2014-DEC-26
FSL version 7.5.660

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

178029 - Gentoo Linux GLSA-201412-33 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-4009, CVE-2009-4010, CVE-2012-1193, CVE-2014-8601

Description

The scan detected that the host is missing the following update:
GLSA-201412-33

Observation

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

http://security.gentoo.org/glsa/glsa-201412-33.xml

Affected packages:
net-dns/pdns-recursor < 3.6.1-r1

17537 - (HT6597) Apple Safari Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-1748, CVE-2014-4452, CVE-2014-4459, CVE-2014-4465, CVE-2014-4466, CVE-2014-4468, CVE-2014-4469, CVE-2014-4470, CVE-2014-4471, CVE-2014-4472, CVE-2014-4473, CVE-2014-4474, CVE-2014-4475

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

Multiple vulnerabilities are present in some versions of Apple Safari. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code.

This update was released because last security fix (HT6596) of Safari has problem.

17542 - Google Chrome Flash Player Vulnerability Prior To 39.0.2171.95

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

Risk Level: High

CVE: CVE-2014-9162, CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9163, CVE-2014-9164

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser for Microsoft Windows, Apple Mac OS X and Linux.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in the Adobe Flash Player component of Google Chrome. Successful exploitation could allow an attacker to execute arbitrary code, bypass security measures or cause a denial of service condition.

17550 - SAP Netweaver Enqueue Server Trace Pattern Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of SAP Netweaver could lead to a denial of service.

Observation

A vulnerability in some versions of SAP Netweaver could lead to a denial of service.

The flaw is due to an unspecified defect. Successful exploitation by a remote attacker could result in a denial of service condition.

17552 - VMware vCloud Automation Center Privilege Escalation

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

Risk Level: High

CVE: CVE-2014-8373

Description

A vulnerability in some versions of VMware vCloud could lead to a privilege escalation.

Observation

A vulnerability in some versions of VMware vCloud could lead to a privilege escalation.

The flaw is in the n the vCAC VMware Remote Console (VMRC) function. Successful exploitation could allow a local user to gain elevated privileges.

88657 - Slackware Linux 14.0, 14.1 SSA:2014-356-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3710, CVE-2014-8142

Description

The scan detected that the host is missing the following update:
SSA:2014-356-02

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=2014&m=slackware-security.400170

Slackware 14.1
x86_64
php-5.4.36-x86_64-1

Slackware 14.0
x86_64
php-5.4.36-x86_64-1

88659 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2014-356-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296

Description

The scan detected that the host is missing the following update:
SSA:2014-356-01

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=2014&m=slackware-security.520762

Slackware 13.0
x86_64
ntp-4.2.8-x86_64-1

Slackware 14.1
x86_64
ntp-4.2.8-x86_64-1

Slackware 13.37
x86_64
ntp-4.2.8-x86_64-1

Slackware 13.1
x86_64
ntp-4.2.8-x86_64-1

Slackware 14.0
x86_64
ntp-4.2.8-x86_64-1

130033 - Debian Linux 7.0 DSA-3108-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296

Description

The scan detected that the host is missing the following update:
DSA-3108-1

Observation

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

http://www.debian.org/security/2014/dsa-3108

Debian 7.0
all
ntp_1:4.2.6.p5+dfsg-2+deb7u1

143319 - SuSE Linux 11.4 openSUSE-SU-2014:1680-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9295, CVE-2014-9296

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1680-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-12/msg00079.html

SuSE Linux 11.4
x86_64
ntp-debugsource-4.2.6p3-6.28.1
ntp-4.2.6p3-6.28.1
ntp-debuginfo-4.2.6p3-6.28.1
ntp-doc-4.2.6p3-6.28.1

i586
ntp-debugsource-4.2.6p3-6.28.1
ntp-4.2.6p3-6.28.1
ntp-debuginfo-4.2.6p3-6.28.1
ntp-doc-4.2.6p3-6.28.1

184656 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2449-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296

Description

The scan detected that the host is missing the following update:
USN-2449-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002772.html

Ubuntu 14.10

ntp_4.2.6.p5+dfsg-3ubuntu2.14.10.1

Ubuntu 14.04

ntp_4.2.6.p5+dfsg-3ubuntu2.14.04.1

Ubuntu 12.04

ntp_4.2.6.p3+dfsg-1ubuntu3.2

Ubuntu 10.04

ntp_4.2.4p8+dfsg-1ubuntu2.2

188708 - Fedora Linux 20 FEDORA-2014-16626 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7840

Description

The scan detected that the host is missing the following update:
FEDORA-2014-16626

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146925.html

Fedora Core 20

qemu-1.6.2-12.fc20

188709 - Fedora Linux 21 FEDORA-2014-17367 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296

Description

The scan detected that the host is missing the following update:
FEDORA-2014-17367

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146911.html

Fedora Core 21

ntp-4.2.6p5-25.fc21

188710 - Fedora Linux 21 FEDORA-2014-16840 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2240

Description

The scan detected that the host is missing the following update:
FEDORA-2014-16840

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146933.html

Fedora Core 21

freetype-2.5.3-13.fc21

188711 - Fedora Linux 21 FEDORA-2014-17009 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1693

Description

The scan detected that the host is missing the following update:
FEDORA-2014-17009

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146939.html

Fedora Core 21

erlang-17.4-1.fc21

17547 - IBM Rational ClearQuest Java and OpenSSL Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-3509, CVE-2014-3511, CVE-2014-4244, CVE-2014-4263, CVE-2014-5139

Description

Multiple vulnerabilities are present in some versions of IBM Rational ClearQuest.

Observation

IBM Rational ClearQuest is a workflow automation software which provides bug tracking and process automation across the application development life cycle.

Multiple vulnerabilities are present in some versions of IBM Rational ClearQuest. The flaws are present in Java Runtime Environment (JRE) and OpenSSL. Successful exploitation could allow an attacker to cause bypass certain security restrictions, disclose sensitive information, manipulate certain data, and cause a Denial of Service.

88658 - Slackware Linux 14.1 SSA:2014-356-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102, CVE-2014-8103

Description

The scan detected that the host is missing the following update:
SSA:2014-356-03

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=2014&m=slackware-security.618701

Slackware 14.1
x86_64
xorg-server-xephyr-1.14.3-x86_64-3
xorg-server-xnest-1.14.3-x86_64-3
xorg-server-1.14.3-x86_64-3
xorg-server-xvfb-1.14.3-x86_64-3

17426 - (HPSBMU03184) HP SiteScope SSL Remote Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

An information disclosure vulnerability is present in some versions of HP SiteScope.

Observation

HP SiteScope is an agentless monitoring software that monitors the availability and performance of IT infrastructures and application components remotely.

An information disclosure vulnerability is present in some versions of HP SiteScope. It's due to the SSLv3 vulnerability known as "POODLE". Successful exploitation by an attacker could result in disclosure of information.

17438 - IBM AIX RSyslog Two Denial of Service Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-3634, CVE-2014-3683

Description

Two denial of service vulnerabilities are present in some versions of IBM AIX.

Observation

Rsyslog is an open-source software for forwarding log messages in an IP network.

Two denial of service vulnerabilities are present in some versions of IBM AIX. The flaws are due to improper handling of specially-crafted messages. Successful exploitation by a remote attacker could cause the rsyslogd service to crash.

17530 - (VMSA-2014-0012) VMware vCenter Server Appliance Cross-Site Scripting Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3797

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 within VMware vCenter Server. Successful exploitation could allow an attacker to execute remote code.

17536 - (SOL15878) F5 BIG-IP bzip2 Integer Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2010-0405

Description

An integer overflow vulnerability is present in some versions of F5 BIG-IP products.

Observation

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

An integer overflow vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the bzip2 component. Successful exploitation could allow an attacker to cause denial of service or execute arbitrary code.

17541 - (SOL15902) F5 BIG-IP Apache Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2010-1623

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Apache Portable Runtime Utility library (APR-util). Successful exploitation could allow an attacker to cause a denial of service condition.

17543 - Trihedral Engineering VTScada Malformed Network Request Denial of Service

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

Risk Level: Medium

CVE: CVE-2014-9192

Description

A vulnerability in some versions of Trihedral Engineering VTScada could lead to a denial of service.

Observation

A vulnerability in some versions of Trihedral Engineering VTScada could lead to a denial of service.

The flaw lies in the handling of a specifically crafted malformed network request. Successful exploitation by a remote attacker could result in a denial of service condition.

17544 - IBM DB2 Multiple Vulnerabilities Prior To 10.5 Fix Pack 5

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-6159, CVE-2014-6209, CVE-2014-6210, CVE-2014-8901

Description

Multiple vulnerabilities are present in some versions of IBM DB2.

Observation

IBM DB2 is a database software.

Multiple vulnerabilities are present in some versions of IBM DB2. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause denial of service.

17549 - (SA-CORE-2014-006) Drupal Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Drupal.

Observation

Drupal is a popular open source content management system.

Multiple vulnerabilities are present in some versions of Drupal. The flaws lie in a password hashing API . Successful exploitation by a remote attacker may cause a denial of service condition and session hijacking.

17555 - (SOL15568) F5 BIG-IP OpenSSL Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3510

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the ssl3_send_client_key_exchange function. Successful exploitation could allow an attacker to cause a denial of service condition.

17556 - (SOL15875) F5 BIG-IP cURL Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-1944

Description

An information disclosure vulnerability is present in some versions of F5 BIG-IP products.

Observation

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

An information disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in cURL component. Successful exploitation could allow an attacker to obtain cookies.

17557 - (SOL15564) F5 BIG-IP OpenSSL TLS ClientHello Message Fragmentation Man-in-The-Middle Attack

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3511

Description

A protocol downgrade issue is present in some versions of F5 BIG-IP systems.

Observation

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

A protocol downgrade issue is present in some versions of F5 BIG-IP systems. The flaw lies in the ssl23_get_client_hello function. Successful exploitation could allow man-in-the-middle attackers to force the use of TLS 1.0 between a client and server that both support later TLS versions.

17558 - (SOL15872) F5 BIG-IP libxml2 Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3660

Description

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

Observation

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

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

17565 - Symantec Web Gateway Command Injection Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2014-7285

Description

A vulnerability in some versions of Symantec Web Gateway could lead to remote code execution.

Observation

A vulnerability in some versions of Symantec Web Gateway could lead to remote code execution.

The flaw occurs as the Symantec Web Gateway management interface is externally accessible from the network environment. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17566 - (SOL15912) F5 BIG-IP Linux Kernel Driver Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3184, CVE-2014-3185, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646

Description

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

Observation

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

Multiple vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in kernel driver. Successful exploitation could allow an attacker to cause a denial of service condition or execute arbitrary code.

17567 - Firebird Server Denial of Server Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-9323

Description

A denial of service vulnerability is present in some versions of Firebird Server.

Observation

Firebird is an open source SQL relational database management system.

A denial of service vulnerability is present in some versions of Firebird Server. The flaw could be triggered by sending a malformed network packet to Firebird server. Successful exploitation could allow a remote attacker to cause a segfault in server.

130032 - Debian Linux 7.0 DSA-3107-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3580

Description

The scan detected that the host is missing the following update:
DSA-3107-1

Observation

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

http://www.debian.org/security/2014/dsa-3107

Debian 7.0
all
subversion_1.6.17dfsg-4+deb7u7

143321 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1685-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8601

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1685-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-12/msg00084.html

SuSE Linux 13.1
x86_64
pdns-recursor-3.6.2-8.4.1
pdns-recursor-debugsource-3.6.2-8.4.1
pdns-recursor-debuginfo-3.6.2-8.4.1

i586
pdns-recursor-3.6.2-8.4.1
pdns-recursor-debugsource-3.6.2-8.4.1
pdns-recursor-debuginfo-3.6.2-8.4.1

SuSE Linux 12.3
x86_64
pdns-recursor-3.6.2-6.4.1
pdns-recursor-debugsource-3.6.2-6.4.1
pdns-recursor-debuginfo-3.6.2-6.4.1

i586
pdns-recursor-3.6.2-6.4.1
pdns-recursor-debugsource-3.6.2-6.4.1
pdns-recursor-debuginfo-3.6.2-6.4.1

143322 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1682-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9087

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1682-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-12/msg00081.html

SuSE Linux 13.1
x86_64
libksba-devel-1.3.0-5.4.1
libksba-debugsource-1.3.0-5.4.1
libksba8-debuginfo-1.3.0-5.4.1
libksba8-1.3.0-5.4.1

i586
libksba-devel-1.3.0-5.4.1
libksba-debugsource-1.3.0-5.4.1
libksba8-debuginfo-1.3.0-5.4.1
libksba8-1.3.0-5.4.1

SuSE Linux 12.3
x86_64
libksba-devel-1.3.0-3.4.1
libksba8-debuginfo-1.3.0-3.4.1
libksba-debugsource-1.3.0-3.4.1
libksba8-1.3.0-3.4.1

i586
libksba-devel-1.3.0-3.4.1
libksba8-debuginfo-1.3.0-3.4.1
libksba-debugsource-1.3.0-3.4.1
libksba8-1.3.0-3.4.1

SuSE Linux 13.2
x86_64
libksba8-debuginfo-1.3.1-4.1
libksba8-1.3.1-4.1
libksba-debugsource-1.3.1-4.1
libksba-devel-1.3.1-4.1

i586
libksba8-debuginfo-1.3.1-4.1
libksba8-1.3.1-4.1
libksba-debugsource-1.3.1-4.1
libksba-devel-1.3.1-4.1

181308 - FreeBSD mutt Denial Of Service Via Crafted Mail Message (c3d43001-8064-11e4-801f-0022156e8794)

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

Risk Level: Medium

CVE: CVE-2014-9116

Description

The scan detected that the host is missing the following update:
mutt -- denial of service via crafted mail message (c3d43001-8064-11e4-801f-0022156e8794)

Observation

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

http://www.vuxml.org/freebsd/c3d43001-8064-11e4-801f-0022156e8794.html

Affected packages:
1.5.22 <= mutt < 1.5.23_7
1.5.22 <= ja-mutt < 1.5.23_7
1.5.22 <= zh-mutt < 1.5.23_7

17559 - (SOL15901) F5 BIG-IP Apache HTTP Server Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2012-2687

Description

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

Observation

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

Multiple cross-site scripting vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in the Apache HTTP Server. Successful exploitation could allow an attacker to execute remote code.

143320 - SuSE Linux 13.2 openSUSE-SU-2014:1688-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8602

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1688-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-12/msg00085.html

SuSE Linux 13.2
x86_64
unbound-debugsource-1.4.22-4.2
unbound-1.4.22-4.2
libunbound2-debuginfo-1.4.22-4.2

unbound-anchor-debuginfo-1.4.22-4.2
unbound-python-debuginfo-1.4.22-4.2
unbound-anchor-1.4.22-4.2
unbound-debuginfo-1.4.22-4.2
unbound-python-1.4.22-4.2
unbound-devel-1.4.22-4.2
libunbound2-1.4.22-4.2

i586
unbound-debugsource-1.4.22-4.2
unbound-1.4.22-4.2
libunbound2-debuginfo-1.4.22-4.2
unbound-anchor-debuginfo-1.4.22-4.2
unbound-python-debuginfo-1.4.22-4.2
unbound-anchor-1.4.22-4.2
unbound-debuginfo-1.4.22-4.2
unbound-python-1.4.22-4.2
unbound-devel-1.4.22-4.2
libunbound2-1.4.22-4.2

noarch
unbound-munin-1.4.22-4.2

130034 - Debian Linux 7.0 DSA-3112-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8145

Description

The scan detected that the host is missing the following update:
DSA-3112-1

Observation

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

http://www.debian.org/security/2014/dsa-3112

Debian 7.0
all
sox_14.4.0-3+deb7u1

17548 - (HPSBMU03043) HP Smart Update Manager Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2014-2608

Description

An information disclosure vulnerability is present in some versions of HP Smart Update Manager.

Observation

HP Smart Update Manager is an application for firmware and driver maintenance on HP servers and blade systems.

An information disclosure vulnerability is present in some versions of HP Smart Update Manager. The flaw lies in HP Smart Update

Manager core component. Successful exploitation could allow an attacker to access potentially sensitive information.

178028 - Gentoo Linux GLSA-201412-32 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3956

Description

The scan detected that the host is missing the following update:
GLSA-201412-32

Observation

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

http://security.gentoo.org/glsa/glsa-201412-32.xml

Affected packages:
mail-mta/sendmail < 8.14.9

17551 - Apple Mac OS X Obsolete Version Detection

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

An obsolete version of Apple Mac OS X is detected on the target.

Observation

Apple Mac OS X is a popular operating system.

An obsolete version of Apple Mac OS X is detected on the target. The vendor no longer provides support or patches for obsolete versions of the product. Use of vulnerable obsolete software may expose the target system to malicious attacks.

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.

10085 - MicroWorld Technologies MailScan Web Based Administration Cross Site Scripting Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2008-3726

Update Details

FASLScript is updated

14410 - Oracle Solaris Obsolete Version Detection

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70073 - freebsd.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70113 - drupal.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70116 - scada.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.