23.amzn1

170753 - Amazon Linux AMI ALAS-2016-775 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
ALAS-2016-775

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-775.html>

Amazon Linux AMI

x86_64

expat-2.1.0-10.21.amzn1

expat-debuginfo-2.1.0-10.21.amzn1

expat-devel-2.1.0-10.21.amzn1

i686

expat-2.1.0-10.21.amzn1

expat-debuginfo-2.1.0-10.21.amzn1

expat-devel-2.1.0-10.21.amzn1

170755 - Amazon Linux AMI ALAS-2016-778 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6816, CVE-2016-8735

Description

The scan detected that the host is missing the following update:
ALAS-2016-778

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-778.html>

Amazon Linux AMI

noarch

tomcat8-el-3.0-api-8.0.39-1.67.amzn1

tomcat8-admin-webapps-8.0.39-1.67.amzn1

tomcat8-javadoc-8.0.39-1.67.amzn1

tomcat8-docs-webapp-8.0.39-1.67.amzn1

tomcat8-jsp-2.3-api-8.0.39-1.67.amzn1

tomcat8-lib-8.0.39-1.67.amzn1

tomcat8-log4j-8.0.39-1.67.amzn1

tomcat8-8.0.39-1.67.amzn1
tomcat8-webapps-8.0.39-1.67.amzn1
tomcat8-servlet-3.1-api-8.0.39-1.67.amzn1

175041 - Scientific Linux Security ERRATA Important: pacemaker on SL7.x x86_64 (1612-1035)

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

Risk Level: High

CVE: CVE-2016-7035

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: pacemaker on SL7.x x86_64 (1612-1035)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=1035>

SL7
x86_64
pacemaker-libs-1.1.15-11.el7_3.2
pacemaker-cluster-libs-1.1.15-11.el7_3.2
pacemaker-cts-1.1.15-11.el7_3.2
pacemaker-nagios-plugins-metadata-1.1.15-11.el7_3.2
pacemaker-debuginfo-1.1.15-11.el7_3.2
pacemaker-remote-1.1.15-11.el7_3.2
pacemaker-libs-devel-1.1.15-11.el7_3.2
pacemaker-doc-1.1.15-11.el7_3.2
pacemaker-1.1.15-11.el7_3.2
pacemaker-cli-1.1.15-11.el7_3.2

175044 - Scientific Linux Security ERRATA Moderate: expat on SL6.x, SL7.x i386/x86_64 (1612-14922)

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

Risk Level: High

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: expat on SL6.x, SL7.x i386/x86_64 (1612-14922)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=14922>

SL7
x86_64
expat-debuginfo-2.1.0-10.el7_3
expat-static-2.1.0-10.el7_3
expat-2.1.0-10.el7_3
expat-devel-2.1.0-10.el7_3

SL6
x86_64
expat-debuginfo-2.0.1-13.el6_8
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

i386
expat-debuginfo-2.0.1-13.el6_8
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

175045 - Scientific Linux Security ERRATA Moderate: dhcp on SL7.x x86_64 (1612-4284)

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

Risk Level: High

CVE: CVE-2016-2774

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: dhcp on SL7.x x86_64 (1612-4284)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=4284>

SL7
x86_64
dhcp-common-4.2.5-47.el7
dhcp-debuginfo-4.2.5-47.el7
dhcp-4.2.5-47.el7
dhclient-4.2.5-47.el7
dhcp-libs-4.2.5-47.el7
dhcp-devel-4.2.5-47.el7

175050 - Scientific Linux Security ERRATA Moderate: tomcat on SL7.x (noarch) (1612-3481)

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

Risk Level: High

CVE: CVE-2015-5174, CVE-2015-5345, 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:
Security ERRATA Moderate: tomcat on SL7.x (noarch) (1612-3481)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=3481>

SL7
noarch
tomcat-webapps-7.0.69-10.el7
tomcat-jsvc-7.0.69-10.el7

tomcat-servlet-3.0-api-7.0.69-10.el7
tomcat-7.0.69-10.el7
tomcat-jsp-2.2-api-7.0.69-10.el7
tomcat-docs-webapp-7.0.69-10.el7
tomcat-admin-webapps-7.0.69-10.el7
tomcat-el-2.2-api-7.0.69-10.el7
tomcat-lib-7.0.69-10.el7
tomcat-javadoc-7.0.69-10.el7

175051 - Scientific Linux Security ERRATA Important: resteasy-base on SL7.x (noarch) (1612-2024)

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

Risk Level: High

CVE: CVE-2016-7050

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: resteasy-base on SL7.x (noarch) (1612-2024)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=2024>

SL7

noarch

resteasy-base-jaxrs-api-3.0.6-4.el7
resteasy-base-tjws-3.0.6-4.el7
resteasy-base-javadoc-3.0.6-4.el7
resteasy-base-jaxrs-all-3.0.6-4.el7
resteasy-base-jettison-provider-3.0.6-4.el7
resteasy-base-providers-pom-3.0.6-4.el7
resteasy-base-atom-provider-3.0.6-4.el7
resteasy-base-client-3.0.6-4.el7
resteasy-base-jaxb-provider-3.0.6-4.el7
resteasy-base-3.0.6-4.el7
resteasy-base-jaxrs-3.0.6-4.el7
resteasy-base-jackson-provider-3.0.6-4.el7
resteasy-base-resteasy-pom-3.0.6-4.el7

175062 - Scientific Linux Security ERRATA Moderate: php on SL7.x x86_64 (1612-6321)

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

Risk Level: High

CVE: CVE-2016-5399, CVE-2016-5766, CVE-2016-5767, CVE-2016-5768

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: php on SL7.x x86_64 (1612-6321)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=6321>

SL7
x86_64
php-bcmath-5.4.16-42.el7
php-devel-5.4.16-42.el7
php-odbc-5.4.16-42.el7
php-intl-5.4.16-42.el7
php-xml-5.4.16-42.el7
php-recode-5.4.16-42.el7
php-pdo-5.4.16-42.el7
php-embedded-5.4.16-42.el7
php-pspell-5.4.16-42.el7
php-debuginfo-5.4.16-42.el7
php-enchant-5.4.16-42.el7
php-ldap-5.4.16-42.el7
php-soap-5.4.16-42.el7
php-dba-5.4.16-42.el7
php-5.4.16-42.el7
php-gd-5.4.16-42.el7
php-cli-5.4.16-42.el7
php-mysqlnd-5.4.16-42.el7
php-mbstring-5.4.16-42.el7
php-fpm-5.4.16-42.el7
php-common-5.4.16-42.el7
php-xmlrpc-5.4.16-42.el7
php-pgsql-5.4.16-42.el7
php-mysql-5.4.16-42.el7
php-snmp-5.4.16-42.el7
php-process-5.4.16-42.el7

175064 - Scientific Linux Security ERRATA Moderate: openssl on SL7.x x86_64 (1612-11841)

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 SL7.x x86_64 (1612-11841)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=11841>

SL7
x86_64
openssl-server-sysvinit-6.6.1p1-31.el7
openssl-clients-6.6.1p1-31.el7
openssl-askpass-6.6.1p1-31.el7
openssl-server-6.6.1p1-31.el7
openssl-debuginfo-6.6.1p1-31.el7
openssl-keycat-6.6.1p1-31.el7
openssl-6.6.1p1-31.el7
pam_ssh_agent_auth-0.9.3-9.31.el7
openssl-ldap-6.6.1p1-31.el7

175065 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-15944)

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

Risk Level: High

CVE: CVE-2016-9079

Description

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

Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-15944)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=15944>

SL5

x86_64

thunderbird-debuginfo-45.5.1-1.el5_11

thunderbird-45.5.1-1.el5_11

i386

thunderbird-debuginfo-45.5.1-1.el5_11

thunderbird-45.5.1-1.el5_11

SL7

x86_64

thunderbird-debuginfo-45.5.1-1.el7_3

thunderbird-45.5.1-1.el7_3

SL6

x86_64

thunderbird-45.5.1-1.el6_8

thunderbird-debuginfo-45.5.1-1.el6_8

i386

thunderbird-45.5.1-1.el6_8

thunderbird-debuginfo-45.5.1-1.el6_8

175067 - Scientific Linux Security ERRATA Important: xen on SL5.x i386/x86_64 (1612-17477)

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

Risk Level: High

CVE: CVE-2016-9637

Description

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

Security ERRATA Important: xen on SL5.x i386/x86_64 (1612-17477)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=17477>

SL5

x86_64
xen-libs-3.0.3-148.el5_11
xen-devel-3.0.3-148.el5_11
xen-3.0.3-148.el5_11
xen-debuginfo-3.0.3-148.el5_11

i386
xen-libs-3.0.3-148.el5_11
xen-devel-3.0.3-148.el5_11
xen-3.0.3-148.el5_11
xen-debuginfo-3.0.3-148.el5_11

175077 - Scientific Linux Security ERRATA Moderate: nettle on SL7.x x86_64 (1612-8927)

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

Risk Level: High

CVE: CVE-2015-8803, CVE-2015-8804, CVE-2015-8805, CVE-2016-6489

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: nettle on SL7.x x86_64 (1612-8927)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=8927>

SL7
x86_64
nettle-2.7.1-8.el7
nettle-debuginfo-2.7.1-8.el7
nettle-devel-2.7.1-8.el7

175079 - Scientific Linux Security ERRATA Important: memcached on SL7.x x86_64 (1612-14560)

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

Risk Level: High

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: memcached on SL7.x x86_64 (1612-14560)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=14560>

SL7
x86_64
memcached-debuginfo-1.4.15-10.el7_3.1
memcached-devel-1.4.15-10.el7_3.1
memcached-1.4.15-10.el7_3.1

175081 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-15252)

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

Risk Level: High

CVE: CVE-2016-5290

Description

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

Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-15252)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=15252>

SL5

x86_64

thunderbird-debuginfo-45.5.0-1.el5_11

thunderbird-45.5.0-1.el5_11

i386

thunderbird-debuginfo-45.5.0-1.el5_11

thunderbird-45.5.0-1.el5_11

SL7

x86_64

thunderbird-debuginfo-45.5.0-1.el7_3

thunderbird-45.5.0-1.el7_3

SL6

x86_64

thunderbird-45.5.0-1.el6_8

thunderbird-debuginfo-45.5.0-1.el6_8

i386

thunderbird-45.5.0-1.el6_8

thunderbird-debuginfo-45.5.0-1.el6_8

191520 - Fedora Linux 24 FEDORA-2016-e45a7e7b13 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6911, CVE-2016-7568, CVE-2016-8670

Description

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

FEDORA-2016-e45a7e7b13

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/2016/12/?count=200&page=2>

Fedora Core 24

21021 - (K48220300) F5 BIG-IP Libxml2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-1836

Description

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

Observation

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

A use-after-free vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the xmlDictComputeFastKey function in libxml2. Successful exploitation could allow an attacker to cause a denial of service condition.

21027 - Cisco IOS Frame Forwarding Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-6473

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw occurs because some specific Layer 2 frames are not properly consumed by the software. Successful exploitation could allow an attacker to cause network storm by injecting the Layer 2 frame into the network segment, leading to a denial of service.

21028 - Cisco IOS SSH X.509 Authentication Bypass Vulnerability (CSCuv89417)

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

Risk Level: Medium

CVE: CVE-2016-6474

Description

A security bypass vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A security bypass vulnerability is present in some versions of Cisco IOS. The flaw lies in the X.509v3 implementation for SSH authentication. Successful exploitation could allow an attacker to bypass security access restrictions and let them impersonate an existing valid user on the system.

21040 - (K71926235) F5 BIG-IP Libxml2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium
CVE: CVE-2016-1838

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the xmlParserPrintFileContextInternal function in libxml2. Successful exploitation could allow an attacker to cause a denial of service condition.

130653 - Debian Linux 8.0 DSA-3740-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2119, CVE-2016-2123, CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
DSA-3740-1

Observation

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

<http://www.debian.org/security/2016/dsa-3740>

Debian 8.0
all
samba_2:4.2.14+dfsg-0+deb8u2

170756 - Amazon Linux AMI ALAS-2016-779 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
ALAS-2016-779

Observation

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

<https://alas.aws.amazon.com/ALAS-2016-779.html>

Amazon Linux AMI
x86_64
vim-debuginfo-8.0.0134-1.43.amzn1
vim-common-8.0.0134-1.43.amzn1
vim-minimal-8.0.0134-1.43.amzn1
vim-enhanced-8.0.0134-1.43.amzn1

vim-filesystem-8.0.0134-1.43.amzn1

i686

vim-filesystem-8.0.0134-1.43.amzn1

vim-common-8.0.0134-1.43.amzn1

vim-minimal-8.0.0134-1.43.amzn1

vim-enhanced-8.0.0134-1.43.amzn1

vim-debuginfo-8.0.0134-1.43.amzn1

175043 - Scientific Linux Security ERRATA Moderate: gimp on SL7.x x86_64 (1612-8585)

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

Risk Level: Medium

CVE: CVE-2016-4994

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: gimp on SL7.x x86_64 (1612-8585)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=8585>

SL7

x86_64

gimp-devel-tools-2.8.16-3.el7

gimp-debuginfo-2.8.16-3.el7

gimp-2.8.16-3.el7

gimp-libs-2.8.16-3.el7

gimp-devel-2.8.16-3.el7

noarch

gimp-help-ja-2.8.2-1.el7

gimp-help-es-2.8.2-1.el7

gimp-help-ru-2.8.2-1.el7

gimp-help-ca-2.8.2-1.el7

gimp-help-fr-2.8.2-1.el7

gimp-help-en_GB-2.8.2-1.el7

gimp-help-2.8.2-1.el7

gimp-help-de-2.8.2-1.el7

gimp-help-it-2.8.2-1.el7

gimp-help-ko-2.8.2-1.el7

gimp-help-nl-2.8.2-1.el7

gimp-help-da-2.8.2-1.el7

gimp-help-nn-2.8.2-1.el7

gimp-help-sl-2.8.2-1.el7

gimp-help-zh_CN-2.8.2-1.el7

gimp-help-pt_BR-2.8.2-1.el7

gimp-help-el-2.8.2-1.el7

gimp-help-sv-2.8.2-1.el7

175046 - Scientific Linux Security ERRATA Moderate: libguestfs and virt-p2v on SL7.x x86_64 (1612-8206)

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 and virt-p2v on SL7.x x86_64 (1612-8206)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=8206>

SL7
x86_64
lua-guestfs-1.32.7-3.el7
ocaml-libguestfs-devel-1.32.7-3.el7
libguestfs-gobject-1.32.7-3.el7
libguestfs-xfstools-1.32.7-3.el7
ocaml-libguestfs-1.32.7-3.el7
libguestfs-devel-1.32.7-3.el7
libguestfs-tools-c-1.32.7-3.el7
ruby-libguestfs-1.32.7-3.el7
python-libguestfs-1.32.7-3.el7
virt-dib-1.32.7-3.el7
libguestfs-rescue-1.32.7-3.el7
libguestfs-gobject-devel-1.32.7-3.el7
perl-Sys-Guestfs-1.32.7-3.el7
libguestfs-rsync-1.32.7-3.el7
libguestfs-1.32.7-3.el7
libguestfs-java-1.32.7-3.el7
libguestfs-debuginfo-1.32.7-3.el7
libguestfs-gfs2-1.32.7-3.el7
libguestfs-java-devel-1.32.7-3.el7

noarch
libguestfs-man-pages-ja-1.32.7-3.el7
libguestfs-man-pages-uk-1.32.7-3.el7
libguestfs-inspect-icons-1.32.7-3.el7
libguestfs-bash-completion-1.32.7-3.el7
libguestfs-javadoc-1.32.7-3.el7
libguestfs-tools-1.32.7-3.el7
libguestfs-gobject-doc-1.32.7-3.el7

175082 - Scientific Linux Security ERRATA Moderate: postgresql on SL7.x x86_64 (1612-3929)

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: postgresql on SL7.x x86_64 (1612-3929)

Observation

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

SL7

x86_64

postgresql-plpython-9.2.18-1.el7

postgresql-server-9.2.18-1.el7

postgresql-devel-9.2.18-1.el7

postgresql-9.2.18-1.el7

postgresql-contrib-9.2.18-1.el7

postgresql-pltcl-9.2.18-1.el7

postgresql-docs-9.2.18-1.el7

postgresql-upgrade-9.2.18-1.el7

postgresql-debuginfo-9.2.18-1.el7

postgresql-libs-9.2.18-1.el7

postgresql-plperl-9.2.18-1.el7

postgresql-test-9.2.18-1.el7

191501 - Fedora Linux 23 FEDORA-2016-b4896f20b3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9920

Description

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

FEDORA-2016-b4896f20b3

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/2016/12/?count=200&page=4>

Fedora Core 23

roundcubemail-1.2.3-1.fc23

191502 - Fedora Linux 23 FEDORA-2016-bf6c3ea62c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1249, CVE-2016-1251

Description

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

FEDORA-2016-bf6c3ea62c

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/2016/12/?count=200&page=2>

Fedora Core 23

perl-DBD-MySQL-4.033-4.fc23

21012 - Cisco IOS Zone-Based Firewall Feature Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-9201

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw is due to a logic error in the Zone-Based Firewall feature of Cisco IOS. Successful exploitation could allow an attacker to pass traffic that should be dropped based on the configuration.

21019 - (K24036027) F5 BIG-IP Libarchive Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-5844

Description

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

Observation

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

A buffer overflow vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in ISO parser in libarchive. Successful exploitation could allow an attacker to cause a denial of service condition.

21020 - (K24322529) F5 BIG-IP Libxml2 Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-4447, CVE-2016-4449

Description

Multiple vulnerabilities are present in some versions of F5 BIG-IP systems.

Observation

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

Multiple vulnerabilities are present in some versions of F5 BIG-IP systems. The flaw lies in various functions in parser.c in libxml2. Successful exploitation could allow an attacker to retrieve sensitive data or cause a denial of service condition.

21038 - (APSB16-45) Vulnerability In Adobe Digital Editions

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-7888, CVE-2016-7889

Description

Multiple vulnerabilities are present in some version of Adobe Digital Editions.

Observation

Adobe Digital Editions is the Adobe's eBook reader software.

Multiple vulnerabilities are present in some version of Adobe Digital Editions. The flaws lie in many components. Successful exploitation by an attacker could lead to information disclosure or cause memory address leak.

21039 - (APSB16-45) Vulnerability In Adobe Digital Editions

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-7888, CVE-2016-7889

Description

Multiple vulnerabilities are present in some version of Adobe Digital Editions.

Observation

Adobe Digital Editions is the Adobe's eBook reader software.

Multiple vulnerabilities are present in some version of Adobe Digital Editions. The flaws lie in many components. Successful exploitation by an attacker could lead to information disclosure or cause memory address leak.

21041 - (K35246595) F5 BIG-IP Libarchive Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-5418

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the way libarchive handles hardlink archive entries of non-zero size. Successful exploitation could allow an attacker to write to arbitrary files.

21045 - (APSB16-44) Vulnerability In Adobe ColdFusion Builder

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-7887

Description

An information disclosure vulnerability is present in some versions of Adobe ColdFusion Builder.

Observation

Adobe ColdFusion Builder is an IDE for web application development.

An information disclosure vulnerability is present in some versions of Adobe ColdFusion Builder. The flaw lies in an unknown component. Successful exploitation could allow an attacker to obtain sensitive information.

The update provided by Adobe bulletin AP SB16-44 resolves this issue. The target system appears to be missing this update.

21046 - (APSB16-44) Vulnerability In Adobe ColdFusion Builder

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-7887

Description

An information disclosure vulnerability is present in some versions of Adobe ColdFusion Builder.

Observation

Adobe ColdFusion Builder is an IDE for web application development.

An information disclosure vulnerability is present in some versions of Adobe ColdFusion Builder. The flaw lies in an unknown component. Successful exploitation could allow an attacker to obtain sensitive information.

The update provided by Adobe bulletin AP SB16-44 resolves this issue. The target system appears to be missing this update.

21047 - Joomla Information Disclosure Vulnerability (20161203)

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

Risk Level: Medium

CVE: CVE-2016-9837

Description

An information disclosure vulnerability is present in some versions of Joomla CMS.

Observation

Joomla! CMS is an open source content management system.

An information disclosure vulnerability is present in some versions of Joomla CMS. The flaw lies in how the Beez3 layout manages the content's access control lists. Successful exploitation of this vulnerability could allow a user to view restricted content.

145103 - SuSE SLES 11 SP4 SUSE-SU-2016:3199-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8899

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3199-1

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-December/002500.html>

SuSE SLES 11 SP4
i586
dnsmasq-2.71-0.16.3

x86_64
dnsmasq-2.71-0.16.3

170754 - Amazon Linux AMI ALAS-2016-773 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4992, CVE-2016-5405, CVE-2016-5416

Description

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

ALAS-2016-773

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2016-773.html>

Amazon Linux AMI

x86_64
389-ds-base-libs-1.3.5.10-11.49.amzn1
389-ds-base-snmp-1.3.5.10-11.49.amzn1
389-ds-base-debuginfo-1.3.5.10-11.49.amzn1
389-ds-base-devel-1.3.5.10-11.49.amzn1
389-ds-base-1.3.5.10-11.49.amzn1

i686
389-ds-base-libs-1.3.5.10-11.49.amzn1
389-ds-base-debuginfo-1.3.5.10-11.49.amzn1
389-ds-base-snmp-1.3.5.10-11.49.amzn1
389-ds-base-devel-1.3.5.10-11.49.amzn1
389-ds-base-1.3.5.10-11.49.amzn1

175042 - Scientific Linux Security ERRATA Moderate: pacemaker on SL7.x x86_64 (1612-11137)

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

Risk Level: Medium

CVE: CVE-2016-7797

Description

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

Security ERRATA Moderate: pacemaker on SL7.x x86_64 (1612-11137)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=11137>

SL7
x86_64

pacemaker-doc-1.1.15-11.el7
pacemaker-nagios-plugins-metadata-1.1.15-11.el7
pacemaker-remote-1.1.15-11.el7
pacemaker-libs-1.1.15-11.el7
pacemaker-1.1.15-11.el7
pacemaker-cluster-libs-1.1.15-11.el7
pacemaker-cts-1.1.15-11.el7
pacemaker-debuginfo-1.1.15-11.el7
pacemaker-libs-devel-1.1.15-11.el7
pacemaker-cli-1.1.15-11.el7

175048 - Scientific Linux Security ERRATA Important: bind on SL7.x x86_64 (1612-1374)

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL7.x x86_64 (1612-1374)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=1374>

SL7
x86_64
bind-lite-devel-9.9.4-38.el7_3
bind-sdb-9.9.4-38.el7_3
bind-pkcs11-utils-9.9.4-38.el7_3
bind-debuginfo-9.9.4-38.el7_3
bind-chroot-9.9.4-38.el7_3
bind-devel-9.9.4-38.el7_3
bind-pkcs11-devel-9.9.4-38.el7_3
bind-pkcs11-libs-9.9.4-38.el7_3
bind-9.9.4-38.el7_3
bind-libs-9.9.4-38.el7_3
bind-utils-9.9.4-38.el7_3
bind-libs-lite-9.9.4-38.el7_3
bind-sdb-chroot-9.9.4-38.el7_3
bind-pkcs11-9.9.4-38.el7_3

noarch
bind-license-9.9.4-38.el7_3

175053 - Scientific Linux Security ERRATA Moderate: curl on SL7.x x86_64 (1612-13541)

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

Risk Level: Medium

CVE: CVE-2016-5419, CVE-2016-5420, CVE-2016-7141

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: curl on SL7.x x86_64 (1612-13541)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=13541>

SL7

x86_64

libcurl-7.29.0-35.el7

libcurl-devel-7.29.0-35.el7

curl-7.29.0-35.el7

curl-debuginfo-7.29.0-35.el7

175054 - Scientific Linux Security ERRATA Moderate: firewalld on SL7.x (noarch) (1612-10449)

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

Risk Level: Medium

CVE: CVE-2016-5410

Description

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

Security ERRATA Moderate: firewalld on SL7.x (noarch) (1612-10449)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=10449>

SL7

noarch

python-firewall-0.4.3.2-8.el7

firewall-applet-0.4.3.2-8.el7

firewalld-filesystem-0.4.3.2-8.el7

firewalld-0.4.3.2-8.el7

firewall-config-0.4.3.2-8.el7

175061 - Scientific Linux Security ERRATA Moderate: libreswan on SL7.x x86_64 (1612-5294)

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

Risk Level: Medium

CVE: CVE-2016-5361

Description

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

Security ERRATA Moderate: libreswan on SL7.x x86_64 (1612-5294)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=5294>

SL7

x86_64

libreswan-debuginfo-3.15-8.el7
libreswan-3.15-8.el7

175071 - Scientific Linux Security ERRATA Moderate: sudo on SL6.x, SL7.x i386/x86_64 (1612-16295)

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: sudo on SL6.x, SL7.x i386/x86_64 (1612-16295)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=16295>

SL7
x86_64
sudo-devel-1.8.6p7-21.el7_3
sudo-debuginfo-1.8.6p7-21.el7_3
sudo-1.8.6p7-21.el7_3

SL6
x86_64
sudo-debuginfo-1.8.6p3-25.el6_8
sudo-devel-1.8.6p3-25.el6_8
sudo-1.8.6p3-25.el6_8

i386
sudo-debuginfo-1.8.6p3-25.el6_8
sudo-devel-1.8.6p3-25.el6_8
sudo-1.8.6p3-25.el6_8

175074 - Scientific Linux Security ERRATA Moderate: squid on SL7.x x86_64 (1612-2373)

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

Risk Level: Medium

CVE: CVE-2016-2569, CVE-2016-2570, CVE-2016-2571, CVE-2016-2572, CVE-2016-3948

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: squid on SL7.x x86_64 (1612-2373)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=2373>

SL7
x86_64
squid-sysvinit-3.5.20-2.el7
squid-migration-script-3.5.20-2.el7

squid-3.5.20-2.el7
squid-debuginfo-3.5.20-2.el7

175075 - Scientific Linux Security ERRATA Moderate: ntp on SL7.x x86_64 (1612-12188)

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2015-5194, CVE-2015-5195, CVE-2015-5196, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7974, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ntp on SL7.x x86_64 (1612-12188)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=12188>

SL7
x86_64
ntpdate-4.2.6p5-25.el7
ntp-debuginfo-4.2.6p5-25.el7
sntp-4.2.6p5-25.el7
ntp-4.2.6p5-25.el7

noarch
ntp-doc-4.2.6p5-25.el7
ntp-perl-4.2.6p5-25.el7

175076 - Scientific Linux Security ERRATA Moderate: pcs on SL7.x x86_64 (1612-2784)

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

Risk Level: Medium

CVE: CVE-2016-0720, CVE-2016-0721

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: pcs on SL7.x x86_64 (1612-2784)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=2784>

SL7
x86_64
pcs-0.9.152-10.el7
pcs-debuginfo-0.9.152-10.el7

175078 - Scientific Linux Security ERRATA Low: glibc on SL7.x x86_64 (1612-13916)

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

Risk Level: Medium

CVE: CVE-2016-3075

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: glibc on SL7.x x86_64 (1612-13916)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=13916>

SL7
x86_64
glibc-utils-2.17-157.el7
glibc-debuginfo-2.17-157.el7
glibc-devel-2.17-157.el7
glibc-static-2.17-157.el7
glibc-headers-2.17-157.el7
glibc-debuginfo-common-2.17-157.el7
glibc-2.17-157.el7
nscd-2.17-157.el7
glibc-common-2.17-157.el7

175083 - Scientific Linux Security ERRATA Moderate: 389-ds-base on SL7.x x86_64 (1612-9692)

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

Risk Level: Medium

CVE: CVE-2016-4992, CVE-2016-5405, CVE-2016-5416

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: 389-ds-base on SL7.x x86_64 (1612-9692)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=9692>

SL7
x86_64
389-ds-base-1.3.5.10-11.el7
389-ds-base-debuginfo-1.3.5.10-11.el7
389-ds-base-libs-1.3.5.10-11.el7
389-ds-base-devel-1.3.5.10-11.el7
389-ds-base-snmp-1.3.5.10-11.el7

182217 - FreeBSD atheme-services Multiple Vulnerabilities (e47ab5db-c333-11e6-ae1b-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2014-9773, CVE-2016-4478

Description

The scan detected that the host is missing the following update:
atheme-services -- multiple vulnerabilities (e47ab5db-c333-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/e47ab5db-c333-11e6-ae1b-002590263bf5.html>

Affected packages:

atheme-services < 7.2.7

191504 - Fedora Linux 24 FEDORA-2016-cb03b6b70f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9839

Description

The scan detected that the host is missing the following update:
FEDORA-2016-cb03b6b70f

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/2016/12/?count=200&page=1>

Fedora Core 24

mapserver-6.2.3-1.fc24

191516 - Fedora Linux 25 FEDORA-2016-04c687d2aa Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9839

Description

The scan detected that the host is missing the following update:
FEDORA-2016-04c687d2aa

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/2016/12/?count=200&page=1>

Fedora Core 25

mapserver-7.0.3-1.git0f9ece8.fc25

21023 - (SYM16-023) Symantec VIP Access Desktop Arbitrary DLL Execution Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-6593

Description

An arbitrary code execution vulnerability exists in some versions of Symantec VIP Access Desktop.

Observation

Symantec VIP Access Desktop is a management software used to protect online transactions and ensure secure access to accounts.

An arbitrary code execution vulnerability exists in some versions of Symantec VIP Access Desktop. The flaw lies in VIP Access Desktop UI Manager component. Successful exploitation of this vulnerability could allow an attacker to load malicious DLL instead of the required product DLL.

21032 - (SB10179) McAfee Endpoint Security Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-8010

Description

A security bypass vulnerability is present in some versions of McAfee Endpoint Security.

Observation

McAfee Endpoint Security is a threat defense tool for workstations.

A security bypass vulnerability is present in some versions of McAfee Endpoint Security. The flaw lies in the McAfee Anti-Malware Core (AMCore) component. Successful exploitation could allow a malicious user to bypass security protections, affecting the integrity of the system.

21034 - (SB10179) McAfee Application Control Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-8010

Description

A security bypass vulnerability exists in some versions of McAfee Application Control.

Observation

McAfee Application Control is a security manager software that prevents execution of unwanted programs.

A security bypass vulnerability exists in some versions of McAfee Application Control. The flaw lies in an unspecified component. Successful exploitation could allow a malicious authenticated user to bypass local security protections.

21049 - (APSB16-46) Vulnerability In Adobe Robohelp

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium
CVE: CVE-2016-7891

Description

A vulnerability is present in Adobe RoboHelp.

Observation

Adobe RoboHelp is a tool used to create help document.

A vulnerability is present in Adobe RoboHelp. The flaw occurs due to an input validation issue. Successful exploitation could allow an attacker to launch cross-site scripting attacks.

The update provided by Adobe bulletin APSB16-46 resolves this issue. The target system appears to be missing this update.

145101 - SuSE SLES 11 SP4 SUSE-SU-2016:3174-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7777, CVE-2016-7908, CVE-2016-7909, CVE-2016-8576, CVE-2016-8667, CVE-2016-8669, CVE-2016-8909, CVE-2016-8910, CVE-2016-9379, CVE-2016-9380, CVE-2016-9381, CVE-2016-9382, CVE-2016-9383, CVE-2016-9385, CVE-2016-9386, CVE-2016-9637

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3174-1

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-December/002492.html>

SuSE SLES 11 SP4

x86_64

xen-kmp-default-4.4.4_10_3.0.101_88-43.5

xen-tools-4.4.4_10-43.5

xen-4.4.4_10-43.5

xen-libs-32bit-4.4.4_10-43.5

xen-libs-4.4.4_10-43.5

xen-doc-html-4.4.4_10-43.5

xen-tools-domU-4.4.4_10-43.5

i586

xen-kmp-default-4.4.4_10_3.0.101_88-43.5

xen-kmp-pae-4.4.4_10_3.0.101_88-43.5

xen-libs-4.4.4_10-43.5

xen-tools-domU-4.4.4_10-43.5

175040 - Scientific Linux Security ERRATA Low: krb5 on SL7.x x86_64 (1612-5972)

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

Risk Level: Medium

CVE: CVE-2016-3119, CVE-2016-3120

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: krb5 on SL7.x x86_64 (1612-5972)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=5972>

SL7
x86_64
libkadm5-1.14.1-26.el7
krb5-devel-1.14.1-26.el7
krb5-debuginfo-1.14.1-26.el7
krb5-libs-1.14.1-26.el7
krb5-server-ldap-1.14.1-26.el7
krb5-pkinit-1.14.1-26.el7
krb5-workstation-1.14.1-26.el7
krb5-server-1.14.1-26.el7

175047 - Scientific Linux Security ERRATA Moderate: libvirt on SL7.x x86_64 (1612-9310)

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

Risk Level: Medium

CVE: CVE-2015-5160, CVE-2015-5313, CVE-2016-5008

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libvirt on SL7.x x86_64 (1612-9310)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=9310>

SL7
x86_64
libvirt-daemon-driver-lxc-2.0.0-10.el7
libvirt-daemon-kvm-2.0.0-10.el7
libvirt-lock-sanlock-2.0.0-10.el7
libvirt-devel-2.0.0-10.el7
libvirt-daemon-2.0.0-10.el7
libvirt-daemon-driver-nwfilter-2.0.0-10.el7
libvirt-daemon-lxc-2.0.0-10.el7
libvirt-daemon-driver-secret-2.0.0-10.el7
libvirt-daemon-driver-interface-2.0.0-10.el7
libvirt-daemon-driver-storage-2.0.0-10.el7
libvirt-daemon-driver-nodedev-2.0.0-10.el7
libvirt-client-2.0.0-10.el7
libvirt-2.0.0-10.el7
libvirt-daemon-config-nwfilter-2.0.0-10.el7
libvirt-docs-2.0.0-10.el7
libvirt-nss-2.0.0-10.el7
libvirt-daemon-driver-network-2.0.0-10.el7
libvirt-debuginfo-2.0.0-10.el7
libvirt-login-shell-2.0.0-10.el7
libvirt-daemon-driver-qemu-2.0.0-10.el7

175068 - Scientific Linux Security ERRATA Moderate: fontconfig on SL7.x x86_64 (1612-5632)

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

Risk Level: Medium

CVE: CVE-2016-5384

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: fontconfig on SL7.x x86_64 (1612-5632)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=5632>

SL7
x86_64
fontconfig-2.10.95-10.el7
fontconfig-devel-2.10.95-10.el7
fontconfig-debuginfo-2.10.95-10.el7

noarch
fontconfig-devel-doc-2.10.95-10.el7

175070 - Scientific Linux Security ERRATA Moderate: systemd on SL7.x x86_64 (1612-1691)

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

Risk Level: Medium

CVE: CVE-2016-7795

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: systemd on SL7.x x86_64 (1612-1691)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=1691>

SL7
x86_64
systemd-219-30.el7_3.3
systemd-debuginfo-219-30.el7_3.3
systemd-sysv-219-30.el7_3.3
systemd-libs-219-30.el7_3.3
systemd-networkd-219-30.el7_3.3
systemd-journal-gateway-219-30.el7_3.3
systemd-python-219-30.el7_3.3
systemd-resolved-219-30.el7_3.3
libgudev1-devel-219-30.el7_3.3
systemd-devel-219-30.el7_3.3
libgudev1-219-30.el7_3.3

175073 - Scientific Linux Security ERRATA Moderate: wget on SL7.x x86_64 (1612-7504)

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

Risk Level: Medium

CVE: CVE-2016-4971

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: wget on SL7.x x86_64 (1612-7504)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=7504>

SL7

x86_64

wget-debuginfo-1.14-13.el7

wget-1.14-13.el7

185522 - Ubuntu Linux 12.04 USN-3159-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7916

Description

The scan detected that the host is missing the following update:
USN-3159-1

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-December/003674.html>

Ubuntu 12.04

linux-image-3.2.0-119-generic-pae_3.2.0-119.162

linux-image-generic_3.2.0.119.134

linux-image-3.2.0-119-powerpc64-smp_3.2.0-119.162

linux-image-generic-pae_3.2.0.119.134

linux-image-omap_3.2.0.119.134

linux-image-3.2.0-119-powerpc-smp_3.2.0-119.162

linux-image-3.2.0-119-virtual_3.2.0-119.162

linux-image-powerpc-smp_3.2.0.119.134

linux-image-3.2.0-119-generic_3.2.0-119.162

linux-image-3.2.0-119-omap_3.2.0-119.162

linux-image-highbank_3.2.0.119.134

linux-image-powerpc64-smp_3.2.0.119.134

linux-image-3.2.0-119-highbank_3.2.0-119.162

linux-image-virtual_3.2.0.119.134

185523 - Ubuntu Linux 12.04 USN-3159-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7916

Description

The scan detected that the host is missing the following update:
USN-3159-2

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-December/003675.html>

Ubuntu 12.04

linux-image-omap4_3.2.0.1497.92

linux-image-3.2.0-1497-omap4_3.2.0-1497.124

185526 - Ubuntu Linux 12.04 USN-3160-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6213, CVE-2016-7916

Description

The scan detected that the host is missing the following update:
USN-3160-2

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-December/003677.html>

Ubuntu 12.04

linux-image-3.13.0-106-generic_3.13.0-106.153~precise1

linux-image-generic-lts-trusty_3.13.0.106.97

linux-image-3.13.0-106-generic-lpae_3.13.0-106.153~precise1

linux-image-generic-lpae-lts-trusty_3.13.0.106.97

185533 - Ubuntu Linux 14.04 USN-3160-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6213, CVE-2016-7916

Description

The scan detected that the host is missing the following update:
USN-3160-1

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-December/003676.html>

Ubuntu 14.04

linux-image-3.13.0-106-powerpc64-smp_3.13.0-106.153
linux-image-3.13.0-106-powerpc64-emb_3.13.0-106.153
linux-image-3.13.0-106-powerpc-e500_3.13.0-106.153
linux-image-generic-lpae_3.13.0.106.114
linux-image-3.13.0-106-generic_3.13.0-106.153
linux-image-powerpc64-smp_3.13.0.106.114
linux-image-powerpc64-emb_3.13.0.106.114
linux-image-3.13.0-106-powerpc-e500mc_3.13.0-106.153
linux-image-powerpc-e500_3.13.0.106.114
linux-image-generic_3.13.0.106.114
linux-image-3.13.0-106-powerpc-smp_3.13.0-106.153
linux-image-3.13.0-106-generic-lpae_3.13.0-106.153
linux-image-powerpc-smp_3.13.0.106.114
linux-image-3.13.0-106-lowlatency_3.13.0-106.153
linux-image-lowlatency_3.13.0.106.114
linux-image-powerpc-e500mc_3.13.0.106.114

191508 - Fedora Linux 24 FEDORA-2016-4871c26b3c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9888

Description

The scan detected that the host is missing the following update:
FEDORA-2016-4871c26b3c

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/2016/12/?count=200&page=3>

Fedora Core 24

libgsf-1.14.33-4.fc24

88830 - Slackware Linux 14.1, 14.2 SSA:2016-348-01 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:2016-348-01

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.399922>

Slackware 14.1
x86_64
mozilla-firefox-45.6.0esr-x86_64-1

Slackware 14.2
x86_64
mozilla-firefox-45.6.0esr-x86_64-1

i586
mozilla-firefox-45.6.0esr-i586-1

130648 - Debian Linux 8.0 DSA-3735-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-3735-1

Observation

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

<http://www.debian.org/security/2016/dsa-3735>

Debian 8.0
all
libgme0_0.5.5-2+deb8u1
libgme-dev_0.5.5-2+deb8u1

130649 - Debian Linux 8.0 DSA-3742-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9956

Description

The scan detected that the host is missing the following update:
DSA-3742-1

Observation

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

<http://www.debian.org/security/2016/dsa-3742>

Debian 8.0
all
flightgear_3.0.0-5+deb8u1

130650 - Debian Linux 8.0 DSA-3738-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6816, CVE-2016-8735, CVE-2016-9774, CVE-2016-9775

Description

The scan detected that the host is missing the following update:
DSA-3738-1

Observation

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

<http://www.debian.org/security/2016/dsa-3738>

Debian 8.0
all
tomcat7_7.0.56-3+deb8u6

130651 - Debian Linux 8.0 DSA-3739-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6816, CVE-2016-8735, CVE-2016-9774, CVE-2016-9775

Description

The scan detected that the host is missing the following update:
DSA-3739-1

Observation

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

<http://www.debian.org/security/2016/dsa-3739>

Debian 8.0
all
tomcat8_8.0.14-1+deb8u5

130652 - Debian Linux 8.0 DSA-3734-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
DSA-3734-1

Observation

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

For more information see:

<http://www.debian.org/security/2016/dsa-3734>

Debian 8.0
all
firefox-esr_45.6.0esr-1~deb8u1

130654 - Debian Linux 8.0 DSA-3741-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1254

Description

The scan detected that the host is missing the following update:
DSA-3741-1

Observation

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

<http://www.debian.org/security/2016/dsa-3741>

Debian 8.0
all
tor_0.2.5.12-4

130655 - Debian Linux 8.0 DSA-3737-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9935

Description

The scan detected that the host is missing the following update:
DSA-3737-1

Observation

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

<http://www.debian.org/security/2016/dsa-3737>

Debian 8.0
all
php5_5.6.29+dfsg-0+deb8u1

130656 - Debian Linux 8.0 DSA-3736-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6255, CVE-2016-8863

Description

The scan detected that the host is missing the following update:
DSA-3736-1

Observation

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

<http://www.debian.org/security/2016/dsa-3736>

Debian 8.0

all

libupnp6-dev_1:1.6.19+git20141001-1+deb8u1

libupnp-dev_1:1.6.19+git20141001-1+deb8u1

libupnp6_1:1.6.19+git20141001-1+deb8u1

libupnp6-doc_1:1.6.19+git20141001-1+deb8u1

libupnp6-dbg_1:1.6.19+git20141001-1+deb8u1

175055 - Scientific Linux Security ERRATA Low: mod_nss on SL7.x x86_64 (1612-4625)

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

Risk Level: Low

CVE: CVE-2016-3099

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: mod_nss on SL7.x x86_64 (1612-4625)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=4625>

SL7

x86_64

mod_nss-debuginfo-1.0.14-7.el7

mod_nss-1.0.14-7.el7

175060 - Scientific Linux Security ERRATA Low: NetworkManager on SL7.x x86_64 (1612-11489)

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

Risk Level: Low

CVE: CVE-2016-0764

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: NetworkManager on SL7.x x86_64 (1612-11489)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=11489>

SL7
x86_64
NetworkManager-libnm-devel-1.4.0-12.el7
NetworkManager-adsl-1.4.0-12.el7
network-manager-applet-1.4.0-2.el7
NetworkManager-wwan-1.4.0-12.el7
NetworkManager-wifi-1.4.0-12.el7
libnma-devel-1.4.0-2.el7
libnl3-devel-3.2.28-2.el7
libnl3-doc-3.2.28-2.el7
NetworkManager-tui-1.4.0-12.el7
NetworkManager-1.4.0-12.el7
libnl3-cli-3.2.28-2.el7
NetworkManager-libreswan-gnome-1.2.4-1.el7
NetworkManager-libreswan-1.2.4-1.el7
NetworkManager-team-1.4.0-12.el7
NetworkManager-debuginfo-1.4.0-12.el7
libnl3-debuginfo-3.2.28-2.el7
NetworkManager-bluetooth-1.4.0-12.el7
NetworkManager-glib-devel-1.4.0-12.el7
NetworkManager-glib-1.4.0-12.el7
libnm-gtk-devel-1.4.0-2.el7
libnm-gtk-1.4.0-2.el7
NetworkManager-libreswan-debuginfo-1.2.4-1.el7
network-manager-applet-debuginfo-1.4.0-2.el7
NetworkManager-config-server-1.4.0-12.el7
nm-connection-editor-1.4.0-2.el7
NetworkManager-libnm-1.4.0-12.el7
libnma-1.4.0-2.el7
libnl3-3.2.28-2.el7

noarch
NetworkManager-dispatcher-routing-rules-1.4.0-12.el7

175072 - Scientific Linux Security ERRATA Low: sudo on SL7.x x86_64 (1612-4962)

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

Risk Level: Low

CVE: CVE-2016-7091

Description

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

Security ERRATA Low: sudo on SL7.x x86_64 (1612-4962)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=4962>

SL7
x86_64
sudo-1.8.6p7-20.el7
sudo-debuginfo-1.8.6p7-20.el7
sudo-devel-1.8.6p7-20.el7

175080 - Scientific Linux Security ERRATA Low: util-linux on SL7.x x86_64 (1612-3139)

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

Risk Level: Low

CVE: CVE-2016-5011

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: util-linux on SL7.x x86_64 (1612-3139)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=3139>

SL7

x86_64

libmount-2.23.2-33.el7

libuuid-2.23.2-33.el7

libmount-devel-2.23.2-33.el7

uuid-devel-2.23.2-33.el7

libblkid-devel-2.23.2-33.el7

util-linux-debuginfo-2.23.2-33.el7

libblkid-2.23.2-33.el7

libuuid-devel-2.23.2-33.el7

util-linux-2.23.2-33.el7

182215 - FreeBSD mozilla Multiple Vulnerabilities (512c0ffd-cd39-4da4-b2dc-81ff4ba8e238)

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

Risk Level: Low

CVE: CVE-2016-9080, CVE-2016-9893, CVE-2016-9894, CVE-2016-9895, CVE-2016-9896, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9903, CVE-2016-9904

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (512c0ffd-cd39-4da4-b2dc-81ff4ba8e238)

Observation

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

<http://www.vuxml.org/freebsd/512c0ffd-cd39-4da4-b2dc-81ff4ba8e238.html>

Affected packages:

firefox < 50.1.0_1,1

seamonkey < 2.47

linux-seamonkey < 2.47

firefox-esr < 45.6.0,1

linux-firefox < 45.6.0,2

libxul < 45.6.0

thunderbird < 45.6.0

linux-thunderbird < 45.6.0

182216 - FreeBSD xen-kernel X86 CMPXCHG8B Emulation Fails To Ignore Operand Size Override (80a897a2-c1a6-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-9932

Description

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

xen-kernel -- x86 CMPXCHG8B emulation fails to ignore operand size override (80a897a2-c1a6-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/80a897a2-c1a6-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.1_1

182218 - FreeBSD xen-kernel X86: Mishandling Of SYSCALL Singlestep During Emulation (942433db-c661-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-10013

Description

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

xen-kernel -- x86: Mishandling of SYSCALL singlestep during emulation (942433db-c661-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/942433db-c661-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.1_2

182219 - FreeBSD wordpress Multiple Vulnerabilities (54e50cd9-c1a8-11e6-ae1b-002590263bf5)

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:

wordpress -- multiple vulnerabilities (54e50cd9-c1a8-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/54e50cd9-c1a8-11e6-ae1b-002590263bf5.html>

Affected packages:

wordpress < 4.6.1,1
de-wordpress < 4.6.1
ja-wordpress < 4.6.1
ru-wordpress < 4.6.1
zh-wordpress-zh_CN < 4.6.1
zh-wordpress-zh_TW < 4.6.1

185525 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3158-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2123, CVE-2016-2125, CVE-2016-2126

Description

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

USN-3158-1

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-December/003673.html>

Ubuntu 12.04

samba_3.6.25-0ubuntu0.12.04.5
libsmbclient_3.6.25-0ubuntu0.12.04.5

Ubuntu 16.04

samba_4.3.11+dfsg-0ubuntu0.16.04.3
winbind_4.3.11+dfsg-0ubuntu0.16.04.3
libsmbclient_4.3.11+dfsg-0ubuntu0.16.04.3

Ubuntu 14.04

samba_4.3.11+dfsg-0ubuntu0.14.04.4
libsmbclient_4.3.11+dfsg-0ubuntu0.14.04.4
winbind_4.3.11+dfsg-0ubuntu0.14.04.4

Ubuntu 16.10

winbind_4.4.5+dfsg-2ubuntu5.2
samba_4.4.5+dfsg-2ubuntu5.2
libsmbclient_4.4.5+dfsg-2ubuntu5.2

185532 - Ubuntu Linux 16.10 USN-3156-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

USN-3156-2

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-December/003672.html>

Ubuntu 16.10

apt_1.3.3

191500 - Fedora Linux 25 FEDORA-2016-a815b7bf5d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202, CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a815b7bf5d

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/2016/12/?count=200&page=3>

Fedora Core 25

chromium-55.0.2883.87-1.fc25

191503 - Fedora Linux 25 FEDORA-2016-ca1d1e1dc1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7030, CVE-2016-9575

Description

The scan detected that the host is missing the following update:
FEDORA-2016-ca1d1e1dc1

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/2016/12/?count=200&page=1>

Fedora Core 25

freeipa-4.4.3-1.fc25

191505 - Fedora Linux 24 FEDORA-2016-e5b72816d0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8399

Description

The scan detected that the host is missing the following update:
FEDORA-2016-e5b72816d0

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/2016/12/?count=200&page=2>

Fedora Core 24

kernel-4.8.14-200.fc24

191506 - Fedora Linux 23 FEDORA-2016-e5ff0ed40c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8649

Description

The scan detected that the host is missing the following update:
FEDORA-2016-e5ff0ed40c

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/2016/12/?count=200&page=4>

Fedora Core 23

lxc-2.0.6-2.fc23

191507 - Fedora Linux 24 FEDORA-2016-bd94ef48c8 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-2016-bd94ef48c8

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/2016/12/?count=200&page=3>

Fedora Core 24

firefox-50.1.0-1.fc24

191509 - Fedora Linux 24 FEDORA-2016-a3bc78de2b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9447

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a3bc78de2b

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/2016/12/?count=200&page=3>

Fedora Core 24

gststreamer-plugins-bad-free-0.10.23-34.fc24

191510 - Fedora Linux 25 FEDORA-2016-fbf9f8b204 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9957, CVE-2016-9958, CVE-2016-9959, CVE-2016-9960, CVE-2016-9961

Description

The scan detected that the host is missing the following update:
FEDORA-2016-fbf9f8b204

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/2016/12/?count=200&page=1>

Fedora Core 25

game-music-emu-0.6.1-1.fc25

191511 - Fedora Linux 24 FEDORA-2016-f4e992b0ac Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9808

Description

The scan detected that the host is missing the following update:
FEDORA-2016-f4e992b0ac

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/2016/12/?count=200&page=3>

Fedora Core 24

gstreamer-plugins-good-0.10.31-17.fc24

191512 - Fedora Linux 24 FEDORA-2016-80a2fba8aa Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9844

Description

The scan detected that the host is missing the following update:
FEDORA-2016-80a2fba8aa

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/2016/12/?count=200&page=2>

Fedora Core 24

unzip-6.0-31.fc24

191513 - Fedora Linux 25 FEDORA-2016-c404a59411 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9580, CVE-2016-9581

Description

The scan detected that the host is missing the following update:
FEDORA-2016-c404a59411

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/2016/12/?count=200&page=1>

Fedora Core 25

openjpeg2-2.1.2-3.fc25

191514 - Fedora Linux 25 FEDORA-2016-98cca07999 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

Description

The scan detected that the host is missing the following update:
FEDORA-2016-98cca07999

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/2016/12/?count=200&page=4>

Fedora Core 25

tomcat-8.0.39-1.fc25

191515 - Fedora Linux 23 FEDORA-2016-9c33466fbb Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

Description

The scan detected that the host is missing the following update:
FEDORA-2016-9c33466fbb

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/2016/12/?count=200&page=4>

Fedora Core 23

tomcat-8.0.39-1.fc23

191517 - Fedora Linux 24 FEDORA-2016-a98c560116 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a98c560116

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/2016/12/?count=200&page=4>

Fedora Core 24

tomcat-8.0.39-1.fc24

191518 - Fedora Linux 25 FEDORA-2016-f115a880a6 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-2016-f115a880a6

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/2016/12/?count=200&page=3>

Fedora Core 25

firefox-50.1.0-1.fc25

191519 - Fedora Linux 23 FEDORA-2016-85eae56259 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-2016-85eae56259

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/2016/12/?count=200&page=2>

Fedora Core 23

firefox-50.1.0-1.fc23

191521 - Fedora Linux 24 FEDORA-2016-e0e1cb2b2b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202, CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

Description

The scan detected that the host is missing the following update:
FEDORA-2016-e0e1cb2b2b

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/2016/12/?count=200&page=3>

Fedora Core 24

chromium-55.0.2883.87-1.fc24

191522 - Fedora Linux 25 FEDORA-2016-1b868c23a9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9815, CVE-2016-9816, CVE-2016-9817, CVE-2016-9818, CVE-2016-9913, CVE-2016-9914, CVE-2016-9915, CVE-2016-9916, CVE-2016-9921, CVE-2016-9922, CVE-2016-9932

Description

The scan detected that the host is missing the following update:
FEDORA-2016-1b868c23a9

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/2016/12/?count=200&page=1>

Fedora Core 25

xen-4.7.1-5.fc25

191523 - Fedora Linux 23 FEDORA-2016-7eea952041 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-2016-7eea952041

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/2016/12/?count=200&page=2>

Fedora Core 23

golang-1.5.4-5.fc23

191524 - Fedora Linux 25 FEDORA-2016-3b4de2babd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9844

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3b4de2babd

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/2016/12/?count=200&page=2>

Fedora Core 25

unzip-6.0-31.fc25

191525 - Fedora Linux 23 FEDORA-2016-cc2916dcf4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9637, CVE-2016-9815, CVE-2016-9816, CVE-2016-9817, CVE-2016-9818, CVE-2016-9913, CVE-2016-9914, CVE-2016-9915, CVE-2016-9916, CVE-2016-9921, CVE-2016-9922

Description

The scan detected that the host is missing the following update:
FEDORA-2016-cc2916dcf4

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/2016/12/?count=200&page=2>

Fedora Core 23

xen-4.5.5-5.fc23

191526 - Fedora Linux 25 FEDORA-2016-02db2f32fd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8399

Description

The scan detected that the host is missing the following update:
FEDORA-2016-02db2f32fd

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/2016/12/?count=200&page=2>

Fedora Core 25

kernel-4.8.14-300.fc25

175056 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1612-10082)

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

Risk Level: Low

CVE: CVE-2016-1981, CVE-2016-3712

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1612-10082)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=10082>

SL7
x86_64
qemu-kvm-1.5.3-126.el7
qemu-kvm-debuginfo-1.5.3-126.el7
qemu-img-1.5.3-126.el7
qemu-kvm-tools-1.5.3-126.el7
qemu-kvm-common-1.5.3-126.el7

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.

3884 - w3who.dll ISAPI Buffer Overflow

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

Risk Level: High

CVE: CVE-2004-1133, CVE-2004-1134

Update Details

Recommendation is updated

4754 - NetGear Wireless Driver Long Beacon Stack Overflow

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

Risk Level: High

CVE: CVE-2006-5972

Update Details

Recommendation is updated

5495 - Sun JRE isInstalled.dnsResolve Overflow

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

Risk Level: High

CVE: CVE-2007-5019

[Update Details](#)

Recommendation is updated

5526 - Symantec Veritas Backup Exec For Windows Servers Unspecified Vulnerability

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

Risk Level: High

CVE: CVE-2007-5126

[Update Details](#)

Recommendation is updated

5656 - RealNetworks RealPlayer Unspecified Buffer Overflow

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

Risk Level: High

CVE: CVE-2008-0098

[Update Details](#)

Recommendation is updated

8724 - Unix Finger Service User Account Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

CVE: CVE-1999-0198

[Update Details](#)

Recommendation is updated

8725 - Unix Finger User Account Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

CVE: CVE-1999-0197

[Update Details](#)

Recommendation is updated

9815 - SMTP Server Too Long Line Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

10672 - GIGABYTE Dldrv2 ActiveX Control Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2010-1517, CVE-2010-1518

[Update Details](#)

Recommendation is updated

12097 - Quest Software Big Brother Arbitrary File Deletion Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12188 - HP 3COM/H3C Intelligent Management Center Img Recv Remote Code Execution

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

Risk Level: High

CVE: CVE-2011-2331

[Update Details](#)

Recommendation is updated

14076 - Windows Explorer BMP File Handling Vulnerability

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

Risk Level: High

CVE: CVE-2007-1946

[Update Details](#)

Recommendation is updated

19849 - Solarwinds Dameware Mini Remote Control Stack Based Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2016-2345

[Update Details](#)

Recommendation is updated Documentation is updated

20726 - Oracle MySQL Server Critical Patch Update October 2016

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-3495, CVE-2016-5507, CVE-2016-5584, CVE-2016-5609, CVE-2016-5612, CVE-2016-5624, CVE-2016-5625, CVE-2016-5626, CVE-2016-5627, CVE-2016-5628, CVE-2016-5629, CVE-2016-5630, CVE-2016-5631, CVE-2016-5632, CVE-2016-5633, CVE-2016-5634, CVE-2016-5635, CVE-2016-6304, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-7440, CVE-2016-8283, CVE-2016-8284, CVE-2016-8286, CVE-2016-8287, CVE-2016-8288, CVE-2016-8289, CVE-2016-8290

[Update Details](#)

CVE is updated

21022 - (APSB16-39) Vulnerabilities In Adobe Flash Player

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-7867, CVE-2016-7868, CVE-2016-7869, CVE-2016-7870, CVE-2016-7871, CVE-2016-7872, CVE-2016-7873, CVE-2016-7874, CVE-2016-7875, CVE-2016-7876, CVE-2016-7877, CVE-2016-7878, CVE-2016-7879, CVE-2016-7880, CVE-2016-7881, CVE-2016-7890, CVE-2016-7892

[Update Details](#)

Risk is updated

21024 - (APSB16-39) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7867, CVE-2016-7868, CVE-2016-7869, CVE-2016-7870, CVE-2016-7871, CVE-2016-7872, CVE-2016-7873, CVE-2016-7874, CVE-2016-7875, CVE-2016-7876, CVE-2016-7877, CVE-2016-7878, CVE-2016-7879, CVE-2016-7880, CVE-2016-7881, CVE-2016-7890, CVE-2016-7892

[Update Details](#)

Risk is updated

141313 - Red Hat Enterprise Linux RHSA-2016-2131 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

CVE is updated

141316 - Red Hat Enterprise Linux RHSA-2016-2130 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-8283

[Update Details](#)

CVE is updated

141322 - Red Hat Enterprise Linux RHSA-2016-2595 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

CVE is updated

141364 - Red Hat Enterprise Linux RHSA-2016-2749 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5507, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-8283

[Update Details](#)

CVE is updated

141379 - Red Hat Enterprise Linux RHSA-2016-2928 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

CVE is updated

141380 - Red Hat Enterprise Linux RHSA-2016-2927 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-5630, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

CVE is updated

144991 - SuSE Linux 13.2 openSUSE-SU-2016:2769-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-3459, CVE-2016-3477, CVE-2016-3486, CVE-2016-3492, CVE-2016-3501, CVE-2016-3521, CVE-2016-3614, CVE-2016-3615, CVE-2016-5439, CVE-2016-5440, CVE-2016-5507, CVE-2016-5584, CVE-2016-5609, CVE-2016-5612, CVE-2016-5626, CVE-2016-5627, CVE-2016-5629, CVE-2016-5630, CVE-2016-6304, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-7440, CVE-2016-8283, CVE-2016-8284, CVE-2016-8288

[Update Details](#)

CVE is updated

163199 - Oracle Enterprise Linux ELSA-2016-2595 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

[Update Details](#)

CVE is updated

800 - Sambar Server Unauthorized Admin Access

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

1117 - Savant Web Server Buffer Overflow

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

Risk Level: High

CVE: CVE-2000-0641, CVE-2001-0433, CVE-2002-1120

[Update Details](#)

Recommendation is updated

3393 - CCBill Arbitrary Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

3395 - Tammie Ad.CGI Remote Arbitrary Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2001-0025, CVE-2005-1350, CVE-2005-1351, CVE-2005-1352

[Update Details](#)

Recommendation is updated

5836 - Microsoft Works WklmgSrv.dll ActiveX Vulnerability

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

Risk Level: High

CVE: CVE-2008-1898

Update Details

Recommendation is updated

5899 - Creative Software AutoUpdate Engine ActiveX Control Stack Overflow

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

Risk Level: High

CVE: CVE-2008-0955

Update Details

Recommendation is updated

7256 - HP LoadRunner XUpload.ocx ActiveX Control Arbitrary File Download

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

Risk Level: High

CVE: CVE-2009-3693

Update Details

Recommendation is updated

7638 - Oracle Document Capture EasyMail ActiveX Control Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2007-4607

Update Details

Recommendation is updated

7930 - Oracle Times-Ten In-Memory Database Denial Of Service Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

8942 - Nginx HTTP Server File Path Parse Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

9603 - Oracle Application Server Arbitrary File Access Vulnerability

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

Risk Level: High

CVE: CVE-2001-0326

[Update Details](#)

Recommendation is updated

9635 - Oracle Application Server dbsnmp And nmo Programs Privilege Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2004-1707

[Update Details](#)

Recommendation is updated

9670 - Wind River Systems VxWorks WDB Target Agent Debug Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2010-2965

[Update Details](#)

Recommendation is updated

9743 - FutureSoft TFTP Server 2000 Remote Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

9831 - TFTPUtil GUI Long Transport Mode Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2010-2028

[Update Details](#)

Recommendation is updated

9835 - ProSysInfo TFTP Server TFTPWIN Long File Name Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2006-4948

[Update Details](#)

Recommendation is updated

10088 - GuildFTPd LIST and CWD Commands Heap Overflow Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2008-4572

[Update Details](#)

Recommendation is updated

10129 - Open&Compact FTP Server Authentication Bypass Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2010-2620

[Update Details](#)

Recommendation is updated

10145 - Open&Compact FTP Server Multiple Buffer Overflow Vulnerabilities

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

10533 - HP Web Jetadmin Remote Information Disclosure Vulnerability

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

Risk Level: High

CVE: CVE-2009-4182

[Update Details](#)

Recommendation is updated

13370 - Novell GroupWise Messenger nmma.exe Login Memory Corruption Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13371 - Novell GroupWise Messenger nmma.exe Arbitrary Memory Corruption Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13456 - Cisco Linksys PlayerPT ActiveX Control SetSource Stack Overflow

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

Risk Level: High

CVE: CVE-2012-0284

[Update Details](#)

Recommendation is updated

13622 - (MS12-034) Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)

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

Risk Level: High

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0164, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848

[Update Details](#)

Recommendation is updated

13624 - (MS12-034) Microsoft Silverlight Double Free Remote Code Execution (2681578)

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

Risk Level: High

CVE: CVE-2012-0176

[Update Details](#)

Recommendation is updated

13625 - (MS12-034) Microsoft Windows .NET Buffer Allocation Remote Code Execution (2681578)

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

Risk Level: High

CVE: CVE-2012-0162

[Update Details](#)

Recommendation is updated

13629 - (MS12-034) Microsoft Windows GDI+ Heap Overflow Remote Code Execution (2681578)

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

Risk Level: High

CVE: CVE-2012-0167

[Update Details](#)

Recommendation is updated

13630 - (MS12-034) Microsoft Windows GDI+ Record Remote Code Execution (2681578)

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

Risk Level: High

CVE: CVE-2012-0165

[Update Details](#)

Recommendation is updated

13631 - (MS12-034) Microsoft Windows TrueType Font Parsing II (2681578)

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

Risk Level: High

CVE: CVE-2012-0159

[Update Details](#)

Recommendation is updated

13632 - (MS12-034) Microsoft Windows TrueType Font Parsing (2681578)

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

Risk Level: High

CVE: CVE-2011-3402

[Update Details](#)

Recommendation is updated

13633 - (MS12-035) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)

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

Risk Level: High

CVE: CVE-2012-0160, CVE-2012-0161

[Update Details](#)

Recommendation is updated

13634 - (MS12-035) Microsoft Windows .NET Deserialization Remote Code Execution (2696777)

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

Risk Level: High

CVE: CVE-2012-0161

Update Details

Recommendation is updated

13635 - (MS12-035) Microsoft Windows .NET Serialization Remote Code Execution (2693777)

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

Risk Level: High

CVE: CVE-2012-0160

Update Details

Recommendation is updated

13733 - Tftpd32 DNS Server Denial Of Service Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

13831 - PHP com_print_typeinfo Function Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-2012-2376

Update Details

Recommendation is updated

14095 - Oracle Business Transaction Management Server FlashTunnelService Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14181 - Oracle Business Transaction Management SOAP Web Service Directory Traversal Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14250 - QNX FTPD Denial of Service

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14324 - RealNetworks RealPlayer 3GP File Handling Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14452 - Sunsolve sscd_suncourier.pl Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2002-0436

[Update Details](#)

Recommendation is updated

14515 - VideoLAN VLC Media Player SWF File Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

15010 - Schneider Electric Vijeo Web Gate Server Denial Of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

15243 - (MS13-052) Microsoft Windows .NET Anonymous Method Injection Remote Code Execution (2861561)

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

Risk Level: High

CVE: CVE-2013-3133

[Update Details](#)

Recommendation is updated

15244 - (MS13-052) Microsoft Windows .NET And Silverlight Array Access Remote Code Execution (2861561)

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

Risk Level: High

CVE: CVE-2013-3131

[Update Details](#)

Recommendation is updated

15245 - (MS13-052) Microsoft Windows .NET And Silverlight Array Allocation Remote Code Execution (2861561)

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

Risk Level: High

CVE: CVE-2013-3134

[Update Details](#)

Recommendation is updated

15247 - (MS13-052) Microsoft Windows .NET Delegate Reflection Remote Code Execution (2861561)

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

Risk Level: High

CVE: CVE-2013-3132

[Update Details](#)

Recommendation is updated

15248 - (MS13-052) Microsoft .NET Framework Delegate Serialization Remote Code Execution (2861561)

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

Risk Level: High

CVE: CVE-2013-3171

[Update Details](#)

Recommendation is updated

15249 - (MS13-052) Microsoft Windows Silverlight Null Pointer Remote Code Execution (2861561)

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

Risk Level: High

CVE: CVE-2013-3178

Update Details

Recommendation is updated

15250 - (MS13-052) Microsoft Windows .NET And Silverlight TrueType Font Parsing Remote Code Execution (2861561)

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

Risk Level: High

CVE: CVE-2013-3129

Update Details

Recommendation is updated

15252 - (MS13-052) Vulnerabilities In .NET Framework And Silverlight Could Allow Remote Code Execution (2861561)

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

Risk Level: High

CVE: CVE-2013-3129, CVE-2013-3131, CVE-2013-3132, CVE-2013-3133, CVE-2013-3134, CVE-2013-3171, CVE-2013-3178

Update Details

Recommendation is updated

15303 - MOXA AWK Search Utility Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

15311 - Multiple BMC Implementation IPMI Cipher Suite 0 Security Bypass Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2013-4782, CVE-2013-4783, CVE-2013-4784

Update Details

Recommendation is updated

15728 - (MS13-082) Vulnerabilities In .NET Framework Could Allow Remote Code Execution (2878890)

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

Risk Level: High

CVE: CVE-2013-3128, CVE-2013-3860, CVE-2013-3861

[Update Details](#)

Recommendation is updated

15780 - EATON VURemote Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

15782 - Moore Industries NCS Configuration Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

15960 - Symantec Workspace Streaming EJInvokerServlet / JMXInvokerServlet Marshalled Object Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

15975 - Microsoft Word Embedded Image Fork Bomb Denial of Service

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

Risk Level: High

CVE: CVE-2013-6801

[Update Details](#)

Recommendation is updated

16258 - Eaton Network Shutdown Module Pi3Web WebServer Denial of Service

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16445 - Delta Electronics WPLSoft DVPSimulator.exe Buffer Overflow Remote Code Execution

Category: General Vulnerability Assessment -> Intrusive -> SCADA

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16620 - Paessler PRTG Network Monitor Server.exe Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16628 - FrameFlow Server Monitor Unspecified Defect Denial Of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16632 - VideoLAN VLC Media Player libpng_plugin.dll Denial of Service

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

Risk Level: High

CVE: CVE-2014-3441

[Update Details](#)

Recommendation is updated

16641 - Nullsoft Winamp Malformed .FLV File Remote Code Execution

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

Risk Level: High

CVE: CVE-2014-3442

Update Details

Recommendation is updated

16648 - RealNetworks RealPlayer GetGUID Function Remote Code Execution

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

Risk Level: High

CVE: CVE-2014-3444

[Update Details](#)

Recommendation is updated

16767 - Novell ZENworks Unspecified Defect Remote Code Execution II

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16768 - Novell ZENworks Unspecified Defect Remote Code Execution I

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17353 - Emerson ROCLINK 800 arpro2.dll ActiveX Control Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17429 - WordPress Media File Renamer Plugin Cross-Site Scripting Vulnerability

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

Risk Level: High

CVE: CVE-2014-2040

[Update Details](#)

Recommendation is updated

17539 - Z-Scada Net Unspecified Defect Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

17550 - SAP Netweaver Enqueue Server Trace Pattern Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

17564 - (SOL15910) F5 BIG-IP Linux Kernel SCTP Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687

Update Details

Recommendation is updated Documentation is updated

17588 - Microsys Promotic TrendsViewCtl Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

17621 - Hewlett Packard Vertica Monitor Thread Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

17858 - Phoenix Contact Software ProConOs MultiProg Protocol Compliant Traffic Remote Code Execution

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

Risk Level: High
CVE: CVE-2014-9195

[Update Details](#)

Recommendation is updated

18063 - Cogent DataHub Web Server Gamma Injection Remote Code Execution

Category: General Vulnerability Assessment -> Intrusive -> SCADA
Risk Level: High
CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated Documentation is updated

18064 - Cogent DataHub Web Server Gamma Injection Remote Code Execution

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated Documentation is updated

18085 - MODX Evolution Unspecified Defect Remote Code Execution

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server
Risk Level: High
CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18228 - Tibbo Systems AggreGate XML External Entity Denial of Service

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA
Risk Level: High
CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18269 - (MS15-044) Vulnerabilities in GDI+ Could Allow Remote Code Execution (3057110)

Category: Windows Host Assessment -> Patches Only
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2015-1670, CVE-2015-1671

[Update Details](#)

Recommendation is updated

18306 - (MS15-044) Microsoft Windows GDI+ TrueType Font Parsing Remote Code Execution (3057110)

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

Risk Level: High

CVE: CVE-2015-1671

[Update Details](#)

Recommendation is updated

18335 - (MS15-044) Microsoft Windows GDI+ TrueType Font Parsing Remote Code Execution (3057110)

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

Risk Level: High

CVE: CVE-2015-1671

[Update Details](#)

Recommendation is updated

18524 - (SOL16715) F5 BIG-IP Multiple libTIFF Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2013-1960, CVE-2013-1961, CVE-2013-4231, CVE-2013-4232, CVE-2013-4243, CVE-2013-4244

[Update Details](#)

Recommendation is updated Documentation is updated

18782 - (MS15-080) Microsoft Office Graphics Component Remote Code Execution (3078662)

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

Risk Level: High

CVE: CVE-2015-2431

[Update Details](#)

Recommendation is updated

18783 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution I (3078662)

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

Risk Level: High

CVE: CVE-2015-2432

[Update Details](#)

Recommendation is updated

18784 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution I (3078662)

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

Risk Level: High

CVE: CVE-2015-2435

Update Details

Recommendation is updated

18785 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution II (3078662)

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

Risk Level: High

CVE: CVE-2015-2455

Update Details

Recommendation is updated

18786 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution III (3078662)

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

Risk Level: High

CVE: CVE-2015-2456

Update Details

Recommendation is updated

18787 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution II (3078662)

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

Risk Level: High

CVE: CVE-2015-2458

Update Details

Recommendation is updated

18788 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution III (3078662)

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

Risk Level: High

CVE: CVE-2015-2459

Update Details

Recommendation is updated

18789 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution IV (3078662)

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

Risk Level: High
CVE: CVE-2015-2460

[Update Details](#)

Recommendation is updated

18790 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution V (3078662)

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

Risk Level: High
CVE: CVE-2015-2461

[Update Details](#)

Recommendation is updated

18791 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution VI (3078662)

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

Risk Level: High
CVE: CVE-2015-2462

[Update Details](#)

Recommendation is updated

18792 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution IV (3078662)

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

Risk Level: High
CVE: CVE-2015-2463

[Update Details](#)

Recommendation is updated

18793 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution V (3078662)

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

Risk Level: High
CVE: CVE-2015-2464

[Update Details](#)

Recommendation is updated

18805 - (MS15-080) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)

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

Risk Level: High
CVE: CVE-2015-2431, CVE-2015-2432, CVE-2015-2433, CVE-2015-2435, CVE-2015-2453, CVE-2015-2454, CVE-2015-2455, CVE-

2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464, CVE-2015-2465

Update Details

Recommendation is updated

18810 - (MS15-080) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)

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

Risk Level: High

CVE: CVE-2015-2431, CVE-2015-2432, CVE-2015-2433, CVE-2015-2435, CVE-2015-2453, CVE-2015-2454, CVE-2015-2455, CVE-2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464, CVE-2015-2465

Update Details

Recommendation is updated

18873 - (SOL17079) F5 BIG-IP Java SE Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-2590, CVE-2015-4732

Update Details

Documentation is updated

18907 - (SOL17173) F5 BIG-IP OpenJDK Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-4760

Update Details

Recommendation is updated Documentation is updated

19334 - (MS15-128) Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)

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

Risk Level: High

CVE: CVE-2015-6106, CVE-2015-6107, CVE-2015-6108

Update Details

Recommendation is updated

19336 - (MS15-128) Microsoft Windows Graphics Memory Corruption Remote Code Execution II (3104503)

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

Risk Level: High

CVE: CVE-2015-6107

[Update Details](#)

Recommendation is updated

19337 - (MS15-128) Microsoft Windows Graphics Memory Corruption Remote Code Execution III (3104503)

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

Risk Level: High

CVE: CVE-2015-6108

[Update Details](#)

Recommendation is updated

19338 - (MS15-128) Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)

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

Risk Level: High

CVE: CVE-2015-6106, CVE-2015-6107, CVE-2015-6108

[Update Details](#)

Recommendation is updated

19556 - (SOL30518307) F5 BIG-IP Java Commons Collections Library Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-4852

[Update Details](#)

Recommendation is updated Documentation is updated

19899 - (MS16-039) Security Update for Microsoft Graphics Component (3148522)

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

Risk Level: High

CVE: CVE-2016-0143, CVE-2016-0145, CVE-2016-0165, CVE-2016-0167

[Update Details](#)

Recommendation is updated

19909 - (MS16-039) Microsoft Windows Win32k Graphics Privilege Escalation III (3148522)

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

Risk Level: High

CVE: CVE-2016-0167

[Update Details](#)

Recommendation is updated

19910 - (MS16-039) Microsoft Windows Graphics Memory Remote Code Execution (3148522)

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

Risk Level: High

CVE: CVE-2016-0145

Update Details

Recommendation is updated

20452 - Cisco Adaptive Security Appliance SNMP Remote Code Execution

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-6366

Update Details

Recommendation is updated Documentation is updated

21010 - (MS16-148) Security Update for Microsoft Office (3204068)

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

Risk Level: High

CVE: CVE-2016-7257, CVE-2016-7262, CVE-2016-7263, CVE-2016-7264, CVE-2016-7265, CVE-2016-7266, CVE-2016-7267, CVE-2016-7268, CVE-2016-7275, CVE-2016-7276, CVE-2016-7277, CVE-2016-7289, CVE-2016-7290, CVE-2016-7291, CVE-2016-7298, CVE-2016-7300

Update Details

Risk is updated

21011 - (MS16-148) Security Update for Microsoft Office (3204068)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7257, CVE-2016-7262, CVE-2016-7263, CVE-2016-7264, CVE-2016-7265, CVE-2016-7266, CVE-2016-7267, CVE-2016-7268, CVE-2016-7275, CVE-2016-7276, CVE-2016-7277, CVE-2016-7289, CVE-2016-7290, CVE-2016-7291, CVE-2016-7298, CVE-2016-7300

Update Details

Risk is updated

32452 - Oracle Solaris 122259-09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-6725, CVE-2008-6679, CVE-2009-0196, CVE-2009-0583, CVE-2009-0584, CVE-2009-0792, CVE-2009-4270, CVE-2010-1628, CVE-2010-1869, CVE-2010-2055, CVE-2010-4054, CVE-2011-4516, CVE-2011-4517

Update Details

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

32454 - Oracle Solaris 122260-09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-6725, CVE-2008-6679, CVE-2009-0196, CVE-2009-0583, CVE-2009-0584, CVE-2009-0792, CVE-2009-4270, CVE-2010-1628, CVE-2010-1869, CVE-2010-2055, CVE-2010-4054, CVE-2011-4516, CVE-2011-4517

Update Details

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

182017 - FreeBSD p7zip Heap Overflow Vulnerability (a9bcaf57-4a7b-11e6-97f7-5453ed2e2b49)

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

Risk Level: High

CVE: CVE-2016-2334

Update Details

Risk is updated

645 - Netscape Enterprise Server 3.6 SP2 Authentication Overflow

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

Risk Level: High

CVE: CVE-1999-0853

Update Details

Recommendation is updated

772 - Netscape FastTrack Authentication Buffer Overflow

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

Risk Level: High

CVE: CVE-1999-0853

Update Details

Recommendation is updated

934 - csMailto.cgi Command Execution

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

Risk Level: High

CVE: CVE-2002-0749

Update Details

Recommendation is updated

3767 - Upload Lite Arbitrary File Upload and Execution Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

4040 - W3Who Buffer Overflow

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

Risk Level: High

CVE: CVE-2004-1133, CVE-2004-1134

[Update Details](#)

Recommendation is updated

4319 - GAMSoft TelSrv Long Username Denial of Service

Category: General Vulnerability Assessment -> Intrusive -> UNIX

Risk Level: High

CVE: CVE-1999-0230, CVE-2000-0166, CVE-2000-0480, CVE-2000-0665, CVE-2001-0348

[Update Details](#)

Observation is updated Recommendation is updated

5064 - Microsoft Word wplib.dll Heap Buffer Overflow

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

Risk Level: High

CVE: CVE-2007-1910

[Update Details](#)

Recommendation is updated

7278 - Oracle Document Capture BlackIce DEVMODE ActiveX Control Remote Command Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

10694 - WordPress Plugin fGallery SQL Injection Vulnerability

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

Risk Level: High

CVE: CVE-2008-0491

[Update Details](#)

Recommendation is updated

12012 - WordPress SocialGrid Plugin "default_services" Cross-Site Scripting Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12135 - WordPress Magazine Theme Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12708 - Sunway ForceControl YRWXIs.ocx ActiveX Control Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12821 - OPC Systems.NET OPCSystemsService Denial Of Service Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12842 - Snort Report target Multiple Remote Command Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14154 - EMC AutoStart Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14158 - EMC AlphaStor Remote Code Execution

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14260 - CYME Power Engineering ChartFX Client Server ActiveX Control Array Indexing Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14455 - WordPress AdWizz Plugin "link" Cross-Site Scripting Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14806 - HMS Netbiter Config Utility Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

15105 - MOXA Mass Configuration Tool Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17354 - NOVUS NConfig Configurator Unspecified Defect Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17355 - Moxa MXview Java Applet Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17417 - Microsys Promotic Visual Basic Code Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17966 - (SOL16122) F5 BIG-IP Linux Kernel Local Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-9322

[Update Details](#)

Recommendation is updated Documentation is updated

18218 - (SOL16383) F5 BIG-IP Linux RPM Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2013-6435

[Update Details](#)

Recommendation is updated Documentation is updated

18711 - (SOL16900) F5 BIG-IP FreeType Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-9657, CVE-2014-9658, CVE-2014-9660, CVE-2014-9661, CVE-2014-9663, CVE-2014-9664, CVE-2014-9667, CVE-2014-9669, CVE-2014-9670, CVE-2014-9671, CVE-2014-9673, CVE-2014-9674, CVE-2014-9675

[Update Details](#)

Documentation is updated

18855 - (SOL17123) F5 BIG-IP Apache Tomcat Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-0230

[Update Details](#)

Documentation is updated

761 - PowerFTP Personal FTP Server Path Disclosure

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2001-0934

[Update Details](#)

Recommendation is updated

780 - WebSitePro win-c-sample.exe Path Disclosure

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

Risk Level: High

CVE: CVE-1999-0178

[Update Details](#)

Recommendation is updated

852 - Oracle9iAS XSQLServlet XSQLConfig.xml disclosure

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

Risk Level: High

CVE: CVE-2002-0568, CVE-2002-0569

[Update Details](#)

Recommendation is updated

884 - Oracle WebDB Admin Backdoor Unauthorized Access

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

933 - Oracle TNS Listener Anonymous Access Allowed

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2002-0567

Update Details

Recommendation is updated

956 - Compaq Web-Based Management default page

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

Risk Level: High

CVE: CVE-2001-0374

Update Details

Recommendation is updated

3048 - Morpheus FastTrack Service Identity Spoofing Vulnerability

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

Risk Level: High

CVE: CVE-2002-0314, CVE-2002-0315

Update Details

Recommendation is updated

3382 - Campas CGI Script Information Leakage Vulnerability

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

Risk Level: High

CVE: CVE-1999-0146

Update Details

Recommendation is updated

3768 - PHP Uploader CGI Application Arbitrary File Upload Vulnerability

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

Risk Level: High

CVE: CVE-2003-1552

Update Details

Recommendation is updated

3774 - Webcom Rguest Arbitrary File Disclosure Vulnerability

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

Risk Level: High

CVE: CVE-1999-0287, CVE-1999-0467

[Update Details](#)

Recommendation is updated

4270 - Network Tools for PHP-Nuke hostinput Vulnerability

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

Risk Level: High

CVE: CVE-2001-0899

[Update Details](#)

Recommendation is updated

4334 - W3C httpd Physical Path Disclosure

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

Risk Level: High

CVE: CVE-2000-0079

[Update Details](#)

Recommendation is updated

4339 - MSN ActiveX Setup BBS Buffer Overflow

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

Risk Level: High

CVE: CVE-1999-1484

[Update Details](#)

Recommendation is updated

4835 - Oracle Portal HTTP Response Splitting

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

Risk Level: High

CVE: CVE-2006-6697, CVE-2006-6699, CVE-2006-6703

[Update Details](#)

Recommendation is updated

4984 - FactoSystem Weblog Multiple SQL Injection Vulnerabilities

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

Risk Level: High

CVE: CVE-2002-1499

[Update Details](#)

Recommendation is updated

5218 - Microsoft Windows XP GDI+ .ICO Handling DoS Vulnerability

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

Risk Level: High

CVE: CVE-2007-2237

Update Details

Recommendation is updated

5469 - VMware vstor-ws60.sys Vulnerability

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

Risk Level: High

CVE: CVE-2007-4591, CVE-2007-4593

Update Details

Recommendation is updated

8716 - XAMPP Insecure Default Password Disclosure Vulnerability

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

Risk Level: High

CVE: CVE-2005-1078

Update Details

Recommendation is updated

8764 - Perforce Server Multiple Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2010-0929, CVE-2010-0930, CVE-2010-0931, CVE-2010-0932, CVE-2010-0933, CVE-2010-0934, CVE-2010-0935

Update Details

Recommendation is updated

8800 - Open Flash Chart PHP Library Arbitrary File Creation Vulnerability

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

Risk Level: High

CVE: CVE-2009-4140

Update Details

Recommendation is updated

9865 - Network Associates WebShield SMTP Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2000-0447

[Update Details](#)

Recommendation is updated

9945 - gIFTPd Default Credentials Unauthorized Access Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> UNIX

Risk Level: High

CVE: CVE-1999-0502

[Update Details](#)

Recommendation is updated

10204 - Webcom Guestbook.cgi Arbitrary Command Execution Vulnerability

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

Risk Level: High

CVE: CVE-1999-0237

[Update Details](#)

Recommendation is updated

11430 - Microsoft Malware Protection Engine Privilege Elevation (2491888)

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

Risk Level: High

CVE: CVE-2011-0037

[Update Details](#)

FASLScript is updated

11610 - WordPress Rating-Widget Plugin Multiple Cross-Site Scripting Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12577 - HP SiteScope Default Credentials Weaknesses

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12709 - Sunway ForceControl SCADA SNMP NetDBServer Integer Signedness Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12798 - Sunway ForceControl SNMP NetDBServer Stack Buffer Overflow Remote Code Execution

Category: General Vulnerability Assessment -> Intrusive -> SCADA

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12875 - Oracle AutoVue AutoVueX ActiveX Control Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12876 - Oracle AutoVue AutoVueX ActiveX Control ExportEdaBom Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12877 - Oracle AutoVue AutoVueX ActiveX Control Export3DBom Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12924 - Oracle DataDirect Multiple Native Wire Protocol ODBC Driver Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12929 - HP Data Protector Media Operations Directory Traversal Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12930 - HP Data Protector Media Operations Heap Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13182 - CoCSoft Stream Down Response Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-2011-5052

[Update Details](#)

Recommendation is updated

13626 - (MS12-034) Microsoft Windows Scrollbar Calculation Privilege Escalation (2681578)

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

Risk Level: High

CVE: CVE-2012-1848

[Update Details](#)

Recommendation is updated

13627 - (MS12-034) Microsoft Windows Keyboard Layout Privilege Escalation (2681578)

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

Risk Level: High

CVE: CVE-2012-0181

[Update Details](#)

Recommendation is updated

13628 - (MS12-034) Microsoft Windows And Messages Privilege Escalation (2681578)

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

Risk Level: High

CVE: CVE-2012-0180

[Update Details](#)

Recommendation is updated

13735 - Microsoft Wordpad Doc File Null Pointer Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16205 - HP 2620 Switches /html/json.html Admin Account Manipulation Cross-Site Request Forgery

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: High

CVE: CVE-2013-6852

[Update Details](#)

Recommendation is updated

17473 - (SOL15867) F5 BIG-IP Multiple Perl Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2012-5195, CVE-2012-5526, CVE-2012-6329, CVE-2013-1667

[Update Details](#)

Recommendation is updated Documentation is updated

17666 - VideoLan VLC Media Player libavcodec Two Remote Code Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-2014-9597, CVE-2014-9598

[Update Details](#)

Recommendation is updated

18903 - VideoLAN VLC Media Player 3GP File Arbitrary Pointer Dereference Vulnerability

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

Risk Level: High

CVE: CVE-2015-5949

[Update Details](#)

Recommendation is updated

19051 - (SOL17263) F5 BIG-IP OpenSSH Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-6563, CVE-2015-6564

[Update Details](#)

Documentation is updated

19310 - TECO JN5 DriveLink LF5 File Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

19313 - TECO AP-PCLINK TPC File Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

19315 - TECO SG2 Client Multiple Remote Code Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

19316 - TECO TP3-PCLINK TPC File Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

19493 - (SOL05770600) F5 BIG-IP Linux Libuser Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-3245, CVE-2015-3246

Update Details

Documentation is updated

19584 - (SOL31026324) F5 BIG-IP Linux Kernel Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-2925, CVE-2015-5307, CVE-2015-8104

Update Details

Recommendation is updated Documentation is updated

19606 - West Control Solutions BlueControl Insecure Library Loading Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

20975 - (MS16-151) Security Update for Windows Kernel-Mode Drivers (3205651)

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

Risk Level: High

CVE: CVE-2016-7259, CVE-2016-7260

Update Details

Risk is updated

20978 - (MS16-149) Security Update for Microsoft Windows (3205655)

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

Risk Level: High

CVE: CVE-2016-7219, CVE-2016-7292

[Update Details](#)

Risk is updated

20993 - (MS16-145) Cumulative Security Update for Microsoft Edge (3204062)

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

Risk Level: High

CVE: CVE-2016-7181, CVE-2016-7206, CVE-2016-7279, CVE-2016-7280, CVE-2016-7281, CVE-2016-7282, CVE-2016-7286, CVE-2016-7287, CVE-2016-7288, CVE-2016-7296, CVE-2016-7297

[Update Details](#)

Risk is updated

88721 - Slackware Linux 14.1 SSA:2015-328-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3210

[Update Details](#)

Risk is updated

181434 - FreeBSD pcre Multiple Vulnerabilities (e69af246-0ae2-11e5-90e4-d050996490d0)

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

Risk Level: High

CVE: CVE-2015-3210, CVE-2015-3217

[Update Details](#)

Risk is updated

182129 - FreeBSD X.org libraries Multiple Vulnerabilities (1cf65085-a760-41d2-9251-943e1af62eb8)

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

Risk Level: High

CVE: CVE-2016-5407

[Update Details](#)

Risk is updated

189503 - Fedora Linux 22 FEDORA-2015-11027 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3210, CVE-2015-5073

[Update Details](#)

Risk is updated

189634 - Fedora Linux 22 FEDORA-2015-12921 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3210, CVE-2015-5073

Update Details

Risk is updated

191232 - Fedora Linux 25 FEDORA-2016-f71cc44cf8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5407

Update Details

Risk is updated

191254 - Fedora Linux 24 FEDORA-2016-5aa206bd16 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5407

Update Details

Risk is updated

191317 - Fedora Linux 23 FEDORA-2016-3b41a9eaa8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5407

Update Details

Risk is updated

762 - PowerFTP Personal FTP Server Directory Disclosure

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2002-1544

Update Details

Recommendation is updated

763 - PowerFTP Personal FTP Server Tilde Denial-of-Service

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

842 - Oracle9i HTTP Server Java Source Disclosure

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

Risk Level: Medium

CVE: CVE-2002-0565

[Update Details](#)

Recommendation is updated

859 - Compaq Survey Utility Anonymous Login

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

Risk Level: Medium

CVE: CVE-1999-0771

[Update Details](#)

Recommendation is updated

935 - FormMail.pl Detected

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

Risk Level: Medium

CVE: CVE-2001-0357

[Update Details](#)

Recommendation is updated

1039 - Omnicron OmniHTTPd Long Request Buffer Overflow

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

Risk Level: Medium

CVE: CVE-2001-0613

[Update Details](#)

Recommendation is updated

1041 - MyWebServer Buffer Overflow

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

Risk Level: Medium

CVE: CVE-2002-1003

[Update Details](#)

Recommendation is updated

3052 - Grokster FastTrack P2P Supernode Packet Handler Buffer Overrun

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0397

[Update Details](#)

Recommendation is updated

3054 - Morpheus FastTrack P2P Supernode Packet Handler Buffer Overrun

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2003-0397

[Update Details](#)

Recommendation is updated

4335 - PowerScripts PlusMail CGI password file Vulnerability

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

Risk Level: Medium

CVE: CVE-2000-0074

[Update Details](#)

Recommendation is updated

5579 - Viewpoint Media Player AxMetaStream ActiveX Stack Overflow

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-5911

[Update Details](#)

Recommendation is updated

6242 - Microsoft Windows Vista TCP/IP Buffer Overflow Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-5229

[Update Details](#)

Recommendation is updated

6566 - Mozilla Firefox 'Libxul' Denial-of-Service Vulnerability

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-5822

[Update Details](#)

Recommendation is updated

6567 - Mozilla Firefox location.hash Denial-of-Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2008-5715

[Update Details](#)

Recommendation is updated

8205 - Sendmail Long IDENT Logging Circumvention Weakness Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

CVE: CVE-2002-2423

[Update Details](#)

Recommendation is updated

9048 - Microsoft Windows Remote Desktop Protocol mstlsapi.dll Private Key Spoofing Vulnerability

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

Risk Level: Medium

CVE: CVE-2005-1794

[Update Details](#)

Recommendation is updated

9338 - Microsoft IIS ASP .NET NULL Character Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2003-0768

[Update Details](#)

Recommendation is updated

9525 - Cisco IOS Virtual LAN 802.1q Frame Injection Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-1999-1129

[Update Details](#)

Recommendation is updated

9534 - Cisco IOS Large TCP Scan Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2002-2052

[Update Details](#)

Recommendation is updated

9563 - Cisco IOS Firewall/IPS Functionality HTTP Unicode Encoding Detection Security Bypass Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2007-2688

[Update Details](#)

Recommendation is updated

9597 - Oracle Application Server query.xsql Sample Page SQL Injection Vulnerability

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

Risk Level: Medium

CVE: CVE-2002-1631

[Update Details](#)

Recommendation is updated

9600 - Oracle Application Server Apache Configuration File Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2002-1635

[Update Details](#)

Recommendation is updated

9608 - Oracle Application Server PL/SQL Module Format String Vulnerability

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

Risk Level: Medium

CVE: CVE-2002-2153

[Update Details](#)

Recommendation is updated

9611 - Oracle Application Server TopLink Mapping Workbench Weak Password Encryption Vulnerability

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

Risk Level: Medium

CVE: CVE-2004-2134

[Update Details](#)

Recommendation is updated

9669 - Unix Account Default Password Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> UNIX

Risk Level: Medium

CVE: CVE-1999-0502

[Update Details](#)

Recommendation is updated

9839 - Microsoft Windows Service Isolation Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2010-1886

[Update Details](#)

Recommendation is updated

11352 - WordPress Featured Content Plugin "param" Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11368 - WordPress x7Host's Videox7 UGC Plugin "listid" Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11376 - WordPress Conduit Banner Plugin "banner-index-field-id" Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11415 - WordPress WP Featured Post With Thumbnail Plugin "src" Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11468 - WordPress YT-Audio Plugin "v" Parameter Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11538 - Novell Netware SSH Remote Buffer Overflow

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11843 - HP LaserJet JetDirect Card Security Bypass Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Printers and Print Servers

Risk Level: Medium

CVE: CVE-1999-1062

[Update Details](#)

Recommendation is updated

11871 - WordPress WP Forum Multiple SQL Injection Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11999 - TCP/IP SYN-FIN Packet Filtering Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Raw Socket

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12110 - RealNetworks Arcade Games StubbyUtil.ProcessMgr ActiveX Remote Code Execution

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12359 - Oracle Java Runtime Environment Insecure File Loading

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12574 - WordPress WP CSS Plugin f Local File Inclusion Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12904 - NexusPHP thanks php SQL Injection Denial Of Service

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

Risk Level: Medium

CVE: CVE-2011-4026

Update Details

Recommendation is updated

13636 - Microsoft Windows Remote Desktop Protocol mstlsapi.dll Private Key Spoofing Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: Medium

CVE: CVE-2005-1794

Update Details

Recommendation is updated

13839 - Samsung AllShare HTTP Header Processing Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14350 - Samsung Galaxy S III Memory Corruption And Arbitrary Code Execution Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Android

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16351 - Multiple Routers RomPager Embedded Web Server ROM-0 Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17019 - Siemens Automation License Manager Service Denial Of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17060 - TP-Link Multiple Routers "rom-0" Authentication Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18488 - Google Android DHCP Parsing Remote Code Execution Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Android

Risk Level: Medium

CVE: CVE-2014-7912, CVE-2014-7913

[Update Details](#)

Recommendation is updated Documentation is updated

18852 - (SOL17028) F5 BIG-IP PHP Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-3411, CVE-2015-3412

Update Details

Documentation is updated

19450 - (SOL17566) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7704

Update Details

Recommendation is updated Documentation is updated

19558 - (SOL17518) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7871

Update Details

Recommendation is updated Documentation is updated

19705 - SAP 3D Visual Enterprise Viewer SketchUp Document Multiple Use-After-Free Remote Code Execution Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-2536

Update Details

Recommendation is updated Risk is updated CVE is updated Documentation is updated

20316 - WECON LeviStudio Buffer Overflow Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-4533, CVE-2016-5781

Update Details

Recommendation is updated

20609 - Cisco IOS Application-Hosting Framework Unauthorized File Access Vulnerability

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

Risk Level: Medium
CVE: CVE-2016-6410

[Update Details](#)

Recommendation is updated Documentation is updated

20714 - Google Chrome Multiple Vulnerabilities Prior To 54.0.2840.59

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

Risk Level: Medium

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194

[Update Details](#)

Risk is updated

20715 - Google Chrome Multiple Vulnerabilities Prior To 54.0.2840.59

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194

[Update Details](#)

Risk is updated

20957 - (MS16-150) Security Update for Windows Secure Kernel Mode (3205642)

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

Risk Level: Medium

CVE: CVE-2016-7271

[Update Details](#)

Recommendation is updated

33145 - Oracle Solaris 150401-44 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5544, CVE-2016-5553

[Update Details](#)

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

88818 - Slackware Linux 14.1, 14.2 SSA:2016-305-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5584, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6663, CVE-2016-7440, CVE-2016-8283

[Update Details](#)

CVE is updated

130625 - Debian Linux 8.0 DSA-3711-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5584, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6663, CVE-2016-7440, CVE-2016-8283

[Update Details](#)

CVE is updated

130644 - Debian Linux 8.0 DSA-3731-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194, CVE-2016-5198, CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202, CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

[Update Details](#)

Risk is updated

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

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

Risk Level: Medium

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

[Update Details](#)

Risk is updated

144944 - SuSE Linux 13.2 openSUSE-SU-2016:2641-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8957, CVE-2015-8958, CVE-2016-5688, CVE-2016-6823, CVE-2016-7101, CVE-2016-7446, CVE-2016-7447, CVE-2016-7448, CVE-2016-7449, CVE-2016-7515, CVE-2016-7516, CVE-2016-7517, CVE-2016-7519, CVE-2016-7522, CVE-2016-7524, CVE-2016-7526, CVE-2016-7527, CVE-2016-7528, CVE-2016-7529, CVE-2016-7531, CVE-2016-7533, CVE-2016-7537, CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684

[Update Details](#)

Risk is updated

144953 - SuSE Linux 13.2 openSUSE-SU-2016:2597-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193

[Update Details](#)

Risk is updated

145021 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2933-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5584, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6663, CVE-2016-7440, CVE-2016-8283

[Update Details](#)

CVE is updated

145052 - SuSE SLES 11 SP4 SUSE-SU-2016:3046-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-2074, CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9429, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633

[Update Details](#)

CVE is updated

181516 - FreeBSD pcre Heap Overflow Vulnerability In Find_fixedlength () (8a1d0e63-1e07-11e5-b43d-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-5073

[Update Details](#)

Risk is updated

182157 - FreeBSD chromium Multiple Vulnerabilities (9118961b-9fa5-11e6-a265-3065ec8fd3ec)

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

Risk Level: Medium

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194

[Update Details](#)

Risk is updated

182183 - FreeBSD Roundcube Arbitrary Command Execution (125f5958-b611-11e6-a9a5-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2016-9920

Update Details

Risk is updated CVE is updated

185469 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3113-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1586, CVE-2016-5181, CVE-2016-5182, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5192, CVE-2016-5194

Update Details

Risk is updated

191361 - Fedora Linux 24 FEDORA-2016-c671aae490 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194, CVE-2016-5198

Update Details

Risk is updated

191383 - Fedora Linux 23 FEDORA-2016-012de4c97e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194, CVE-2016-5198

Update Details

Risk is updated

191385 - Fedora Linux 25 FEDORA-2016-35049d9d97 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194, CVE-2016-5198

Update Details

Risk is updated

643 - Netscape Enterprise Server 3.6 SP2 Accept Buffer Overflow

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

Risk Level: Medium

CVE: CVE-1999-0751

[Update Details](#)

Recommendation is updated

790 - Oracle Solaris Common Desktop Environment (CDE) dtspcd Information Leakage

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

1056 - Multiple Vendor Access Point Information Leakage

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

1841 - RSA ClearTrust BASICA Authentication Form Cross-Site Scripting

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

1958 - Efficient Networks 5861 Router NMap Denial-of-Service

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2003-1250

[Update Details](#)

Observation is updated Recommendation is updated

2367 - Sun Java App Server PE 8.0 Path Disclosure

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

3180 - RealPlayer RealMedia ".rm" Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

4173 - Visual Studio 6.0 Project Name Buffer Overflow Vulnerability

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

Risk Level: Medium

CVE: CVE-2006-1043

[Update Details](#)

Recommendation is updated

4329 - WindMail Metacharacter Vulnerability

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

Risk Level: Medium

CVE: CVE-2000-0242

[Update Details](#)

Recommendation is updated

4345 - OmniHTTPD visadmin.exe Denial of Service

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

Risk Level: Medium

CVE: CVE-1999-0970

[Update Details](#)

Recommendation is updated

4986 - Microsoft Windows Vista Local Privilege Escalation Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

5458 - Sony MicroVault USB Fingerprint Hidden Folder Vulnerability

Category: Windows Host Assessment -> Trojans, Backdoors, Viruses, and Malware
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-4785

[Update Details](#)

Recommendation is updated

5540 - Xunlei Web Thunder DPCClient.Vod.1 ActiveX Vulnerability

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

Risk Level: Medium

CVE: CVE-2007-5064

[Update Details](#)

Recommendation is updated

5563 - Mozilla Firefox Data URL Scheme Design Flaw

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

6006 - Yahoo Messenger VBscript Remote Denial of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

6558 - Mozilla Firefox XUL/XML Parser Corruption Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-1232

[Update Details](#)

Recommendation is updated

7129 - Microsoft Wordpad Memory Exhaustion Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

7750 - Oracle Reports Server Multiple Cross Site Scripting Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2005-2379

[Update Details](#)

Recommendation is updated

8317 - Cisco TFTP Server Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

8499 - Sun Java System Directory Server LDAP Search Request Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2010-0313

[Update Details](#)

Recommendation is updated

8701 - ROBS-PROJECTS Digital Sales IPN Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-0328

[Update Details](#)

Recommendation is updated

8726 - Nuked-Klan phpinfo Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2003-1371

[Update Details](#)

Recommendation is updated

8757 - Perforce P4Web Client Two Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

9212 - Oracle Application Server Portal Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2008-2138

[Update Details](#)

Recommendation is updated

9295 - Oracle Database Alter Session Set Events Code Execution Vulnerability

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

Risk Level: Medium

CVE: CVE-2006-7067

[Update Details](#)

Recommendation is updated

9503 - Oracle Database Server CREATE ANY DIRECTORY Privilege Escalation Vulnerability

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

Risk Level: Medium

CVE: CVE-2008-6065

[Update Details](#)

Recommendation is updated

9561 - Cisco IOS Regular Expression Engine Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2007-4430

[Update Details](#)

Recommendation is updated

9626 - Oracle Application Server DMS Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2007-1609

[Update Details](#)

Recommendation is updated

9631 - Oracle Application Server Multiple Components Default Credentials Privilege Escalation Vulnerability

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

Risk Level: Medium

CVE: CVE-2002-1637

[Update Details](#)

Recommendation is updated

9632 - Oracle Application Server HTTP Request Smuggling Vulnerability

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

Risk Level: Medium

CVE: CVE-2005-2093

[Update Details](#)

Recommendation is updated

9824 - SolarWinds TFTP Server Option Acknowledgement Request Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2009-3115

[Update Details](#)

Recommendation is updated

9858 - SquirrelMail Multiple Remote Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

9859 - Network Associates WebShield SMTP GET_CONFIG Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2000-0448

[Update Details](#)

Recommendation is updated

9911 - Cisco IOS TACACS+ Body Length Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2000-0486

Update Details

Recommendation is updated

9922 - University Of Washington pop2d Remote File Read Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

9948 - gIFTPd ZIP Plugins Multiple Directory Traversal Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

CVE: CVE-2005-0483

Update Details

Recommendation is updated

10031 - Xerver Administration Interface currentPath Directory Traversal Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-3561

Update Details

Recommendation is updated

10058 - Xerver Administration Interface portNr Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-4658

Update Details

Recommendation is updated

10515 - Nuked-Klan Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2003-1238

[Update Details](#)

Recommendation is updated

10703 - WordPress Vodpod Video Gallery Plugin "gid" Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2010-4875

[Update Details](#)

Recommendation is updated

10925 - WordPress Safe Search Plugin 'v1' Parameter Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2010-4518

[Update Details](#)

Recommendation is updated

10973 - VMware Server Web Access Interface Directory Traversal Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11139 - WordPress RSS Feed Reader For WordPress Plugin "rss url" Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2011-0740

[Update Details](#)

Recommendation is updated

11397 - Xerver HTTP Response Splitting Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-4086

[Update Details](#)

Recommendation is updated

11407 - HP Power Manager Server Cross Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2011-0277

[Update Details](#)

Recommendation is updated

11464 - WordPress TagNinja Plugin 'id' Parameter Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11550 - HP StorageWorks File Migration Agent Archive Manipulation Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11722 - Citrix MetaFrame Client Specified Published Applications Enumeration Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11913 - Microsoft Word 2003 MSO.dll Null Pointer Dereference Vulnerability

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

Risk Level: Medium

CVE: CVE-2010-3200

[Update Details](#)

Recommendation is updated

12005 - TCP/IP Firewall Rule Bypass Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Raw Socket

Risk Level: Medium

CVE: CVE-2002-2438

[Update Details](#)

Recommendation is updated

12068 - WordPress WP-StarsRateBox Plugin Cross Site Scripting And SQL Injection Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12163 - Quest NetVault SmartDisk libnvbasics.dll Integer Overflow Denial Of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12172 - Quest NetVault SmartDisk libnvbasics.dll Denial Of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12319 - Microsoft Windows SMB Response Denial Of Service Vulnerability

Category: Windows Host Assessment -> No Credentials Required

Risk Level: Medium

CVE: CVE-2000-1227

[Update Details](#)

Recommendation is updated

12356 - Sybase Advantage Database Server Memory Corruption Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12608 - Microsoft Windows Server 2008 R1 Local Denial Of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12635 - WordPress Donation Plugin did Parameter SQL Injection Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12669 - Carel Industries PlantVisor Enhanced Directory Traversal Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: Medium

CVE: CVE-2011-3487

[Update Details](#)

Recommendation is updated

12896 - Oracle Hyperion Financial Management TList6 ActiveX Control Remote Code Execution

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12935 - Oracle Hyperion Strategic Finance Client TTF16 ActiveX SetDevNames Remote Code Execution

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13008 - WordPress Bonus Theme s Parameter Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13009 - WordPress Simple Balance Theme s Parameter Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13235 - Rockwell Automation FactoryTalk Diagnostics Receiver Service Denial of Service Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13368 - WordPress uCan Post Plugin Multiple Parameters Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13623 - (MS12-034) Microsoft Windows .NET Index Comparison Remote Code Execution (2681578)

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

Risk Level: Medium

CVE: CVE-2012-0164

[Update Details](#)

Recommendation is updated

13968 - Honeywell PowerNet Twin Client RFSync.exe Denial of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14179 - Trend Micro InterScan Messaging Security Suite Cross-Site Scripting and Request Forgery Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2012-2995, CVE-2012-2996

[Update Details](#)

Recommendation is updated

14390 - RealNetworks RealPlayer Watch Folders Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2012-4987

[Update Details](#)

Recommendation is updated

14424 - VideoLAN VLC Media Player SHAddToRecentDocs() Function Denial of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14464 - Oracle Java SE OpenJDK Hash Table Denial of Service II

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

Risk Level: Medium

CVE: CVE-2012-5373

[Update Details](#)

Recommendation is updated

14582 - MODx Login User Enumeration Weakness

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14971 - Cisco Linksys EA2700 Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

15134 - D-Link DIR-635 "data" Cross-Site Scripting and Cross-Site Request Forgery Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

15141 - Siemens Solid Edge ST5 ActiveX Controls Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

15205 - WordPress Content Slide Plugin Cross-Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-2708

Update Details

Recommendation is updated

15214 - WordPress Stream Video Player Plugin Cross-Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-2706

Update Details

Recommendation is updated

15230 - Cisco Video Surveillance Operations Manager Help Page Redirection Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-3376

[Update Details](#)

Recommendation is updated

15290 - WordPress Dropdown Menu Widget Plugin Cross Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-2704

[Update Details](#)

Recommendation is updated

15296 - WordPress Sharebar Plugin Cross-Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-3491

[Update Details](#)

Recommendation is updated

15529 - WordPress Mingle Forum Plugin Cross-Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-0736

[Update Details](#)

Recommendation is updated

15600 - TP-LINK TD-W8951ND Router Cross-Site Scripting and Request Forgery Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

15619 - Cisco Prime Network Control System (NCS) Health Monitor Login Page Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2012-5990

[Update Details](#)

Recommendation is updated

15730 - (MS13-082) Microsoft .NET Framework JSON Parsing Denial of Service (2878890)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3861

[Update Details](#)

Recommendation is updated

15731 - (MS13-082) Microsoft .NET Framework Entity Expansion Denial of Service (2878890)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3860

[Update Details](#)

Recommendation is updated

15732 - (MS13-082) Microsoft .NET Framework OpenType Font Remote Code Execution (2878890)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3128

[Update Details](#)

Recommendation is updated

15758 - WordPress WP Ultimate Email Marketer Plugin Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2013-3263, CVE-2013-3264

[Update Details](#)

Recommendation is updated

15962 - Cisco Adaptive Security Appliance Software Phone Proxy Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-6682

[Update Details](#)

Recommendation is updated

15963 - Cisco Adaptive Security Appliance Software Auto-Update Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-5568

[Update Details](#)

Recommendation is updated

15994 - Wordpress dhtmlxSpreadsheet Plugin Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-6281

[Update Details](#)

Recommendation is updated

16270 - Cisco NX-OS Software Label Distribution Protocol Message Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-0677

[Update Details](#)

Recommendation is updated

16271 - Cisco NX-OS Software TACACS+ Command Authorization Local Security Bypass

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-0676

[Update Details](#)

Recommendation is updated

16386 - Cisco Adaptive Security Appliance Phone Proxy sec_db Race Condition Security Bypass

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-0739

[Update Details](#)

Recommendation is updated

16457 - Cisco Adaptive Security Appliance WebVPN Login Page Cross-Site Scripting

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-2120

[Update Details](#)

Recommendation is updated Documentation is updated

16670 - Microsoft Windows Two Denial of Service Vulnerabilities

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16797 - Cisco NX-OS HSRP Authentication Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3295

[Update Details](#)

Recommendation is updated

16933 - DotNetNuke Multiple Modules Arbitrary File Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17281 - SSLv3 Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3566

[Update Details](#)

Recommendation is updated

17415 - FESTO Robotino View Unspecified Defect Remote Denial of Service

Category: Windows Host Assessment -> SCADA

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18107 - Panasonic Configurator DL Remote Denial of Service

Category: Windows Host Assessment -> SCADA

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18305 - (MS15-044) Microsoft Windows GDI+ OpenType Font Parsing Remote Code Execution (3057110)

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

Risk Level: Medium

CVE: CVE-2015-1670

[Update Details](#)

Recommendation is updated

18403 - (SOL16344) F5 BIG-IP Apache Tomcat Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-0227

[Update Details](#)

Recommendation is updated Documentation is updated

18409 - (SOL16435) F5 BIG-IP GNU C Library Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-6040

[Update Details](#)

Recommendation is updated 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 Documentation is updated

18487 - (SOL16480) F5 BIG-IP unzip Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-8139, CVE-2014-8140, CVE-2014-8141

[Update Details](#)

Recommendation is updated Documentation 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 Documentation is updated

18509 - Cisco Catalyst 6500 Series Switches IPsec Tunnel Handling Denial of Service

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

Risk Level: Medium

CVE: CVE-2015-0771

Update Details

Recommendation is updated

18510 - Novell ZENworks Mobile Management Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

18523 - Cisco NX-OS Nexus MDS MOTD Telnet Login Reset Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-0775

Update Details

Recommendation is updated

18715 - (SOL16863) F5 BIG-IP Apache Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-5704

Update Details

Documentation is updated

18881 - Cisco NX-OS Address Resolution Protocol Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-4323

Update Details

Recommendation is updated

19046 - Cisco Nexus 9000 Series Switches Reserved VLAN Number Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-6295

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 Documentation is updated

19121 - Cisco NX-OS Nexus 3000 SNMP Non-Existent OID Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-6308

Update Details

Recommendation is updated

19176 - (SOL17315) F5 BIG-IP SNMP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3565

Update Details

Recommendation is updated Documentation is updated

19335 - (MS15-128) Microsoft Windows Graphics Memory Corruption Remote Code Execution I (3104503)

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

Risk Level: Medium

CVE: CVE-2015-6106

Update Details

Recommendation is updated

19445 - (SOL17515) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7855

[Update Details](#)

Recommendation is updated Documentation is updated

19446 - (SOL17517) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7701

[Update Details](#)

Recommendation is updated Documentation is updated

19448 - (SOL17526) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7848

[Update Details](#)

Recommendation is updated Documentation is updated

19757 - (MS16-035) Microsoft .NET Framework XML Validation Security Bypass (3141780)

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

Risk Level: Medium

CVE: CVE-2016-0132

[Update Details](#)

Recommendation is updated

19764 - (MS16-035) Security Update for .NET Framework to Address Security Feature Bypass (3141780)

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

Risk Level: Medium

CVE: CVE-2016-0132

[Update Details](#)

Recommendation is updated

19884 - (SOL21057235) F5 BIG-IP Libpng Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7981

[Update Details](#)

Documentation is updated

19907 - (MS16-039) Microsoft Windows Win32k Graphics Privilege Escalation I (3148522)

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

Risk Level: Medium

CVE: CVE-2016-0143

Update Details

Recommendation is updated

19908 - (MS16-039) Microsoft Windows Win32k Graphics Privilege Escalation II (3148522)

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

Risk Level: Medium

CVE: CVE-2016-0165

Update Details

Recommendation is updated

20599 - Oracle MySQL Unspecified Defect Privilege Escalation

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

Risk Level: Medium

CVE: CVE-2016-6663

Update Details

Recommendation is updated Documentation is updated

38204 - Mozilla Firefox XUL/XML Parser Corruption Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2009-1232

Update Details

Recommendation is updated

44005 - Microsoft Windows spoolss Remote Denial of Service

Category: Windows Host Assessment -> No Credentials Required

Risk Level: Medium

CVE: CVE-2006-6296

Update Details

Recommendation is updated

88798 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-236-01 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

88799 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-236-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

130565 - Debian Linux 8.0 DSA-3650-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

130566 - Debian Linux 8.0 DSA-3649-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

144848 - SuSE Linux 13.2 openSUSE-SU-2016:2208-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

144882 - SuSE SLES 11 SP4 SUSE-SU-2016:2346-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

144884 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2345-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

Update Details

Risk is updated

182098 - FreeBSD gnupg Attacker Who Obtains 4640 Bits From The RNG Can Trivially Predict The Next 160 Bits Of Output (e1c71d8d-64d9-11e6-

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

Risk Level: Medium

CVE: CVE-2016-6313

Update Details

Risk is updated

185388 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3065-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

Update Details

Risk is updated

185389 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3064-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

Update Details

Risk is updated

191040 - Fedora Linux 25 FEDORA-2016-b66a0aef08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

Update Details

Risk is updated

191046 - Fedora Linux 24 FEDORA-2016-9864953aa3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

191048 - Fedora Linux 25 FEDORA-2016-aab0a156ab Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

191060 - Fedora Linux 23 FEDORA-2016-2b4ecfa79f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

191110 - Fedora Linux 23 FEDORA-2016-3a0195918f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

[Update Details](#)

Risk is updated

3772 - Web Cart Order Execution Application Vulnerability

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

Risk Level: Medium

CVE: CVE-1999-0610

[Update Details](#)

Recommendation is updated

3861 - Home FTP Information Disclosure

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

Risk Level: Medium

CVE: CVE-2005-2726, CVE-2005-2727, CVE-2006-0355, CVE-2006-0356

[Update Details](#)

Recommendation is updated

4295 - Way-BOARD CGI Information Disclosure

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

Risk Level: Medium

CVE: CVE-2001-0214

[Update Details](#)

Recommendation is updated

5888 - Mozilla Firefox JSFrame Vulnerability

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

Risk Level: Medium

CVE: CVE-2008-2419

[Update Details](#)

Recommendation is updated

6626 - Safari For Windows XML Tag Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-1233

[Update Details](#)

Recommendation is updated

8634 - Sun Java System Web Server WebDAV LOCK Request File Disclosure

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

8945 - WeOnlyDo! SFTP ActiveX Control Remote Arbitrary File Access Vulnerability

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

Risk Level: Medium

CVE: CVE-2006-1175

[Update Details](#)

Recommendation is updated

11536 - WordPress PHP Speedy Plugin "page" Parameter Local File Inclusion Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11672 - RSA ClearTrust Login Page Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11829 - WordPress Placester Plugin "ajax_action" Parameter Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16384 - Cisco Adaptive Security Appliance Phone Proxy CTL Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-0738

[Update Details](#)

Recommendation is updated

18313 - (SOL16389) F5 BIG-IP MySQL Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-5908, CVE-2014-0386, CVE-2014-0393, CVE-2014-0401, CVE-2014-0402, CVE-2014-0412, CVE-2014-0437

[Update Details](#)

Recommendation is updated Documentation is updated

18410 - (SOL16506) F5 BIG-IP NTP Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-1799

[Update Details](#)

Recommendation is updated Documentation is updated

18794 - (MS15-080) Microsoft Windows CSRSS Privilege Escalation (3078662)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2453

[Update Details](#)

Recommendation is updated

19203 - (SOL17199) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3690

[Update Details](#)

Recommendation is updated Documentation is updated

19447 - (SOL17529) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7703

[Update Details](#)

Recommendation is updated Documentation is updated

19451 - (SOL17528) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7850

[Update Details](#)

Recommendation is updated Documentation is updated

19452 - (SOL17530) F5 BIG-IP NTP Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7691, CVE-2015-7692, CVE-2015-7702

[Update Details](#)

Recommendation is updated Documentation is updated

19483 - (SOL17525) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7853

[Update Details](#)

Recommendation is updated Documentation is updated

19484 - Cisco Nexus 5000 Series USB Driver Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-6394

Update Details

Documentation is updated

33162 - Oracle Solaris 150400-44 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553

Update Details

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

145069 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3053-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9429, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633

Update Details

CVE is updated

647 - Netscape Enterprise Server INDEX Directory Disclosure

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

Risk Level: Low

CVE: CVE-2001-0250

Update Details

Recommendation is updated

698 - Netscape Enterprise Server Administration Console

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

851 - Oracle9iAS Web Server globals.jsa disclosure

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

Risk Level: Low

CVE: CVE-2002-0562

[Update Details](#)

Recommendation is updated

860 - Netscape Enterprise Server Internal IP Address Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

873 - Novell GroupWise Web Root Disclosure

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

Risk Level: Low

CVE: CVE-1999-1006, CVE-2002-0341

[Update Details](#)

Recommendation is updated

886 - SilverStream Application Server Database Structure Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

895 - PHP info.php Information Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

896 - SilverStream Application Server Directory Listing Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

897 - SilverStream Application Server Configuration Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

912 - WebStar ssi_demo.ssi Information Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

964 - Redhat Stronghold Secure Webserver Sample Script Path Disclosure

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

Risk Level: Low

CVE: CVE-2001-0868

Update Details

Recommendation is updated

968 - New Atlanta ServletExec 4.x ISAPI Physical Path Disclosure

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

Risk Level: Low

CVE: CVE-2002-0892

Update Details

Recommendation is updated

1139 - OmniHTTPD Sample Scripts Cross-Site Scripting Vulnerabilities

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

Risk Level: Low

CVE: CVE-2002-1455

Update Details

Recommendation is updated

1350 - PHP phptonuke.php Directory Traversal

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

Risk Level: Low

CVE: CVE-2002-1913

[Update Details](#)

Recommendation is updated

3771 - Web Cart Application Configuration Vulnerability

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

Risk Level: Low

CVE: CVE-1999-0610

[Update Details](#)

Recommendation is updated

4208 - One or Zero Helpdesk SQL Injection

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

Risk Level: Low

CVE: CVE-2003-0303

[Update Details](#)

Recommendation is updated

4242 - MSN Messenger Service Message Spoof

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

Risk Level: Low

CVE: CVE-2002-0472

[Update Details](#)

Recommendation is updated

4294 - Muscat Empower CGI Path Disclosure

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

Risk Level: Low

CVE: CVE-2001-0224

[Update Details](#)

Recommendation is updated

4314 - Stalkerlab Mailers File Disclosure

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

Risk Level: Low

CVE: CVE-2000-0726

[Update Details](#)

Recommendation is updated

4993 - Google Desktop Anti-DNS Pinning vulnerability

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

5000 - Perl anacondaclip.pl Directory Traversal

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

Risk Level: Low

CVE: CVE-2001-0593

[Update Details](#)

Recommendation is updated

9583 - Cisco IOS Online Help Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Low

CVE: CVE-2000-0345

[Update Details](#)

Recommendation is updated

9588 - Yahoo! Toolbar Internet Explorer Security Bypass Vulnerability

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

10065 - Home FTP Server 'MKD' Command Multiple Directory Traversal Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Low

CVE: CVE-2009-4053

[Update Details](#)

Recommendation is updated

11275 - PHP expose_php Information Disclosure Vulnerability

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13273 - Support Incident Tracker Search.php Cross Site Scripting

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

Risk Level: Low

CVE: CVE-2011-3830

[Update Details](#)

Recommendation is updated

182191 - FreeBSD Mozilla SVG Animation Remote Code Execution (18f39fb6-7400-4063-acaf-0806e92c094f)

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

Risk Level: Low

CVE: CVE-2016-9079

[Update Details](#)

FASLScript is updated

191499 - Fedora Linux 24 FEDORA-2016-5ec2475e3f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9755, CVE-2016-9756, CVE-2016-9777, CVE-2016-9811

[Update Details](#)

CVE is updated

9630 - Oracle Application Server Single Sign-On Login Page Spoofing Vulnerability

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

Risk Level: Low

CVE: CVE-2004-1877

[Update Details](#)

Recommendation is updated

10030 - Xerver Administration Interface currentPath Cross Site Scripting Vulnerability

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

Risk Level: Low

CVE: CVE-2009-3562

[Update Details](#)

Recommendation is updated

11865 - HP Web Jetadmin setinfo.hts Script Directory Traversal Vulnerability

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

Risk Level: Low

CVE: CVE-2004-1857

[Update Details](#)

Recommendation is updated

18795 - (MS15-080) Microsoft Windows KMD Security Bypass (3078662)

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

Risk Level: Low

CVE: CVE-2015-2454

[Update Details](#)

Recommendation is updated

18796 - (MS15-080) Microsoft Windows Shell Security Bypass (3078662)

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

Risk Level: Low

CVE: CVE-2015-2465

[Update Details](#)

Recommendation is updated

18798 - (MS15-080) Microsoft Windows Kernel ASLR Security Bypass (3078662)

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

Risk Level: Low

CVE: CVE-2015-2433

[Update Details](#)

Recommendation is updated

5007 - Microsoft Windows Sticky Keys Vulnerability

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18853 - (SOL17049) F5 BIG-IP PHP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2015-4598

[Update Details](#)

Documentation is updated

12000 - TCP Port 0 Open Possible Backdoor Detected

Category: General Vulnerability Assessment -> Intrusive -> Raw Socket

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

70046 - macosx.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

70048 - adobe.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

HOW TO UPDATE

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

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

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

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 2016 McAfee, Inc.

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