2016-JUN-02
FSL version 7.5.825

MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

20105 - (SYM16-008) Symantec Antivirus Engine Malformed PE Header Parser Vulnerability

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-2208

Description

A vulnerability is present in some versions of Symantec Antivirus Engine.

Observation

Symantec Antivirus Engine is a content scanning engine used in many Symantec security products.

A vulnerability is present in some versions of Symantec Antivirus Engine. The flaw is due to improper handling of a specifically-crafted PE header file. Successful exploitation could allow an attacker to cause an immediate system crash.

20110 - (VMSA-2016-0005) VMware Player Privilege Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2016-2077

Description

A privilege escalation vulnerability is present in some versions of VMware Player.

Observation

VMware Player is a free virtualization software package.

A privilege escalation vulnerability is present in some versions of VMware Player. The flaw is due to improper referencing executable files on Windows. Successful exploitation could allow a local attacker to gain elevated privileges.

20119 - (SB10156) McAfee Web Gateway Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-5345, CVE-2016-0702, CVE-2016-0705, CVE-2016-0787, CVE-2016-0797

Description

Multiple vulnerabilities are present in some versions of McAfee Web Gateway.

Observation

McAfee Web Gateway is a web based security control system designed to prevent web application attacks.

Multiple vulnerabilities are present in some versions of McAfee Web Gateway. The flaws lie in several components. Successful exploitation could allow an attacker to retrieve sensitive data or cause a denial of service condition.

141198 - Red Hat Enterprise Linux RHSA-2016-1137 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2108

Description

The scan detected that the host is missing the following update:
RHSA-2016-1137

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-May/msg00043.html

RHEL5D
x86_64
openssl-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-debuginfo-0.9.8e-40.el5_11

i386
openssl-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-debuginfo-0.9.8e-40.el5_11

RHEL5S
i386
openssl-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-devel-0.9.8e-40.el5_11
openssl-debuginfo-0.9.8e-40.el5_11

x86_64
openssl-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-devel-0.9.8e-40.el5_11
openssl-debuginfo-0.9.8e-40.el5_11

160105 - CentOS 5 CESA-2016-1137 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2108

Description

The scan detected that the host is missing the following update:
CESA-2016-1137

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-May/021901.html

CentOS 5
i386
openssl-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-devel-0.9.8e-40.el5_11

i686
openssl-0.9.8e-40.el5_11

x86_64
openssl-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-devel-0.9.8e-40.el5_11

163098 - Oracle Enterprise Linux ELSA-2016-1137 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2016-2108

Description

The scan detected that the host is missing the following update:
ELSA-2016-1137

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006100.html

OEL5
i386
openssl-0.9.8e-40.0.1.el5_11
openssl-devel-0.9.8e-40.0.1.el5_11
openssl-perl-0.9.8e-40.0.1.el5_11

x86_64
openssl-0.9.8e-40.0.1.el5_11
openssl-devel-0.9.8e-40.0.1.el5_11
openssl-perl-0.9.8e-40.0.1.el5_11

174961 - Scientific Linux Security ERRATA Important: openssl on SL5.x i386/x86_64 (1605-10785)

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

Risk Level: High

CVE: CVE-2016-2108

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: openssl on SL5.x i386/x86_64 (1605-10785)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1605&L=scientific-linux-errata&F=&S=&P=10785

SL5
x86_64
openssl-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-devel-0.9.8e-40.el5_11
openssl-debuginfo-0.9.8e-40.el5_11

i386
openssl-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-devel-0.9.8e-40.el5_11
openssl-debuginfo-0.9.8e-40.el5_11

178178 - Gentoo Linux GLSA-201605-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2708, CVE-2015-2709, CVE-2015-2710, CVE-2015-2711, CVE-2015-2712, CVE-2015-2713, CVE-2015-2714, CVE-2015-2715, CVE-2015-2716, CVE-2015-2717, CVE-2015-2718, CVE-2015-4473, CVE-2015-4474, CVE-2015-4475, CVE-2015-4477, CVE-2015-4478, CVE-2015-4479, CVE-2015-4480, CVE-2015-4481, CVE-2015-4482, CVE-2015-4483, CVE-2015-4484, CVE-2015-4485, CVE-2015-4486, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4490, CVE-2015-4491, CVE-2015-4492, CVE-2015-4493, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2016-1523, CVE-2016-1930, CVE-2016-1931, CVE-2016-1933, CVE-2016-1935, CVE-2016-1937, CVE-2016-1938, CVE-2016-1939, CVE-2016-1940, CVE-2016-1941, CVE-2016-1942, CVE-2016-1943, CVE-2016-1944, CVE-2016-1945, CVE-2016-1946, CVE-2016-1947, CVE-2016-1948, CVE-2016-1949, CVE-2016-1950, CVE-2016-1952, CVE-2016-1953, CVE-2016-1954, CVE-2016-1955, CVE-2016-1956, CVE-2016-1957, CVE-2016-1958, CVE-2016-1959, CVE-2016-1960, CVE-2016-1961, CVE-2016-1962, CVE-2016-1963, CVE-2016-1964, CVE-2016-1965, CVE-2016-1966, CVE-2016-1967, CVE-2016-1968, CVE-2016-1969, CVE-2016-1970, CVE-2016-1971, CVE-2016-1972, CVE-2016-1973, CVE-2016-1974, CVE-2016-1975, CVE-2016-1976, CVE-2016-1977, CVE-2016-1978, CVE-2016-1979, CVE-2016-2790, CVE-2016-2791, CVE-2016-2792, CVE-2016-2793, CVE-2016-2794, CVE-2016-2795, CVE-2016-2796, CVE-2016-2797, CVE-2016-2798, CVE-2016-2799, CVE-2016-2800, CVE-2016-2801, CVE-2016-2802

Description

The scan detected that the host is missing the following update:
GLSA-201605-06

Observation

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

https://security.gentoo.org/glsa/201605-06

Affected packages:
dev-libs/nspr < 4.12
dev-libs/nss < 3.22.2
mail-client/thunderbird < 38.7.0
mail-client/thunderbird-bin < 38.7.0
www-client/firefox < 38.7.0
www-client/firefox-bin < 38.7.0

181957 - FreeBSD chromium Multiple Vulnerablities (7da1da96-24bb-11e6-bd31-3065ec8fd3ec)

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

Risk Level: High

CVE: CVE-2016-1660, CVE-2016-1661, CVE-2016-1662, CVE-2016-1663, CVE-2016-1664, CVE-2016-1665, CVE-2016-1666

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerablities (7da1da96-24bb-11e6-bd31-3065ec8fd3ec)

Observation

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

http://www.vuxml.org/freebsd/7da1da96-24bb-11e6-bd31-3065ec8fd3ec.html

Affected packages:
chromium < 50.0.2661.94
chromium-npapi < 50.0.2661.94
chromium-pulse < 50.0.2661.94

20097 - (VMSA-2016-0005) VMware Workstation Privilege Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2016-2077

Description

A privilege escalation vulnerability is present in some versions of VMware Workstation.

Observation

VMware Workstation is a virtualization software.

A privilege escalation vulnerability is present in some versions of VMware Workstation. The flaw lies in how VMware Workstation reference one of its executable. Successful exploitation could allow a local attacker to elevate its privileges.

20111 - (APSB16-17) Vulnerability In Adobe Connect

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

Risk Level: High

CVE: CVE-2016-4118

Description

A vulnerability is present in some versions of Adobe Connect.

Observation

Adobe Connect is a network meeting solution.

A vulnerability is present in some versions of Adobe Connect. The flaw lies in Adobe Connect Add-in Windows Installer. Successful exploitation could allow an attacker to execute arbitrary code via malicious DLL.

The update provided by Adobe bulletin APSB16-17 resolves this issue. The target system appears to be missing this update.

20112 - (SB10159) McAfee ePolicy Orchestrator Multiple Java Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

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

Observation

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

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator. The flaws lie in the Java JRE component. Successful exploitation could allow an attacker to disclose information, cause a denial of service condition or execute remote code.

130505 - Debian Linux 8.0 DSA-3589-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7552, CVE-2015-8875

Description

The scan detected that the host is missing the following update:
DSA-3589-1

Observation

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

http://www.debian.org/security/2016/dsa-3589

Debian 8.0
all
libgdk-pixbuf2.0-dev_2.31.1-2+deb8u5
libgdk-pixbuf2.0-0-udeb_2.31.1-2+deb8u5
libgdk-pixbuf2.0-0_2.31.1-2+deb8u5
libgdk-pixbuf2.0-0-dbg_2.31.1-2+deb8u5
libgdk-pixbuf2.0-doc_2.31.1-2+deb8u5
libgdk-pixbuf2.0-common_2.31.1-2+deb8u5
gir1.2-gdkpixbuf-2.0_2.31.1-2+deb8u5

141204 - Red Hat Enterprise Linux RHSA-2016-1132 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3210, CVE-2015-3217, CVE-2015-4792, CVE-2015-4802, CVE-2015-4815, CVE-2015-4816, CVE-2015-4819, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4879, CVE-2015-4895, CVE-2015-4913, CVE-2015-5073, CVE-2015-8381, CVE-2015-8383, CVE-2015-8384, CVE-2015-8385, CVE-2015-8386, CVE-2015-8388, CVE-2015-8391, CVE-2015-8392, CVE-2015-8395, CVE-2016-0505, CVE-2016-0546, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0606, CVE-2016-0608, CVE-2016-0609, CVE-2016-0610, CVE-2016-0616, CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0651, CVE-2016-0655, CVE-2016-0666, CVE-2016-0668, CVE-2016-1283, CVE-2016-2047, CVE-2016-3191

Description

The scan detected that the host is missing the following update:
RHSA-2016-1132

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-May/msg00042.html

RHEL6_6S
x86_64
rh-mariadb100-mariadb-server-10.0.25-4.el6
rh-mariadb100-mariadb-config-10.0.25-4.el6
rh-mariadb100-mariadb-devel-10.0.25-4.el6
rh-mariadb100-mariadb-errmsg-10.0.25-4.el6
rh-mariadb100-mariadb-10.0.25-4.el6
rh-mariadb100-mariadb-debuginfo-10.0.25-4.el6
rh-mariadb100-mariadb-oqgraph-engine-10.0.25-4.el6
rh-mariadb100-mariadb-bench-10.0.25-4.el6
rh-mariadb100-mariadb-common-10.0.25-4.el6
rh-mariadb100-mariadb-test-10.0.25-4.el6

RHEL6S
x86_64
rh-mariadb100-mariadb-server-10.0.25-4.el6
rh-mariadb100-mariadb-config-10.0.25-4.el6
rh-mariadb100-mariadb-devel-10.0.25-4.el6
rh-mariadb100-mariadb-errmsg-10.0.25-4.el6
rh-mariadb100-mariadb-10.0.25-4.el6
rh-mariadb100-mariadb-debuginfo-10.0.25-4.el6
rh-mariadb100-mariadb-oqgraph-engine-10.0.25-4.el6
rh-mariadb100-mariadb-bench-10.0.25-4.el6
rh-mariadb100-mariadb-common-10.0.25-4.el6
rh-mariadb100-mariadb-test-10.0.25-4.el6

RHEL6WS
x86_64
rh-mariadb100-mariadb-server-10.0.25-4.el6
rh-mariadb100-mariadb-config-10.0.25-4.el6
rh-mariadb100-mariadb-devel-10.0.25-4.el6
rh-mariadb100-mariadb-errmsg-10.0.25-4.el6
rh-mariadb100-mariadb-10.0.25-4.el6
rh-mariadb100-mariadb-debuginfo-10.0.25-4.el6
rh-mariadb100-mariadb-oqgraph-engine-10.0.25-4.el6
rh-mariadb100-mariadb-bench-10.0.25-4.el6
rh-mariadb100-mariadb-common-10.0.25-4.el6
rh-mariadb100-mariadb-test-10.0.25-4.el6

RHEL7S
x86_64
rh-mariadb100-mariadb-oqgraph-engine-10.0.25-4.el7
rh-mariadb100-mariadb-errmsg-10.0.25-4.el7
rh-mariadb100-mariadb-devel-10.0.25-4.el7
rh-mariadb100-mariadb-config-10.0.25-4.el7
rh-mariadb100-mariadb-10.0.25-4.el7
rh-mariadb100-mariadb-debuginfo-10.0.25-4.el7
rh-mariadb100-mariadb-common-10.0.25-4.el7
rh-mariadb100-mariadb-bench-10.0.25-4.el7
rh-mariadb100-mariadb-server-10.0.25-4.el7
rh-mariadb100-mariadb-test-10.0.25-4.el7

RHEL7WS
x86_64
rh-mariadb100-mariadb-oqgraph-engine-10.0.25-4.el7
rh-mariadb100-mariadb-errmsg-10.0.25-4.el7
rh-mariadb100-mariadb-devel-10.0.25-4.el7
rh-mariadb100-mariadb-config-10.0.25-4.el7
rh-mariadb100-mariadb-10.0.25-4.el7
rh-mariadb100-mariadb-debuginfo-10.0.25-4.el7
rh-mariadb100-mariadb-common-10.0.25-4.el7
rh-mariadb100-mariadb-bench-10.0.25-4.el7
rh-mariadb100-mariadb-server-10.0.25-4.el7
rh-mariadb100-mariadb-test-10.0.25-4.el7

144632 - SuSE Linux 13.2 openSUSE-SU-2016:1415-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1415-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00110.html

SuSE Linux 13.2
i586
libreoffice-math-5.0.6.3-31.3
libreoffice-writer-extensions-5.0.6.3-31.3
libreoffice-base-drivers-postgresql-5.0.6.3-31.3
libreoffice-base-drivers-mysql-5.0.6.3-31.3
libreoffice-debugsource-5.0.6.3-31.3
libreoffice-base-debuginfo-5.0.6.3-31.3
libreoffice-pyuno-debuginfo-5.0.6.3-31.3
libreoffice-base-drivers-mysql-debuginfo-5.0.6.3-31.3
libreoffice-calc-extensions-5.0.6.3-31.3
libreoffice-kde4-debuginfo-5.0.6.3-31.3
libreoffice-impress-debuginfo-5.0.6.3-31.3
libreoffice-math-debuginfo-5.0.6.3-31.3
libreoffice-gnome-debuginfo-5.0.6.3-31.3
libreoffice-writer-5.0.6.3-31.3
libreoffice-debuginfo-5.0.6.3-31.3
libreoffice-base-drivers-postgresql-debuginfo-5.0.6.3-31.3
libreoffice-kde4-5.0.6.3-31.3
libreoffice-sdk-doc-5.0.6.3-31.3
libreoffice-draw-5.0.6.3-31.3
libreoffice-writer-debuginfo-5.0.6.3-31.3
libreoffice-calc-debuginfo-5.0.6.3-31.3
libreoffice-mailmerge-5.0.6.3-31.3
libreoffice-gtk3-debuginfo-5.0.6.3-31.3
libreoffice-base-5.0.6.3-31.3
libreoffice-gtk3-5.0.6.3-31.3
libreoffice-calc-5.0.6.3-31.3

libreoffice-filters-optional-5.0.6.3-31.3
libreoffice-impress-5.0.6.3-31.3
libreoffice-officebean-5.0.6.3-31.3
libreoffice-gnome-5.0.6.3-31.3
libreoffice-draw-debuginfo-5.0.6.3-31.3
libreoffice-sdk-debuginfo-5.0.6.3-31.3
libreoffice-officebean-debuginfo-5.0.6.3-31.3
libreoffice-5.0.6.3-31.3
libreoffice-sdk-5.0.6.3-31.3
libreoffice-pyuno-5.0.6.3-31.3

noarch
libreoffice-l10n-xh-5.0.6.3-31.3
libreoffice-l10n-hi-5.0.6.3-31.3
libreoffice-l10n-gu-5.0.6.3-31.3
libreoffice-l10n-de-5.0.6.3-31.3
libreoffice-l10n-lt-5.0.6.3-31.3
libreoffice-branding-upstream-5.0.6.3-31.3
libreoffice-l10n-sl-5.0.6.3-31.3
libreoffice-l10n-hu-5.0.6.3-31.3
libreoffice-l10n-fa-5.0.6.3-31.3
libreoffice-l10n-pl-5.0.6.3-31.3
libreoffice-l10n-te-5.0.6.3-31.3
libreoffice-l10n-mai-5.0.6.3-31.3
libreoffice-l10n-es-5.0.6.3-31.3
libreoffice-l10n-zh-Hant-5.0.6.3-31.3
libreoffice-l10n-or-5.0.6.3-31.3
libreoffice-l10n-si-5.0.6.3-31.3
libreoffice-l10n-pa-5.0.6.3-31.3
libreoffice-l10n-hr-5.0.6.3-31.3
libreoffice-l10n-nl-5.0.6.3-31.3
libreoffice-l10n-kn-5.0.6.3-31.3
libreoffice-l10n-as-5.0.6.3-31.3
libreoffice-l10n-tn-5.0.6.3-31.3
libreoffice-l10n-nso-5.0.6.3-31.3
libreoffice-icon-theme-sifr-5.0.6.3-31.3
libreoffice-l10n-nb-5.0.6.3-31.3
libreoffice-icon-theme-oxygen-5.0.6.3-31.3
libreoffice-l10n-ro-5.0.6.3-31.3
libreoffice-l10n-cy-5.0.6.3-31.3
libreoffice-l10n-th-5.0.6.3-31.3
libreoffice-l10n-en-5.0.6.3-31.3
libreoffice-l10n-kk-5.0.6.3-31.3
libreoffice-l10n-sr-5.0.6.3-31.3
libreoffice-l10n-cs-5.0.6.3-31.3
libreoffice-l10n-pt-BR-5.0.6.3-31.3
libreoffice-l10n-uk-5.0.6.3-31.3
libreoffice-l10n-ve-5.0.6.3-31.3
libreoffice-l10n-ml-5.0.6.3-31.3
libreoffice-l10n-it-5.0.6.3-31.3
libreoffice-l10n-lv-5.0.6.3-31.3
libreoffice-icon-theme-hicontrast-5.0.6.3-31.3
libreoffice-icon-theme-galaxy-5.0.6.3-31.3
libreoffice-l10n-fi-5.0.6.3-31.3
libreoffice-l10n-pt-PT-5.0.6.3-31.3
libreoffice-l10n-zu-5.0.6.3-31.3
libreoffice-l10n-ss-5.0.6.3-31.3
libreoffice-icon-theme-breeze-5.0.6.3-31.3
libreoffice-l10n-ca-5.0.6.3-31.3
libreoffice-l10n-nr-5.0.6.3-31.3

libreoffice-l10n-ko-5.0.6.3-31.3
libreoffice-l10n-el-5.0.6.3-31.3
libreoffice-l10n-sv-5.0.6.3-31.3
libreoffice-l10n-ga-5.0.6.3-31.3
libreoffice-l10n-zh-Hans-5.0.6.3-31.3
libreoffice-l10n-br-5.0.6.3-31.3
libreoffice-l10n-sk-5.0.6.3-31.3
libreoffice-l10n-ru-5.0.6.3-31.3
libreoffice-l10n-tr-5.0.6.3-31.3
libreoffice-l10n-nn-5.0.6.3-31.3
libreoffice-l10n-ts-5.0.6.3-31.3
libreoffice-l10n-bg-5.0.6.3-31.3
libreoffice-l10n-fr-5.0.6.3-31.3
libreoffice-l10n-he-5.0.6.3-31.3
libreoffice-l10n-da-5.0.6.3-31.3
libreoffice-l10n-bn-5.0.6.3-31.3
libreoffice-icon-theme-tango-5.0.6.3-31.3
libreoffice-l10n-af-5.0.6.3-31.3
libreoffice-l10n-et-5.0.6.3-31.3
libreoffice-l10n-mr-5.0.6.3-31.3
libreoffice-l10n-ja-5.0.6.3-31.3
libreoffice-l10n-dz-5.0.6.3-31.3
libreoffice-l10n-eu-5.0.6.3-31.3
libreoffice-l10n-st-5.0.6.3-31.3
libreoffice-l10n-ta-5.0.6.3-31.3
libreoffice-l10n-ar-5.0.6.3-31.3
libreoffice-l10n-gl-5.0.6.3-31.3

x86_64
libreoffice-math-5.0.6.3-31.3
libreoffice-writer-extensions-5.0.6.3-31.3
libreoffice-base-drivers-postgresql-5.0.6.3-31.3
libreoffice-base-drivers-mysql-5.0.6.3-31.3
libreoffice-debugsource-5.0.6.3-31.3
libreoffice-base-debuginfo-5.0.6.3-31.3
libreoffice-pyuno-debuginfo-5.0.6.3-31.3
libreoffice-base-drivers-mysql-debuginfo-5.0.6.3-31.3
libreoffice-calc-extensions-5.0.6.3-31.3
libreoffice-kde4-debuginfo-5.0.6.3-31.3
libreoffice-impress-debuginfo-5.0.6.3-31.3
libreoffice-math-debuginfo-5.0.6.3-31.3
libreoffice-gnome-debuginfo-5.0.6.3-31.3
libreoffice-writer-5.0.6.3-31.3
libreoffice-debuginfo-5.0.6.3-31.3
libreoffice-base-drivers-postgresql-debuginfo-5.0.6.3-31.3
libreoffice-kde4-5.0.6.3-31.3
libreoffice-sdk-doc-5.0.6.3-31.3
libreoffice-draw-5.0.6.3-31.3
libreoffice-writer-debuginfo-5.0.6.3-31.3
libreoffice-calc-debuginfo-5.0.6.3-31.3
libreoffice-mailmerge-5.0.6.3-31.3
libreoffice-gtk3-debuginfo-5.0.6.3-31.3
libreoffice-base-5.0.6.3-31.3
libreoffice-gtk3-5.0.6.3-31.3
libreoffice-calc-5.0.6.3-31.3
libreoffice-filters-optional-5.0.6.3-31.3
libreoffice-impress-5.0.6.3-31.3
libreoffice-officebean-5.0.6.3-31.3
libreoffice-gnome-5.0.6.3-31.3
libreoffice-draw-debuginfo-5.0.6.3-31.3

libreoffice-sdk-debuginfo-5.0.6.3-31.3
libreoffice-officebean-debuginfo-5.0.6.3-31.3
libreoffice-5.0.6.3-31.3
libreoffice-sdk-5.0.6.3-31.3
libreoffice-pyuno-5.0.6.3-31.3

181956 - FreeBSD chromium Multiple Vulnerabilities (4dfafa16-24ba-11e6-bd31-3065ec8fd3ec)

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

Risk Level: High

CVE: CVE-2016-1667, CVE-2016-1668, CVE-2016-1669, CVE-2016-1670, CVE-2016-1671

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (4dfafa16-24ba-11e6-bd31-3065ec8fd3ec)

Observation

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

http://www.vuxml.org/freebsd/4dfafa16-24ba-11e6-bd31-3065ec8fd3ec.html

Affected packages:
chromium < 50.0.2661.102
chromium-npapi < 50.0.2661.102
chromium-pulse < 50.0.2661.102

20116 - Google Chrome Multiple Vulnerabilities Prior To 51.0.2704.63

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

Risk Level: High

CVE: CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1676, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, access sensitive information, bypass security measures or execute arbitrary code.

20117 - Google Chrome Multiple Vulnerabilities Prior To 51.0.2704.63

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1676, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, access sensitive information, bypass security measures or execute arbitrary code.

20100 - (HT206379) Apple iTunes Privilege Escalation Vulnerability Prior To 12.4

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

Risk Level: High

CVE: CVE-2016-1742

Description

A privilege escalation vulnerability is present in some versions of Apple iTunes.

Observation

Apple iTunes is a media management software.

A privilege escalation vulnerability is present in some versions of Apple iTunes. The flaw lies within product installer. Successful exploitation could allow an attacker to execute local arbitrary code or escalate privileges in the target system.

20109 - Cisco Adaptive Security Appliance XML Parser Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1385

Description

A denial of service vulnerability is present in some versions of Cisco Adaptive Security Appliance Software.

Observation

Cisco Adaptive Security Appliance Software is an operating system used in Cisco ASA device.

A denial of service vulnerability is present in some versions of Cisco Adaptive Security Appliance Software. The flaw occurs due to insufficient hardening of the XML parser configuration. Successful exploitation could allow an attacker to cause system instability or a reload of the affected system.

20122 - Google Chrome Multiple Vulnerabilities Prior To 51.0.2704.79

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

Risk Level: High

CVE: CVE-2016-1696, CVE-2016-1697, CVE-2016-1698, CVE-2016-1699, CVE-2016-1700, CVE-2016-1701, CVE-2016-1702, CVE-2016-1703

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, access sensitive information, bypass security measures, or execute arbitrary code.

20123 - Google Chrome Multiple Vulnerabilities Prior To 51.0.2704.79

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1696, CVE-2016-1697, CVE-2016-1698, CVE-2016-1699, CVE-2016-1700, CVE-2016-1701, CVE-2016-1702, CVE-2016-1703

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, access sensitive information, bypass security measures, or execute arbitrary code.

144633 - SuSE Linux 13.2 openSUSE-SU-2016:1417-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3697

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1417-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00111.html

SuSE Linux 13.2
x86_64
docker-1.9.1-56.1
docker-debuginfo-1.9.1-56.1
docker-debugsource-1.9.1-56.1

noarch
docker-test-1.9.1-56.1
docker-zsh-completion-1.9.1-56.1
docker-bash-completion-1.9.1-56.1

144635 - SuSE SLES 10 SP4 SUSE-SU-2016:1445-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0222, CVE-2014-7815, CVE-2015-5278, CVE-2015-8743, CVE-2016-2270, CVE-2016-2271, CVE-2016-2391, CVE-2016-2841

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1445-1

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-May/002084.html

SuSE SLES 10 SP4
x86_64
xen-kmp-debug-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-3.2.3_17040_46-0.25.1
xen-libs-32bit-3.2.3_17040_46-0.25.1
xen-tools-3.2.3_17040_46-0.25.1
xen-tools-domU-3.2.3_17040_46-0.25.1
xen-libs-3.2.3_17040_46-0.25.1
xen-doc-pdf-3.2.3_17040_46-0.25.1
xen-doc-html-3.2.3_17040_46-0.25.1
xen-devel-3.2.3_17040_46-0.25.1
xen-doc-ps-3.2.3_17040_46-0.25.1
xen-kmp-default-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-kmp-smp-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-kmp-kdump-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-tools-ioemu-3.2.3_17040_46-0.25.1

i586
xen-kmp-debug-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-kmp-bigsmp-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-kmp-vmi-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-3.2.3_17040_46-0.25.1
xen-tools-3.2.3_17040_46-0.25.1
xen-kmp-vmipae-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-tools-domU-3.2.3_17040_46-0.25.1
xen-libs-3.2.3_17040_46-0.25.1
xen-doc-pdf-3.2.3_17040_46-0.25.1
xen-doc-html-3.2.3_17040_46-0.25.1
xen-devel-3.2.3_17040_46-0.25.1
xen-doc-ps-3.2.3_17040_46-0.25.1
xen-kmp-default-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-kmp-smp-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-kmp-kdump-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1
xen-tools-ioemu-3.2.3_17040_46-0.25.1
xen-kmp-kdumppae-3.2.3_17040_46_2.6.16.60_0.132.8-0.25.1

144636 - SuSE Linux 13.2 openSUSE-SU-2016:1453-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2563

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1453-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00131.html

SuSE Linux 13.2
x86_64
putty-debugsource-0.67-4.10.1
putty-0.67-4.10.1
putty-debuginfo-0.67-4.10.1

i586
putty-debugsource-0.67-4.10.1
putty-0.67-4.10.1
putty-debuginfo-0.67-4.10.1

144637 - SuSE SLES 12, 12 SP1 SUSE-SU-2016:1457-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3566, CVE-2015-8076, CVE-2015-8077, CVE-2015-8078

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1457-1

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-May/002085.html

SuSE SLES 12 SP1
x86_64
perl-Cyrus-IMAP-2.3.18-37.1
cyrus-imapd-debuginfo-2.3.18-37.1
perl-Cyrus-IMAP-debuginfo-2.3.18-37.1
perl-Cyrus-SIEVE-managesieve-debuginfo-2.3.18-37.1
perl-Cyrus-SIEVE-managesieve-2.3.18-37.1
cyrus-imapd-debugsource-2.3.18-37.1

SuSE SLES 12
x86_64
perl-Cyrus-IMAP-2.3.18-37.1
cyrus-imapd-debuginfo-2.3.18-37.1
perl-Cyrus-IMAP-debuginfo-2.3.18-37.1
perl-Cyrus-SIEVE-managesieve-debuginfo-2.3.18-37.1
perl-Cyrus-SIEVE-managesieve-2.3.18-37.1
cyrus-imapd-debugsource-2.3.18-37.1

144641 - SuSE Linux 13.2 openSUSE-SU-2016:1441-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1283, CVE-2016-0718

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1441-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00125.html

SuSE Linux 13.2
x86_64
libexpat-devel-32bit-2.1.0-14.3.1
expat-2.1.0-14.3.1
libexpat1-2.1.0-14.3.1
libexpat-devel-2.1.0-14.3.1
expat-debugsource-2.1.0-14.3.1
expat-debuginfo-2.1.0-14.3.1
expat-debuginfo-32bit-2.1.0-14.3.1
libexpat1-32bit-2.1.0-14.3.1
libexpat1-debuginfo-32bit-2.1.0-14.3.1
libexpat1-debuginfo-2.1.0-14.3.1

i586
expat-2.1.0-14.3.1
libexpat1-2.1.0-14.3.1
libexpat-devel-2.1.0-14.3.1
expat-debugsource-2.1.0-14.3.1
expat-debuginfo-2.1.0-14.3.1
libexpat1-debuginfo-2.1.0-14.3.1

185298 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2987-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2497, CVE-2014-9709, CVE-2015-8874, CVE-2015-8877, CVE-2016-3074

Description

The scan detected that the host is missing the following update:
USN-2987-1

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-May/003443.html

Ubuntu 12.04

libgd2-xpm_2.0.36~rc1~dfsg-6ubuntu2.1
libgd2-noxpm_2.0.36~rc1~dfsg-6ubuntu2.1

Ubuntu 16.04

libgd3_2.1.1-4ubuntu0.16.04.1

Ubuntu 15.10

libgd3_2.1.1-4ubuntu0.15.10.1

Ubuntu 14.04

libgd3_2.1.0-3ubuntu0.1

185300 - Ubuntu Linux 12.04, 14.04, 15.10 USN-2985-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2207, CVE-2014-8121, CVE-2014-9761, CVE-2015-1781, CVE-2015-5277, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2016-2856, CVE-2016-3075

Description

The scan detected that the host is missing the following update:
USN-2985-1

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-May/003441.html

Ubuntu 12.04

libc6-dev_2.15-0ubuntu10.14
libc6_2.15-0ubuntu10.14

Ubuntu 15.10

libc6-dev_2.21-0ubuntu4.2
libc6_2.21-0ubuntu4.2

Ubuntu 14.04

libc6_2.19-0ubuntu6.8
libc6-dev_2.19-0ubuntu6.8

185301 - Ubuntu Linux 12.04, 14.04, 15.10 USN-2985-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2207, CVE-2014-8121, CVE-2014-9761, CVE-2015-1781, CVE-2015-5277, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2016-2856, CVE-2016-3075

Description

The scan detected that the host is missing the following update:
USN-2985-2

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-May/003442.html

Ubuntu 12.04

libc6_2.15-0ubuntu10.15
libc-bin_2.15-0ubuntu10.15
libc6-dev_2.15-0ubuntu10.15

Ubuntu 15.10

libc-bin_2.21-0ubuntu4.3
libc6_2.21-0ubuntu4.3
libc6-dev_2.21-0ubuntu4.3

Ubuntu 14.04

libc6_2.19-0ubuntu6.9
libc6-dev_2.19-0ubuntu6.9
libc-bin_2.19-0ubuntu6.9

20099 - (HPSBGN03570) HPE UCMDB Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-2001

Description

A vulnerability is present in some versions of HP UCMDB.

Observation

HP UCMDB is a product for enterprise system general management.

A vulnerability is present in some versions of HP UCMDB. The flaw lies in unspecified components. Successful exploitation could allow an attacker to retrieve sensitive data or conduct URL redirection attacks.

20101 - (HPSBGN03570) HPE UCMDB Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-2001

Description

A vulnerability is present in some versions of HP UCMDB.

Observation

HP UCMDB is a product for enterprise system general management.

A vulnerability is present in some versions of HP UCMDB. The flaw lies in unspecified components. Successful exploitation could allow an attacker to retrieve sensitive data or conduct URL redirection attacks.

20108 - (HPSBUX03606) HPE HP-UX Apache Tomcat 7 Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of HP-UX.

Observation

HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP-UX. The flaws lie in Tomcat. Successful exploitation could allow an attacker to obtain sensitive information, cause denial of service or execute arbitrary code.

20118 - (VMSA-2016-0006) VMware vCenter Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-2078

Description

A cross-site scripting vulnerability is present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

A cross-site scripting vulnerability is present in some versions of VMware vCenter Server. The flaw lies in the Web Client. Successful exploitation could allow an attacker to execute remote code.

88779 - Slackware Linux 14.1 SSA:2016-145-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1541

Description

The scan detected that the host is missing the following update:
SSA:2016-145-01

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.352685

Slackware 14.1
x86_64
libarchive-3.1.2-x86_64-2

141201 - Red Hat Enterprise Linux RHSA-2016-1138 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4554, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
RHSA-2016-1138

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-May/msg00044.html

RHEL6S
i386
squid-3.1.23-16.el6_8.4
squid-debuginfo-3.1.23-16.el6_8.4

x86_64
squid-3.1.23-16.el6_8.4
squid-debuginfo-3.1.23-16.el6_8.4

RHEL6WS
x86_64
squid-3.1.23-16.el6_8.4
squid-debuginfo-3.1.23-16.el6_8.4

i386
squid-3.1.23-16.el6_8.4
squid-debuginfo-3.1.23-16.el6_8.4

141202 - Red Hat Enterprise Linux RHSA-2016-1139 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-0801, CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
RHSA-2016-1139

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-May/msg00045.html

RHEL7S
ppc64
squid-3.3.8-26.el7_2.3
squid-sysvinit-3.3.8-26.el7_2.3
squid-debuginfo-3.3.8-26.el7_2.3

RHEL7WS
x86_64
squid-3.3.8-26.el7_2.3
squid-sysvinit-3.3.8-26.el7_2.3
squid-debuginfo-3.3.8-26.el7_2.3

141203 - Red Hat Enterprise Linux RHSA-2016-1140 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-0801, CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
RHSA-2016-1140

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-May/msg00046.html

RHEL6S
i386
squid34-debuginfo-3.4.14-9.el6_8.3
squid34-3.4.14-9.el6_8.3

x86_64
squid34-debuginfo-3.4.14-9.el6_8.3
squid34-3.4.14-9.el6_8.3

RHEL6WS
x86_64
squid34-debuginfo-3.4.14-9.el6_8.3
squid34-3.4.14-9.el6_8.3

i386
squid34-debuginfo-3.4.14-9.el6_8.3
squid34-3.4.14-9.el6_8.3

160106 - CentOS 7 CESA-2016-1139 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
CESA-2016-1139

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-May/021900.html

CentOS 7
x86_64
squid-sysvinit-3.3.8-26.el7_2.3
squid-3.3.8-26.el7_2.3

160107 - CentOS 6 CESA-2016-1140 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
CESA-2016-1140

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-May/021897.html

CentOS 6
x86_64
squid34-3.4.14-9.el6_8.3

i686
squid34-3.4.14-9.el6_8.3

160108 - CentOS 6 CESA-2016-1138 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4554, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
CESA-2016-1138

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-May/021896.html

CentOS 6
x86_64
squid-3.1.23-16.el6_8.4

i686
squid-3.1.23-16.el6_8.4

163097 - Oracle Enterprise Linux ELSA-2016-1139 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
ELSA-2016-1139

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006095.html

OEL7
x86_64
squid-sysvinit-3.3.8-26.el7_2.3
squid-3.3.8-26.el7_2.3

163099 - Oracle Enterprise Linux ELSA-2016-1138 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4554, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
ELSA-2016-1138

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006097.html

OEL6
x86_64
squid-3.1.23-16.el6_8.4

i386
squid-3.1.23-16.el6_8.4

163100 - Oracle Enterprise Linux ELSA-2016-1140 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
ELSA-2016-1140

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006098.html

OEL6
x86_64
squid34-3.4.14-9.el6_8.3

i386
squid34-3.4.14-9.el6_8.3

178179 - Gentoo Linux GLSA-201605-04 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8242, CVE-2014-9512

Description

The scan detected that the host is missing the following update:
GLSA-201605-04

Observation

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

https://security.gentoo.org/glsa/201605-04

Affected packages:
net-misc/rsync < 3.1.2

178180 - Gentoo Linux GLSA-201605-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-0025

Description

The scan detected that the host is missing the following update:
GLSA-201605-03

Observation

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

https://security.gentoo.org/glsa/201605-03

Affected packages:
media-libs/libfpx < 1.3.1_p6

181959 - FreeBSD cacti Multiple Vulnerabilities (6167b341-250c-11e6-a6fb-003048f2e514)

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

Risk Level: Medium

CVE: CVE-2016-3659

Description

The scan detected that the host is missing the following update:
cacti -- multiple vulnerabilities (6167b341-250c-11e6-a6fb-003048f2e514)

Observation

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

http://www.vuxml.org/freebsd/6167b341-250c-11e6-a6fb-003048f2e514.html

Affected packages:
cacti < 0.8.8h

181960 - FreeBSD php Multiple Vulnerabilities (6b110175-246d-11e6-8dd3-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2013-7456, CVE-2016-4343, CVE-2016-5093, CVE-2016-5094, CVE-2016-5096

Description

The scan detected that the host is missing the following update:
php -- multiple vulnerabilities (6b110175-246d-11e6-8dd3-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/6b110175-246d-11e6-8dd3-002590263bf5.html

Affected packages:
php70-gd < 7.0.7
php70-intl < 7.0.7
php56 < 5.6.22
php56-gd < 5.6.22
php55 < 5.5.36
php55-gd < 5.5.36
php55-phar < 5.5.36

20113 - BlackBerry Enterprise Service Management Console Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-1916, CVE-2016-1917, CVE-2016-1918, CVE-2016-3126

Description

Multiple vulnerabilities are present in some versions of BlackBerry Enterprise Service.

Observation

BlackBerry Enterprise Service is a popular wireless management software package.

Multiple vulnerabilities are present in some versions of BlackBerry Enterprise Service. The flaws lie in the Management Console. Successful exploitation could allow an attacker to force user to perform some unwanted actions.

20114 - BlackBerry Enterprise Service Management Console Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-1916, CVE-2016-1917, CVE-2016-1918, CVE-2016-3126

Description

Multiple vulnerabilities are present in some versions of BlackBerry Enterprise Service.

Observation

BlackBerry Enterprise Service is a popular wireless management software package.

Multiple vulnerabilities are present in some versions of BlackBerry Enterprise Service. The flaws lie in the Management Console. Successful exploitation could allow an attacker to force user to perform some unwanted actions.

20115 - (CTX213313) Citrix NetScaler Login Form Hijacking Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-4945

Description

A vulnerability is present in some versions of Citrix NetScaler.

Observation

Citrix NetScaler is a widely used product that helps enterprises to protect, control and improve their services.

A vulnerability is present in some versions of Citrix NetScaler. The flaw lies in how this product handles session cookies. Successful exploitation could allow a malicious user to hijack login form values through cookie tampering.

88778 - Slackware Linux 14.0, 14.1 SSA:2016-148-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7995

Description

The scan detected that the host is missing the following update:
SSA:2016-148-02

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.386546

Slackware 14.1
x86_64
libxslt-1.1.29-x86_64-1

Slackware 14.0
x86_64
libxslt-1.1.29-x86_64-1

130506 - Debian Linux 8.0 DSA-3587-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7456, CVE-2015-8874, CVE-2015-8877

Description

The scan detected that the host is missing the following update:
DSA-3587-1

Observation

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

http://www.debian.org/security/2016/dsa-3587

Debian 8.0
all
libgd2-noxpm-dev_2.1.0-5+deb8u3
libgd-dev_2.1.0-5+deb8u3
libgd-tools_2.1.0-5+deb8u3
libgd-dbg_2.1.0-5+deb8u3
libgd2-xpm-dev_2.1.0-5+deb8u3
libgd3_2.1.0-5+deb8u3

132240 - Oracle VM OVMSA-2016-0082 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7852, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0082

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-May/000469.html
http://oss.oracle.com/pipermail/oraclevm-errata/2016-May/000470.html

OVM3.3
x86_64
ntp-4.2.6p5-10.el6.1
ntpdate-4.2.6p5-10.el6.1

OVM3.4
x86_64
ntp-4.2.6p5-10.el6.1
ntpdate-4.2.6p5-10.el6.1

141199 - Red Hat Enterprise Linux RHSA-2016-1141 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

Description

The scan detected that the host is missing the following update:
RHSA-2016-1141

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-May/msg00047.html

RHEL7S
noarch
ntp-doc-4.2.6p5-22.el7_2.2
ntp-perl-4.2.6p5-22.el7_2.2

RHEL6S
i386
ntpdate-4.2.6p5-10.el6.1
ntp-perl-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1
ntp-debuginfo-4.2.6p5-10.el6.1

noarch
ntp-doc-4.2.6p5-10.el6.1

x86_64
ntpdate-4.2.6p5-10.el6.1
ntp-perl-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1
ntp-debuginfo-4.2.6p5-10.el6.1

RHEL6WS
x86_64
ntpdate-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1
ntp-debuginfo-4.2.6p5-10.el6.1

i386
ntpdate-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1
ntp-debuginfo-4.2.6p5-10.el6.1

RHEL7D
x86_64
ntpdate-4.2.6p5-22.el7_2.2
ntp-4.2.6p5-22.el7_2.2
ntp-debuginfo-4.2.6p5-22.el7_2.2
sntp-4.2.6p5-22.el7_2.2

noarch
ntp-doc-4.2.6p5-22.el7_2.2
ntp-perl-4.2.6p5-22.el7_2.2

RHEL6D
i386
ntpdate-4.2.6p5-10.el6.1
ntp-perl-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1
ntp-debuginfo-4.2.6p5-10.el6.1

noarch
ntp-doc-4.2.6p5-10.el6.1

x86_64
ntpdate-4.2.6p5-10.el6.1
ntp-perl-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1
ntp-debuginfo-4.2.6p5-10.el6.1

RHEL7WS
x86_64
ntpdate-4.2.6p5-22.el7_2.2
ntp-4.2.6p5-22.el7_2.2
ntp-debuginfo-4.2.6p5-22.el7_2.2
sntp-4.2.6p5-22.el7_2.2

noarch
ntp-doc-4.2.6p5-22.el7_2.2
ntp-perl-4.2.6p5-22.el7_2.2

141200 - Red Hat Enterprise Linux RHSA-2016-1166 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2099, CVE-2013-7440, CVE-2014-9365

Description

The scan detected that the host is missing the following update:
RHSA-2016-1166

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-May/msg00048.html

RHEL6_6S
x86_64
python27-python-devel-2.7.8-16.el6
python27-python-2.7.8-16.el6
python27-runtime-1.1-25.el6
python27-python-tools-2.7.8-16.el6
python27-numpy-1.7.1-10.el6
python27-numpy-debuginfo-1.7.1-10.el6
python27-1.1-25.el6
python27-python-bson-3.2.1-1.el6
python27-python-pymongo-gridfs-3.2.1-1.el6
python27-python-debug-2.7.8-16.el6
python27-python-pymongo-doc-3.2.1-1.el6
python27-numpy-f2py-1.7.1-10.el6
python27-python-libs-2.7.8-16.el6
python27-PyYAML-debuginfo-3.10-14.el6
python27-scldevel-1.1-25.el6
python27-python-debuginfo-2.7.8-16.el6
python27-tkinter-2.7.8-16.el6
python27-PyYAML-3.10-14.el6
python27-scipy-0.12.1-3.el6
python27-python-test-2.7.8-16.el6

python27-scipy-debuginfo-0.12.1-3.el6
python27-python-pymongo-3.2.1-1.el6
python27-python-pymongo-debuginfo-3.2.1-1.el6

noarch
python27-python-docutils-0.11-2.el6
python27-python-pip-7.1.0-2.el6
python27-python-virtualenv-13.1.0-1.el6

RHEL6S
x86_64
python27-python-devel-2.7.8-16.el6
python27-python-2.7.8-16.el6
python27-runtime-1.1-25.el6
python27-python-tools-2.7.8-16.el6
python27-numpy-1.7.1-10.el6
python27-numpy-debuginfo-1.7.1-10.el6
python27-1.1-25.el6
python27-python-bson-3.2.1-1.el6
python27-python-pymongo-gridfs-3.2.1-1.el6
python27-python-debug-2.7.8-16.el6
python27-python-pymongo-doc-3.2.1-1.el6
python27-numpy-f2py-1.7.1-10.el6
python27-python-libs-2.7.8-16.el6
python27-PyYAML-debuginfo-3.10-14.el6
python27-scldevel-1.1-25.el6
python27-python-debuginfo-2.7.8-16.el6
python27-tkinter-2.7.8-16.el6
python27-PyYAML-3.10-14.el6
python27-scipy-0.12.1-3.el6
python27-python-test-2.7.8-16.el6
python27-scipy-debuginfo-0.12.1-3.el6
python27-python-pymongo-3.2.1-1.el6
python27-python-pymongo-debuginfo-3.2.1-1.el6

noarch
python27-python-docutils-0.11-2.el6
python27-python-pip-7.1.0-2.el6
python27-python-virtualenv-13.1.0-1.el6

RHEL6WS
x86_64
python27-python-devel-2.7.8-16.el6
python27-python-2.7.8-16.el6
python27-runtime-1.1-25.el6
python27-python-tools-2.7.8-16.el6
python27-numpy-1.7.1-10.el6
python27-numpy-debuginfo-1.7.1-10.el6
python27-1.1-25.el6
python27-python-bson-3.2.1-1.el6
python27-python-pymongo-gridfs-3.2.1-1.el6
python27-python-debug-2.7.8-16.el6
python27-python-pymongo-doc-3.2.1-1.el6
python27-numpy-f2py-1.7.1-10.el6
python27-python-libs-2.7.8-16.el6
python27-PyYAML-debuginfo-3.10-14.el6
python27-scldevel-1.1-25.el6
python27-python-debuginfo-2.7.8-16.el6
python27-tkinter-2.7.8-16.el6
python27-PyYAML-3.10-14.el6

python27-scipy-0.12.1-3.el6
python27-python-test-2.7.8-16.el6
python27-scipy-debuginfo-0.12.1-3.el6
python27-python-pymongo-3.2.1-1.el6
python27-python-pymongo-debuginfo-3.2.1-1.el6

noarch
python27-python-docutils-0.11-2.el6
python27-python-pip-7.1.0-2.el6
python27-python-virtualenv-13.1.0-1.el6

RHEL7S
x86_64
python27-scipy-debuginfo-0.12.1-4.el7
python27-python-debug-2.7.8-14.el7
python27-runtime-1.1-25.el7
python27-python-libs-2.7.8-14.el7
python27-1.1-25.el7
python27-python-debuginfo-2.7.8-14.el7
python27-scldevel-1.1-25.el7
python27-python-pymongo-gridfs-3.2.1-1.el7
python27-python-test-2.7.8-14.el7
python27-python-pymongo-doc-3.2.1-1.el7
python27-numpy-f2py-1.7.1-10.el7
python27-python-2.7.8-14.el7
python27-tkinter-2.7.8-14.el7
python27-numpy-1.7.1-10.el7
python27-python-tools-2.7.8-14.el7
python27-numpy-debuginfo-1.7.1-10.el7
python27-PyYAML-3.10-14.el7
python27-scipy-0.12.1-4.el7
python27-python-bson-3.2.1-1.el7
python27-python-pymongo-3.2.1-1.el7
python27-python-pymongo-debuginfo-3.2.1-1.el7
python27-python-devel-2.7.8-14.el7
python27-PyYAML-debuginfo-3.10-14.el7

noarch
python27-python-pip-7.1.0-2.el7
python27-python-virtualenv-13.1.0-1.el7

RHEL7WS
x86_64
python27-scipy-debuginfo-0.12.1-4.el7
python27-python-debug-2.7.8-14.el7
python27-runtime-1.1-25.el7
python27-python-libs-2.7.8-14.el7
python27-1.1-25.el7
python27-python-debuginfo-2.7.8-14.el7
python27-scldevel-1.1-25.el7
python27-python-pymongo-gridfs-3.2.1-1.el7
python27-python-test-2.7.8-14.el7
python27-python-pymongo-doc-3.2.1-1.el7
python27-numpy-f2py-1.7.1-10.el7
python27-python-2.7.8-14.el7
python27-tkinter-2.7.8-14.el7
python27-numpy-1.7.1-10.el7
python27-python-tools-2.7.8-14.el7
python27-numpy-debuginfo-1.7.1-10.el7
python27-PyYAML-3.10-14.el7

python27-scipy-0.12.1-4.el7
python27-python-bson-3.2.1-1.el7
python27-python-pymongo-3.2.1-1.el7
python27-python-pymongo-debuginfo-3.2.1-1.el7
python27-python-devel-2.7.8-14.el7
python27-PyYAML-debuginfo-3.10-14.el7

noarch
python27-python-pip-7.1.0-2.el7
python27-python-virtualenv-13.1.0-1.el7

144634 - SuSE Linux 13.2 openSUSE-SU-2016:1439-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7995

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1439-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00123.html

SuSE Linux 13.2
x86_64
libxslt-python-debugsource-1.1.28-7.3.1
libxslt1-debuginfo-32bit-1.1.28-7.3.1
libxslt-python-1.1.28-7.3.1
libxslt1-1.1.28-7.3.1
libxslt-devel-1.1.28-7.3.1
libxslt1-debuginfo-1.1.28-7.3.1
libxslt-debugsource-1.1.28-7.3.1
libxslt-python-debuginfo-1.1.28-7.3.1
libxslt1-32bit-1.1.28-7.3.1
libxslt-tools-1.1.28-7.3.1
libxslt-devel-32bit-1.1.28-7.3.1
libxslt-tools-debuginfo-1.1.28-7.3.1

i586
libxslt-python-debugsource-1.1.28-7.3.1
libxslt-python-1.1.28-7.3.1
libxslt1-1.1.28-7.3.1
libxslt-devel-1.1.28-7.3.1
libxslt1-debuginfo-1.1.28-7.3.1
libxslt-debugsource-1.1.28-7.3.1
libxslt-python-debuginfo-1.1.28-7.3.1
libxslt-tools-1.1.28-7.3.1
libxslt-tools-debuginfo-1.1.28-7.3.1

144640 - SuSE Linux 13.2 openSUSE-SU-2016:1444-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8080

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1444-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00126.html

SuSE Linux 13.2
x86_64
redis-debuginfo-2.8.22-2.9.1
redis-2.8.22-2.9.1
redis-debugsource-2.8.22-2.9.1

i586
redis-debuginfo-2.8.22-2.9.1
redis-2.8.22-2.9.1
redis-debugsource-2.8.22-2.9.1

144642 - SuSE Linux 13.2 openSUSE-SU-2016:1446-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3627, CVE-2016-3705

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1446-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00127.html

SuSE Linux 13.2
i586
libxml2-debugsource-2.9.3-7.11.1
python-libxml2-2.9.3-7.11.1
libxml2-tools-debuginfo-2.9.3-7.11.1
libxml2-2-2.9.3-7.11.1
python-libxml2-debuginfo-2.9.3-7.11.1
python-libxml2-debugsource-2.9.3-7.11.1
libxml2-tools-2.9.3-7.11.1
libxml2-2-debuginfo-2.9.3-7.11.1
libxml2-devel-2.9.3-7.11.1

noarch
libxml2-doc-2.9.3-7.11.1

x86_64
libxml2-2-32bit-2.9.3-7.11.1
libxml2-debugsource-2.9.3-7.11.1

python-libxml2-2.9.3-7.11.1
libxml2-devel-32bit-2.9.3-7.11.1
libxml2-tools-debuginfo-2.9.3-7.11.1
libxml2-2-2.9.3-7.11.1
python-libxml2-debuginfo-2.9.3-7.11.1
python-libxml2-debugsource-2.9.3-7.11.1
libxml2-tools-2.9.3-7.11.1
libxml2-2-debuginfo-2.9.3-7.11.1
libxml2-2-debuginfo-32bit-2.9.3-7.11.1
libxml2-devel-2.9.3-7.11.1

160104 - CentOS 6, 7 CESA-2016-1141 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

Description

The scan detected that the host is missing the following update:
CESA-2016-1141

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-May/021898.html
http://lists.centos.org/pipermail/centos-announce/2016-May/021899.html

CentOS 7
x86_64
ntp-4.2.6p5-22.el7.centos.2
sntp-4.2.6p5-22.el7.centos.2
ntpdate-4.2.6p5-22.el7.centos.2

noarch
ntp-perl-4.2.6p5-22.el7.centos.2
ntp-doc-4.2.6p5-22.el7.centos.2

CentOS 6
i686
ntp-4.2.6p5-10.el6.centos.1
ntp-perl-4.2.6p5-10.el6.centos.1
ntpdate-4.2.6p5-10.el6.centos.1

noarch
ntp-doc-4.2.6p5-10.el6.centos.1

x86_64
ntp-4.2.6p5-10.el6.centos.1
ntp-perl-4.2.6p5-10.el6.centos.1
ntpdate-4.2.6p5-10.el6.centos.1

163096 - Oracle Enterprise Linux ELSA-2016-1141 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7979, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

Description

The scan detected that the host is missing the following update:
ELSA-2016-1141

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006096.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006099.html

OEL7
x86_64
ntp-doc-4.2.6p5-22.el7_2.2
ntp-4.2.6p5-22.el7_2.2
ntpdate-4.2.6p5-22.el7_2.2
ntp-perl-4.2.6p5-22.el7_2.2
sntp-4.2.6p5-22.el7_2.2

OEL6
x86_64
ntp-doc-4.2.6p5-10.el6.1
ntpdate-4.2.6p5-10.el6.1
ntp-perl-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1

i386
ntp-doc-4.2.6p5-10.el6.1
ntpdate-4.2.6p5-10.el6.1
ntp-perl-4.2.6p5-10.el6.1
ntp-4.2.6p5-10.el6.1

178177 - Gentoo Linux GLSA-201605-05 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7041, CVE-2014-2583, CVE-2015-3238

Description

The scan detected that the host is missing the following update:
GLSA-201605-05

Observation

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

https://security.gentoo.org/glsa/201605-05

Affected packages:
sys-libs/pam < 1.2.1

185299 - Ubuntu Linux 14.04, 15.10, 16.04 USN-2950-5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
USN-2950-5

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-May/003440.html

Ubuntu 16.04

samba_4.3.9+dfsg-0ubuntu0.16.04.2

Ubuntu 15.10

samba_4.3.9+dfsg-0ubuntu0.15.10.2

Ubuntu 14.04

samba_4.3.9+dfsg-0ubuntu0.14.04.3

144638 - SuSE Linux 13.2 openSUSE-SU-2016:1440-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2110

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1440-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00124.html

SuSE Linux 13.2
i586
ctdb-tests-debuginfo-4.2.4-37.1
libndr-krb5pac-devel-4.2.4-37.1
samba-pidl-4.2.4-37.1
libdcerpc-atsvc0-debuginfo-4.2.4-37.1
libsamdb0-debuginfo-4.2.4-37.1
samba-test-4.2.4-37.1
libsmbclient-raw0-debuginfo-4.2.4-37.1
samba-libs-debuginfo-4.2.4-37.1
samba-libs-4.2.4-37.1
libndr-standard-devel-4.2.4-37.1
ctdb-pcp-pmda-debuginfo-4.2.4-37.1
libdcerpc-binding0-debuginfo-4.2.4-37.1
samba-test-devel-4.2.4-37.1
libndr-standard0-4.2.4-37.1

libdcerpc-binding0-4.2.4-37.1
libwbclient0-debuginfo-4.2.4-37.1
libsmbclient0-debuginfo-4.2.4-37.1
libndr0-4.2.4-37.1
ctdb-devel-4.2.4-37.1
libsamba-credentials-devel-4.2.4-37.1
libsamba-hostconfig0-4.2.4-37.1
libdcerpc-samr-devel-4.2.4-37.1
libsamba-credentials0-debuginfo-4.2.4-37.1
libdcerpc-atsvc-devel-4.2.4-37.1
libndr0-debuginfo-4.2.4-37.1
libregistry0-debuginfo-4.2.4-37.1
libnetapi-devel-4.2.4-37.1
libtevent-util-devel-4.2.4-37.1
samba-client-debuginfo-4.2.4-37.1
libdcerpc-samr0-debuginfo-4.2.4-37.1
ctdb-pcp-pmda-4.2.4-37.1
libndr-krb5pac0-4.2.4-37.1
libsmbclient-raw0-4.2.4-37.1
libsamba-passdb0-4.2.4-37.1
libsamba-util0-4.2.4-37.1
libndr-nbt0-4.2.4-37.1
ctdb-4.2.4-37.1
libsmbclient-devel-4.2.4-37.1
samba-python-4.2.4-37.1
libnetapi0-4.2.4-37.1
libsamba-passdb-devel-4.2.4-37.1
libwbclient0-4.2.4-37.1
samba-client-4.2.4-37.1
libsmbldap0-debuginfo-4.2.4-37.1
libdcerpc0-debuginfo-4.2.4-37.1
libsamba-credentials0-4.2.4-37.1
libgensec0-4.2.4-37.1
samba-core-devel-4.2.4-37.1
libndr-nbt0-debuginfo-4.2.4-37.1
samba-winbind-debuginfo-4.2.4-37.1
samba-python-debuginfo-4.2.4-37.1
libdcerpc0-4.2.4-37.1
libsamba-policy-devel-4.2.4-37.1
libsmbldap-devel-4.2.4-37.1
libtevent-util0-4.2.4-37.1
ctdb-debuginfo-4.2.4-37.1
libdcerpc-samr0-4.2.4-37.1
libdcerpc-atsvc0-4.2.4-37.1
libsmbclient0-4.2.4-37.1
libgensec0-debuginfo-4.2.4-37.1
libsmbconf0-debuginfo-4.2.4-37.1
libsamba-util-devel-4.2.4-37.1
libndr-krb5pac0-debuginfo-4.2.4-37.1
libsamba-passdb0-debuginfo-4.2.4-37.1
samba-debuginfo-4.2.4-37.1
libsamba-hostconfig-devel-4.2.4-37.1
libdcerpc-devel-4.2.4-37.1
libregistry-devel-4.2.4-37.1
libwbclient-devel-4.2.4-37.1
libsmbldap0-4.2.4-37.1
samba-winbind-4.2.4-37.1
libgensec-devel-4.2.4-37.1
libndr-standard0-debuginfo-4.2.4-37.1
libnetapi0-debuginfo-4.2.4-37.1

libsamdb0-4.2.4-37.1
libsamba-hostconfig0-debuginfo-4.2.4-37.1
libsmbclient-raw-devel-4.2.4-37.1
libtevent-util0-debuginfo-4.2.4-37.1
samba-4.2.4-37.1
libsmbconf0-4.2.4-37.1
libsmbconf-devel-4.2.4-37.1
libregistry0-4.2.4-37.1
libsamba-policy0-debuginfo-4.2.4-37.1
ctdb-tests-4.2.4-37.1
libsamdb-devel-4.2.4-37.1
samba-test-debuginfo-4.2.4-37.1
libsamba-policy0-4.2.4-37.1
libndr-nbt-devel-4.2.4-37.1
libndr-devel-4.2.4-37.1
libsamba-util0-debuginfo-4.2.4-37.1
samba-debugsource-4.2.4-37.1

noarch
samba-doc-4.2.4-37.1

x86_64
libndr-standard0-debuginfo-32bit-4.2.4-37.1
libndr-nbt0-32bit-4.2.4-37.1
libregistry-devel-4.2.4-37.1
libsmbldap0-debuginfo-32bit-4.2.4-37.1
libsmbclient-raw0-4.2.4-37.1
libdcerpc0-debuginfo-4.2.4-37.1
libndr-standard-devel-4.2.4-37.1
libgensec-devel-4.2.4-37.1
libsamba-credentials0-4.2.4-37.1
samba-libs-debuginfo-4.2.4-37.1
libndr-standard0-32bit-4.2.4-37.1
libsamdb-devel-4.2.4-37.1
libsamba-hostconfig-devel-4.2.4-37.1
libnetapi0-debuginfo-4.2.4-37.1
libwbclient0-4.2.4-37.1
libdcerpc-samr-devel-4.2.4-37.1
samba-test-4.2.4-37.1
samba-python-4.2.4-37.1
libsmbconf-devel-4.2.4-37.1
samba-debuginfo-4.2.4-37.1
libgensec0-debuginfo-4.2.4-37.1
libdcerpc-samr0-32bit-4.2.4-37.1
libdcerpc-binding0-debuginfo-4.2.4-37.1
libsamdb0-debuginfo-4.2.4-37.1
libsmbldap-devel-4.2.4-37.1
libsmbclient0-debuginfo-4.2.4-37.1
libwbclient-devel-4.2.4-37.1
samba-winbind-debuginfo-4.2.4-37.1
libtevent-util0-debuginfo-4.2.4-37.1
libgensec0-debuginfo-32bit-4.2.4-37.1
samba-winbind-debuginfo-32bit-4.2.4-37.1
libsamba-credentials0-debuginfo-4.2.4-37.1
libndr-krb5pac0-4.2.4-37.1
ctdb-tests-debuginfo-4.2.4-37.1
libndr-standard0-4.2.4-37.1
libsamba-policy0-32bit-4.2.4-37.1
libsamba-credentials0-32bit-4.2.4-37.1
libndr-krb5pac0-debuginfo-4.2.4-37.1

libsmbconf0-debuginfo-4.2.4-37.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-37.1
libsmbclient0-32bit-4.2.4-37.1
libgensec0-32bit-4.2.4-37.1
libtevent-util0-debuginfo-32bit-4.2.4-37.1
libsamba-hostconfig0-4.2.4-37.1
libsmbconf0-debuginfo-32bit-4.2.4-37.1
libsamba-util0-debuginfo-32bit-4.2.4-37.1
libsamba-passdb0-4.2.4-37.1
samba-pidl-4.2.4-37.1
libdcerpc-samr0-debuginfo-32bit-4.2.4-37.1
libsamba-credentials0-debuginfo-32bit-4.2.4-37.1
libwbclient0-debuginfo-32bit-4.2.4-37.1
samba-test-debuginfo-4.2.4-37.1
libtevent-util0-4.2.4-37.1
libndr-nbt0-debuginfo-4.2.4-37.1
libdcerpc-binding0-4.2.4-37.1
libsamba-credentials-devel-4.2.4-37.1
libregistry0-32bit-4.2.4-37.1
libsamba-util0-4.2.4-37.1
libsmbclient-raw0-32bit-4.2.4-37.1
libtevent-util-devel-4.2.4-37.1
libndr0-4.2.4-37.1
libsamba-hostconfig0-debuginfo-4.2.4-37.1
libsamba-passdb0-debuginfo-4.2.4-37.1
libregistry0-4.2.4-37.1
libndr-nbt0-4.2.4-37.1
libdcerpc-samr0-4.2.4-37.1
samba-4.2.4-37.1
samba-libs-32bit-4.2.4-37.1
libdcerpc-binding0-32bit-4.2.4-37.1
ctdb-pcp-pmda-4.2.4-37.1
ctdb-debuginfo-4.2.4-37.1
libsmbclient-raw0-debuginfo-4.2.4-37.1
libsamba-util0-debuginfo-4.2.4-37.1
samba-libs-debuginfo-32bit-4.2.4-37.1
libregistry0-debuginfo-4.2.4-37.1
libdcerpc0-32bit-4.2.4-37.1
libndr-krb5pac0-32bit-4.2.4-37.1
libdcerpc0-4.2.4-37.1
libtevent-util0-32bit-4.2.4-37.1
libsamba-policy0-debuginfo-32bit-4.2.4-37.1
samba-core-devel-4.2.4-37.1
libndr-nbt-devel-4.2.4-37.1
ctdb-4.2.4-37.1
libsmbclient0-4.2.4-37.1
libsamdb0-debuginfo-32bit-4.2.4-37.1
libndr-standard0-debuginfo-4.2.4-37.1
libgensec0-4.2.4-37.1
libdcerpc-atsvc0-32bit-4.2.4-37.1
libsamba-policy0-debuginfo-4.2.4-37.1
libsmbclient-devel-4.2.4-37.1
ctdb-devel-4.2.4-37.1
samba-client-debuginfo-32bit-4.2.4-37.1
libndr0-debuginfo-4.2.4-37.1
libsmbldap0-debuginfo-4.2.4-37.1
libsmbconf0-4.2.4-37.1
libsamba-policy0-4.2.4-37.1
libsamba-passdb0-32bit-4.2.4-37.1
libsamba-util-devel-4.2.4-37.1

libndr-krb5pac0-debuginfo-32bit-4.2.4-37.1
libsamba-passdb0-debuginfo-32bit-4.2.4-37.1
libdcerpc-atsvc0-debuginfo-4.2.4-37.1
libsamba-util0-32bit-4.2.4-37.1
libsmbclient0-debuginfo-32bit-4.2.4-37.1
libnetapi0-debuginfo-32bit-4.2.4-37.1
libnetapi-devel-4.2.4-37.1
samba-libs-4.2.4-37.1
samba-winbind-4.2.4-37.1
libnetapi0-32bit-4.2.4-37.1
libsamdb0-32bit-4.2.4-37.1
libdcerpc0-debuginfo-32bit-4.2.4-37.1
libndr0-32bit-4.2.4-37.1
ctdb-pcp-pmda-debuginfo-4.2.4-37.1
samba-test-devel-4.2.4-37.1
samba-winbind-32bit-4.2.4-37.1
samba-python-debuginfo-4.2.4-37.1
libsmbldap0-32bit-4.2.4-37.1
libsamba-hostconfig0-32bit-4.2.4-37.1
libnetapi0-4.2.4-37.1
libwbclient0-debuginfo-4.2.4-37.1
libsamba-passdb-devel-4.2.4-37.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-37.1
samba-client-debuginfo-4.2.4-37.1
samba-debugsource-4.2.4-37.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-37.1
libwbclient0-32bit-4.2.4-37.1

88777 - Slackware Linux 14.0, 14.1 SSA:2016-148-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-7456, CVE-2016-5093, CVE-2016-5094, CVE-2016-5096

Description

The scan detected that the host is missing the following update:
SSA:2016-148-03

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.397230

Slackware 14.1
x86_64
php-5.6.22-x86_64-1

Slackware 14.0
x86_64
php-5.6.22-x86_64-1

88780 - Slackware Linux 14.1 SSA:2016-152-02 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:2016-152-02

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.360791

Slackware 14.1
x86_64
mozilla-thunderbird-45.1.1-x86_64-1

88781 - Slackware Linux 14.0, 14.1 SSA:2016-152-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5118

Description

The scan detected that the host is missing the following update:
SSA:2016-152-01

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.397749

Slackware 14.1
x86_64
imagemagick-6.8.6_10-x86_64-3

Slackware 14.0
x86_64
imagemagick-6.7.7_10-x86_64-3

88782 - Slackware Linux 14.0, 14.1 SSA:2016-148-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4447, CVE-2016-4448, CVE-2016-4449

Description

The scan detected that the host is missing the following update:
SSA:2016-148-01

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.404722

Slackware 14.1
x86_64
libxml2-2.9.4-x86_64-1

Slackware 14.0
x86_64
libxml2-2.9.4-x86_64-1

130507 - Debian Linux 8.0 DSA-3588-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1902, CVE-2016-4423

Description

The scan detected that the host is missing the following update:
DSA-3588-1

Observation

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

http://www.debian.org/security/2016/dsa-3588

Debian 8.0
all
php-symfony-locale_2.3.21+dfsg-4+deb8u3
php-symfony-finder_2.3.21+dfsg-4+deb8u3
php-symfony-stopwatch_2.3.21+dfsg-4+deb8u3
php-symfony-process_2.3.21+dfsg-4+deb8u3
php-symfony-serializer_2.3.21+dfsg-4+deb8u3
php-symfony-http-kernel_2.3.21+dfsg-4+deb8u3
php-symfony-doctrine-bridge_2.3.21+dfsg-4+deb8u3
php-symfony-event-dispatcher_2.3.21+dfsg-4+deb8u3
php-symfony-templating_2.3.21+dfsg-4+deb8u3
php-symfony-translation_2.3.21+dfsg-4+deb8u3
php-symfony-monolog-bridge_2.3.21+dfsg-4+deb8u3
php-symfony-class-loader_2.3.21+dfsg-4+deb8u3
php-symfony-options-resolver_2.3.21+dfsg-4+deb8u3
php-symfony-debug_2.3.21+dfsg-4+deb8u3
php-symfony-proxy-manager-bridge_2.3.21+dfsg-4+deb8u3
php-symfony-config_2.3.21+dfsg-4+deb8u3
php-symfony-filesystem_2.3.21+dfsg-4+deb8u3
php-symfony-classloader_2.3.21+dfsg-4+deb8u3
php-symfony-twig-bridge_2.3.21+dfsg-4+deb8u3
php-symfony-web-profiler-bundle_2.3.21+dfsg-4+deb8u3
php-symfony-propel1-bridge_2.3.21+dfsg-4+deb8u3
php-symfony-browser-kit_2.3.21+dfsg-4+deb8u3
php-symfony-property-access_2.3.21+dfsg-4+deb8u3
php-symfony-routing_2.3.21+dfsg-4+deb8u3
php-symfony-form_2.3.21+dfsg-4+deb8u3
php-symfony-swiftmailer-bridge_2.3.21+dfsg-4+deb8u3
php-symfony-framework-bundle_2.3.21+dfsg-4+deb8u3
php-symfony-twig-bundle_2.3.21+dfsg-4+deb8u3
php-symfony-yaml_2.3.21+dfsg-4+deb8u3
php-symfony-css-selector_2.3.21+dfsg-4+deb8u3
php-symfony-http-foundation_2.3.21+dfsg-4+deb8u3
php-symfony-intl_2.3.21+dfsg-4+deb8u3

php-symfony-security_2.3.21+dfsg-4+deb8u3
php-symfony-console_2.3.21+dfsg-4+deb8u3
php-symfony-dependency-injection_2.3.21+dfsg-4+deb8u3
php-symfony-dom-crawler_2.3.21+dfsg-4+deb8u3
php-symfony-validator_2.3.21+dfsg-4+deb8u3
php-symfony-security-bundle_2.3.21+dfsg-4+deb8u3
php-symfony-eventdispatcher_2.3.21+dfsg-4+deb8u3

144643 - SuSE Linux 13.2 openSUSE-SU-2016:1434-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5099

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1434-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00119.html

SuSE Linux 13.2
noarch
phpMyAdmin-4.4.15.6-33.1

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

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

Risk Level: Low

CVE: CVE-2016-2074

Description

The scan detected that the host is missing the following update:
openvswitch -- MPLS buffer overflow (b53bbf58-257f-11e6-9f4d-20cf30e32f6d)

Observation

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

http://www.vuxml.org/freebsd/b53bbf58-257f-11e6-9f4d-20cf30e32f6d.html

Affected packages:
openvswitch <= 2.3.2_1

181954 - FreeBSD nginx A Specially Crafted Request Might Result In Worker Process Crash (36cf7670-2774-11e6-af29-f0def16c5c1b)

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

Risk Level: Low

CVE: CVE-2016-4450

Description

The scan detected that the host is missing the following update:
nginx -- a specially crafted request might result in worker process crash (36cf7670-2774-11e6-af29-f0def16c5c1b)

Observation

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

http://www.vuxml.org/freebsd/36cf7670-2774-11e6-af29-f0def16c5c1b.html

Affected packages:
1.4.0 <= nginx < 1.10.1
1.3.9 <= nginx-devel < 1.11.1

181955 - FreeBSD chromium Multiple Vulnerabilities (1a6bbb95-24b8-11e6-bd31-3065ec8fd3ec)

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

Risk Level: Low

CVE: CVE-2016-1672, CVE-2016-1673, CVE-2016-1674, CVE-2016-1675, CVE-2016-1677, CVE-2016-1678, CVE-2016-1679, CVE-2016-1680, CVE-2016-1681, CVE-2016-1682, CVE-2016-1683, CVE-2016-1684, CVE-2016-1685, CVE-2016-1686, CVE-2016-1687, CVE-2016-1688, CVE-2016-1689, CVE-2016-1690, CVE-2016-1691, CVE-2016-1692, CVE-2016-1693, CVE-2016-1694, CVE-2016-1695

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (1a6bbb95-24b8-11e6-bd31-3065ec8fd3ec)

Observation

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

http://www.vuxml.org/freebsd/1a6bbb95-24b8-11e6-bd31-3065ec8fd3ec.html

Affected packages:
chromium < 51.0.2704.63
chromium-npapi < 51.0.2704.63
chromium-pulse < 51.0.2704.63

181958 - FreeBSD phpmyadmin XSS And Sensitive Data Leakage (00ec1be1-22bb-11e6-9ead-6805ca0b3d42)

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

Risk Level: Low

CVE: CVE-2016-5097, CVE-2016-5099

Description

The scan detected that the host is missing the following update:
phpmyadmin -- XSS and sensitive data leakage (00ec1be1-22bb-11e6-9ead-6805ca0b3d42)

Observation

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

http://www.vuxml.org/freebsd/00ec1be1-22bb-11e6-9ead-6805ca0b3d42.html

Affected packages:

4.6.0 <= phpmyadmin < 4.6.2

185297 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2986-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8872, CVE-2016-4804

Description

The scan detected that the host is missing the following update:
USN-2986-1

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-May/003444.html

Ubuntu 12.04

dosfstools_3.0.12-1ubuntu1.3

Ubuntu 16.04

dosfstools_3.0.28-2ubuntu0.1

Ubuntu 15.10

dosfstools_3.0.28-1ubuntu0.1

Ubuntu 14.04

dosfstools_3.0.26-1ubuntu0.1

185302 - Ubuntu Linux 15.10, 16.04 USN-2988-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1581, CVE-2016-1582

Description

The scan detected that the host is missing the following update:
USN-2988-1

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-May/003445.html

Ubuntu 15.10

lxd_0.20-0ubuntu4.2

Ubuntu 16.04

lxd_2.0.2-0ubuntu1~16.04.1

144639 - SuSE Linux 13.2 openSUSE-SU-2016:1423-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7705, CVE-2015-7848, CVE-2015-7849, CVE-2015-7850, CVE-2015-7851, CVE-2015-7852, CVE-2015-7853, CVE-2015-7854, CVE-2015-7855, CVE-2015-7871, CVE-2015-7973, CVE-2015-7974, CVE-2015-7975, CVE-2015-7976, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158, CVE-2016-1547, CVE-2016-1548, CVE-2016-1549, CVE-2016-1550, CVE-2016-1551, CVE-2016-2516, CVE-2016-2517, CVE-2016-2518, CVE-2016-2519

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1423-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00114.html

SuSE Linux 13.2
x86_64
ntp-debuginfo-4.2.8p7-25.15.1
ntp-debugsource-4.2.8p7-25.15.1
ntp-doc-4.2.8p7-25.15.1
ntp-4.2.8p7-25.15.1

i586
ntp-debuginfo-4.2.8p7-25.15.1
ntp-debugsource-4.2.8p7-25.15.1
ntp-doc-4.2.8p7-25.15.1
ntp-4.2.8p7-25.15.1

ENHANCED CHECKS

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

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

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

12097 - Quest Software Big Brother Arbitrary File Deletion Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14093 - Oracle Java Applet SB Bypass Remote Code Execution

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

Risk Level: High

CVE: CVE-2012-4681

Update Details

Observation is updated

15845 - NETGEAR WNDR3700v4 ping6 Diagnostic Page Command Injection Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated Documentation is updated

181933 - FreeBSD OpenSSL Multiple Vulnerabilities (01d729ca-1143-11e6-b55e-b499baebfeaf)

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176

Update Details

FASLScript 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 -> Instrusive -> 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

10129 - Open&Compact FTP Server Authentication Bypass Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2010-2620

Update Details

Description is updated Recommendation is updated

10145 - Open&Compact FTP Server Multiple Buffer Overflow Vulnerabilities

Category: General Vulnerability Assessment -> Instrusive -> Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

11830 - (APSA11-02) Adobe Flash Player/Acrobat/Reader Doc Remote Code Execution

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

Risk Level: High

CVE: CVE-2011-0611

Update Details

Observation 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

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

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

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

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

16809 - Oracle Database Multiple Unspecified Remote Code Execution Vulnerabilities

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

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

6190 - (MS08-067) Microsoft Windows Server Service Vulnerability (958644)

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

Risk Level: High

CVE: CVE-2008-4250

Update Details

Observation is updated

6240 - (MS08-067) Microsoft Windows Server Service Vulnerability Intrusive (958644)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2008-4250

Update Details

Observation 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

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

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

18855 - (SOL17123) F5 BIG-IP Apache Tomcat Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-0230

Update Details

FASLScript 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

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

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

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

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

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 -> Instrusive -> Web Server

Risk Level: High

CVE: CVE-2009-4140

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

19708 - Netgear Management System NMS300 Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-1524, CVE-2016-1525

Update Details

Recommendation is updated

130503 - Debian Linux 8.0 DSA-3582-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0718

Update Details

Risk is updated

181952 - FreeBSD expat Denial Of Service Vulnerability On Malformed Input (57b3aba7-1e25-11e6-8dd3-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-0718

Update Details
Risk is updated

185291 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2983-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-0718

Update Details
Risk is updated

190591 - Fedora Linux 22 FEDORA-2016-6fd7a31d36 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-4021

Update Details
Risk is updated

190625 - Fedora Linux 24 FEDORA-2016-8f4b54b005 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-4021

Update Details
Risk is updated

190631 - Fedora Linux 23 FEDORA-2016-5733ad20f5 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-4021

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

1039 - Omnicron OmniHTTPd Long Request Buffer Overflow

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

Risk Level: Medium

CVE: CVE-2001-0613

Update Details

Recommendation is updated

1041 - MyWebServer Buffer Overflow

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

Risk Level: Medium

CVE: CVE-2002-1003

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

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

6767 - (MS09-025) Microsoft Windows Driver Class Registration Vulnerability (968537)

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

Risk Level: Medium

CVE: CVE-2009-1125

Update Details

Observation 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

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

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

19558 - (SOL17518) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7871

Update Details

FASLScript 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

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

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

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

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

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

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

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

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

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

11371 - OraMon oramon.ini Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2008-6869

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

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

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

19453 - (SOL17516) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5
Risk Level: Medium
CVE: CVE-2015-7852

Update Details
FASLScript 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

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

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

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

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

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

14541 - HP Systems Insight Manager Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14542 - Mozilla Firefox Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

15211 - VMware Fusion Obsolete Version Detection

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70083 - misc-network-id.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.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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