2013-NOV-21

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

15857 - Mozilla Firefox Multiple Vulnerabilities Prior To 25.0

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

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-5590, CVE-2013-5591, CVE-2013-5592, CVE-2013-5593, CVE-2013-5595, CVE-2013-5596, CVE-2013-5597, CVE-2013-5598, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5603, CVE-2013-5604

DISA IAVA: 2013-A-0203

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct clickjacking attacks, cause a denial of service condition, or execute arbitrary code.

15858 - Mozilla Firefox Multiple Vulnerabilities Prior To 25.0

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-5590, CVE-2013-5591, CVE-2013-5592, CVE-2013-5593, CVE-2013-5595, CVE-2013-5596, CVE-2013-5597, CVE-2013-5598, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5603, CVE-2013-5604

DISA IAVA: 2013-A-0203

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct clickjacking attacks, cause a denial of service condition, or execute arbitrary code.

15890 - (VMSA-2013-0012) VMware vCenter Java Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2013-1500, CVE-2013-1571, CVE-2013-2400, CVE-2013-2407, CVE-2013-2412, CVE-2013-2437, CVE-2013-2442, CVE-2013-2443, CVE-2013-2444, CVE-2013-2445, CVE-2013-2446, CVE-2013-2447, CVE-2013-2448, CVE-2013-2449, CVE-2013-2450, CVE-2013-2451, CVE-2013-2452, CVE-2013-2453, CVE-2013-2454, CVE-2013-2455, CVE-2013-2456, CVE-2013-2457, CVE-2013-2458, CVE-2013-2459, CVE-2013-2460, CVE-2013-2461, CVE-2013-2462, CVE-2013-2463, CVE-2013-2464, CVE-2013-2465, CVE-2013-2466, CVE-2013-2467, CVE-2013-2468, CVE-2013-2469, CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-3743, CVE-2013-3744

Description

Multiple vulnerabilities are present in VMware vCenter and VMware Update Manager.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere, and VMware Update Manager is an automated patch management solution for VMware vSphere hosts.

Multiple vulnerabilities are present in VMware vCenter and VMware Update Manager. The flaws lie in Java Runtime Environment component. Successful exploitation could allow an attacker to cause a denial of service or execute arbitrary code.

15891 - (VMSA-2013-0012) VMware vCenter Update Manager Java Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2013-1500, CVE-2013-1571, CVE-2013-2400, CVE-2013-2407, CVE-2013-2412, CVE-2013-2437, CVE-2013-2442, CVE-2013-2443, CVE-2013-2444, CVE-2013-2445, CVE-2013-2446, CVE-2013-2447, CVE-2013-2448, CVE-2013-2449, CVE-2013-2450, CVE-2013-2451, CVE-2013-2452, CVE-2013-2453, CVE-2013-2454, CVE-2013-2455, CVE-2013-2456, CVE-2013-2457, CVE-2013-2458, CVE-2013-2459, CVE-2013-2460, CVE-2013-2461, CVE-2013-2462, CVE-2013-2463, CVE-2013-2464, CVE-2013-2465, CVE-2013-2466, CVE-2013-2467, CVE-2013-2468, CVE-2013-2469, CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-3743, CVE-2013-3744

Description

Multiple vulnerabilities are present in VMware vCenter and VMware Update Manager.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere, and VMware Update Manager is an automated patch management solution for VMware vSphere hosts.

Multiple vulnerabilities are present in VMware vCenter and VMware Update Manager. The flaws lie in Java Runtime Environment component. Successful exploitation could allow an attacker to cause a denial of service or execute arbitrary code.

15903 - Cisco IOS Software Session Initiation Protocol Denial of Service

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

Risk Level: High

CVE: CVE-2013-5553

Description

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

Observation

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

The flaw is due to how a crafted SIP message over IPv4 or IPv6 is handled. Successful exploitation by a remote attacker could result in a denial of service condition.

15950 - (HT6002) Apple Keynote Security Bypass Vulnerability

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

Risk Level: High

CVE: CVE-2013-5148

Description

A security bypass vulnerability is present in some versions of Keynote.

Observation

Keynote is a presentation application developed as a part of the iWork suite.

A security bypass vulnerability is present in some versions of Keynote. The screen may be unlocked if the workstation was put to sleep while in Keynote presentation mode.

15953 - Google Chrome Multiple Vulnerabilities Prior To 31.0.1650.48

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

Risk Level: High

CVE: CVE-2013-2931, CVE-2013-6621, CVE-2013-6622, CVE-2013-6623, CVE-2013-6624, CVE-2013-6625, CVE-2013-6626, CVE-2013-6627, CVE-2013-6628, CVE-2013-6629, CVE-2013-6630, CVE-2013-6631

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 occurs due to multiple use-after-free and other logic issues. Successful exploitation could allow an attacker to obtain sensitive information or execute arbitrary code.

15954 - Google Chrome Multiple Memory Corruption Vulnerabilities Prior To 31.0.1650.57

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

Risk Level: High

CVE: CVE-2013-6632, CVE-2013-6802

Description

Multiple memory corruption vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple memory corruption vulnerabilities are present in some versions of Google Chrome. The flaws occurs due to multiple memory corruption issues. Successful exploitation could allow an attacker to execute arbitrary code.

15955 - (HPSBMU02935) HP LoadRunner Virtual User Generator Code Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-2013-4837, CVE-2013-4838, CVE-2013-4839

Description

Multiple unspecified vulnerabilities are present in some versions of HP LoadRunner.

Observation

HP LoadRunner is a test automation software.

Multiple unspecified vulnerabilities are present in some versions of HP LoadRunner. The flaw lies in virtual user generator component. Successful exploitation could allow an attacker to execute arbitrary code.

15960 - Symantec Workspace Streaming EJBInvokerServlet / JMXInvokerServlet Marshalled Object Vulnerability

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

Risk Level: High

Description

A remote code execution vulnerability is present in some versions of Symantec Workspace Streaming.

Observation

Symantec Workspace Virtualization provides on-demand application provisioning, real-time software license management among other features.

A remote code execution vulnerability is present in some versions of Symantec Workspace Streaming. The flaw lies in the SWS Streamlet Engine service which does not properly restrict access to the invoker/EJBInvokerServlet and invoker/JMXInvokerServlet servlets. Successful exploitation could allow an attacker to execute arbitrary code with system privileges.

15964 - Joomla! Multiple Cross Site Scripting Vulnerabilities

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

Risk Level: High

Description

Multiple cross-site scripting vulnerabilities present in some versions of Joomla!.

Observation

Joomla! is a content management system.

Multiple cross-site scripting vulnerabilities present in some versions of Joomla!. The flaws lie in multiple php files. Successful exploitation could allow an attacker to execute arbitrary code within the security context of the current user.

15966 - (APSB13-27) Vulnerabilities In Adobe ColdFusion

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

Risk Level: High

CVE: CVE-2013-5326, CVE-2013-5328

Description

Multiple vulnerabilities are present in some versions of Adobe ColdFusion.

Observation

Adobe ColdFusion is a web application development platform.

Multiple vulnerabilities are present in some versions of Adobe ColdFusion. The flaws lie in multiple components. It allows unauthorized attackers to read arbitrary files or to inject arbitrary web script or HTML.

The update provided by Adobe bulletin APSB13-27 resolves these issues. The target system appears to be missing this update.

58725 - Debian Linux 7.0 DSA-2797-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2931, CVE-2013-5590, CVE-2013-5595, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5604, CVE-2013-6621, CVE-2013-6622, CVE-2013-6623, CVE-2013-6624, CVE-2013-6625, CVE-2013-6626, CVE-2013-6627, CVE-2013-6628, CVE-2013-6629, CVE-2013-6630, CVE-2013-6631, CVE-2013-6632

Description

The scan detected that the host is missing the following update: DSA-2797-1

Observation

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

http://lists.debian.org/debian-security-announce/2013/msg00211.html
http://lists.debian.org/debian-security-announce/2013/msg00209.html

Debian 7.0
i386
chromium-dbg_31.0.1650.57-1~deb7u1
icedove-dbg_17.0.10-1~deb7u1
icedove-dev_17.0.10-1~deb7u1
icedove_17.0.10-1~deb7u1
iceowl-extension_17.0.10-1~deb7u1
chromium_31.0.1650.57-1~deb7u1

93206 - Mandriva Linux MBS1 MDVSA-2013-267 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5790, CVE-2013-5797, CVE-2013-5800, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5814, CVE-2013-5817, CVE-2013-5820, CVE-2013-5823, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5838, CVE-2013-5840, CVE-2013-5842, CVE-2013-5849, CVE-2013-5850, CVE-2013-5851

Description

The scan detected that the host is missing the following update: MDVSA-2013-267

Observation

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

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2013:267/

Mandriva Linux mbs1

x86_64
java-1.7.0-openjdk-accessibility-1.7.0.60-2.4.3.1
java-1.7.0-openjdk-devel-1.7.0.60-2.4.3.1
java-1.7.0-openjdk-javadoc-1.7.0.60-2.4.3.1
java-1.7.0-openjdk-headless-1.7.0.60-2.4.3.1
java-1.7.0-openjdk-demo-1.7.0.60-2.4.3.1
java-1.7.0-openjdk-src-1.7.0.60-2.4.3.1

93207 - Mandriva Linux MES5 MDVSA-2013-266 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5790, CVE-2013-5797, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5814, CVE-2013-5817, CVE-2013-5820, CVE-2013-5823, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5840, CVE-2013-5842, CVE-2013-5849, CVE-2013-5850

Description

The scan detected that the host is missing the following update: MDVSA-2013-266

Observation

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

https://www.mandriva.com/en/support/security/advisories/mes5/MDVSA-2013:266/

Mandriva Linux mes5
i586
java-1.6.0-openjdk-src-1.6.0.0-35.b24.7
java-1.6.0-openjdk-devel-1.6.0.0-35.b24.7
java-1.6.0-openjdk-javadoc-1.6.0.0-35.b24.7
java-1.6.0-openjdk-demo-1.6.0.0-35.b24.7

x86_64
java-1.6.0-openjdk-src-1.6.0.0-35.b24.7
java-1.6.0-openjdk-devel-1.6.0.0-35.b24.7
java-1.6.0-openjdk-javadoc-1.6.0.0-35.b24.7
java-1.6.0-openjdk-demo-1.6.0.0-35.b24.7

140341 - Red Hat Enterprise Linux RHSA-2013-1518 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-5329, CVE-2013-5330

Description

The scan detected that the host is missing the following update: RHSA-2013-1518

Observation

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

https://rhn.redhat.com/errata/RHSA-2013-1518.html

RHEL5D

x86_64
flash-plugin-11.2.202.327-1.el5

i386
flash-plugin-11.2.202.327-1.el5

RHEL6D
x86_64
flash-plugin-11.2.202.327-1.el6

i386
flash-plugin-11.2.202.327-1.el6

RHEL6WS
x86_64
flash-plugin-11.2.202.327-1.el6

i386
flash-plugin-11.2.202.327-1.el6

RHEL5S
x86_64
flash-plugin-11.2.202.327-1.el5

i386
flash-plugin-11.2.202.327-1.el5

RHEL6S
x86_64
flash-plugin-11.2.202.327-1.el6

i386
flash-plugin-11.2.202.327-1.el6

170219 - Amazon Linux AMI ALAS-2013-238 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4365

Description

The scan detected that the host is missing the following update: ALAS-2013-238

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-238

Amazon Linux AMI
i686
mod_fcgid-2.3.9-1.6.amzn1
mod_fcgid-debuginfo-2.3.9-1.6.amzn1

x86_64
mod_fcgid-2.3.9-1.6.amzn1
mod_fcgid-debuginfo-2.3.9-1.6.amzn1

170220 - Amazon Linux AMI ALAS-2013-239 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4365

Description

The scan detected that the host is missing the following update: ALAS-2013-239

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-239

Amazon Linux AMI
i686
mod24_fcgid-debuginfo-2.3.9-1.7.amzn1
mod24_fcgid-2.3.9-1.7.amzn1

x86_64
mod24_fcgid-debuginfo-2.3.9-1.7.amzn1
mod24_fcgid-2.3.9-1.7.amzn1

170227 - Amazon Linux AMI ALAS-2013-246 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5790, CVE-2013-5797, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5814, CVE-2013-5817, CVE-2013-5820, CVE-2013-5823, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5840, CVE-2013-5842, CVE-2013-5849, CVE-2013-5850

Description

The scan detected that the host is missing the following update: ALAS-2013-246

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-246

Amazon Linux AMI
i686
java-1.6.0-openjdk-demo-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-devel-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-javadoc-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-debuginfo-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-src-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-1.6.0.0-65.1.11.14.57.amzn1

x86_64
java-1.6.0-openjdk-demo-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-devel-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-javadoc-1.6.0.0-65.1.11.14.57.amzn1

java-1.6.0-openjdk-debuginfo-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-src-1.6.0.0-65.1.11.14.57.amzn1
java-1.6.0-openjdk-1.6.0.0-65.1.11.14.57.amzn1

170228 - Amazon Linux AMI ALAS-2013-234 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4396

Description

The scan detected that the host is missing the following update: ALAS-2013-234

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-234

Amazon Linux AMI
i686
xorg-x11-server-common-1.13.0-11.18.amzn1
xorg-x11-server-Xephyr-1.13.0-11.18.amzn1
xorg-x11-server-debuginfo-1.13.0-11.18.amzn1
xorg-x11-server-Xnest-1.13.0-11.18.amzn1
xorg-x11-server-Xvfb-1.13.0-11.18.amzn1

x86_64
xorg-x11-server-common-1.13.0-11.18.amzn1
xorg-x11-server-Xephyr-1.13.0-11.18.amzn1
xorg-x11-server-debuginfo-1.13.0-11.18.amzn1
xorg-x11-server-Xnest-1.13.0-11.18.amzn1
xorg-x11-server-Xvfb-1.13.0-11.18.amzn1

170229 - Amazon Linux AMI ALAS-2013-235 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5790, CVE-2013-5797, CVE-2013-5800, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5814, CVE-2013-5817, CVE-2013-5820, CVE-2013-5823, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5838, CVE-2013-5840, CVE-2013-5842, CVE-2013-5849, CVE-2013-5850, CVE-2013-5851

Description

The scan detected that the host is missing the following update: ALAS-2013-235

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-235

Amazon Linux AMI
i686
java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.2.32.amzn1

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.2.32.amzn1
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.2.32.amzn1
java-1.7.0-openjdk-1.7.0.45-2.4.3.2.32.amzn1
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.2.32.amzn1

x86_64
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.2.32.amzn1
java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.2.32.amzn1
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.2.32.amzn1
java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.2.32.amzn1
java-1.7.0-openjdk-1.7.0.45-2.4.3.2.32.amzn1

177778 - Gentoo Linux GLSA-201311-09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-3696, CVE-2010-3697, CVE-2011-2701, CVE-2012-3547

Description

The scan detected that the host is missing the following update: GLSA-201311-09

Observation

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

http://security.gentoo.org/glsa/glsa-201311-09.xml

Affected packages:
net-dialup/freeradius < 2.2.0

181107 - FreeBSD chromium Multiple Memory Corruption Issues (e62ab2af-4df4-11e3-b0cf-00262d5ed8ee)

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

Risk Level: High

CVE: CVE-2013-6632

Description

The scan detected that the host is missing the following update: chromium -- multiple memory corruption issues (e62ab2af-4df4-11e3-b0cf-00262d5ed8ee)

Observation

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

http://www.vuxml.org/freebsd/e62ab2af-4df4-11e3-b0cf-00262d5ed8ee.html

Affected packages:
chromium < 31.0.1650.57

184217 - Ubuntu Linux 10.04 USN-2029-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2186

Description

The scan detected that the host is missing the following update: USN-2029-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-November/002317.html

Ubuntu 10.04

libcommons-fileupload-java_1.2.1-3ubuntu2.1

184218 - Ubuntu Linux 10.04, 12.04, 12.10, 13.04, 13.10 USN-2030-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606

Description

The scan detected that the host is missing the following update: USN-2030-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-November/002318.html

Ubuntu 10.04

libnss3-1d_3.15.3-0ubuntu0.10.04.1

Ubuntu 12.10

libnss3_3.15.3-0ubuntu0.12.10.1

Ubuntu 13.10

libnss3_3.15.3-0ubuntu0.13.10.1

Ubuntu 12.04

libnss3_3.15.3-0ubuntu0.12.04.1

Ubuntu 13.04

libnss3_3.15.3-0ubuntu0.13.04.1

187317 - Fedora Linux 20 FEDORA-2013-21000 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4551

Description

The scan detected that the host is missing the following update: FEDORA-2013-21000

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/121867.html

Fedora Core 20

xen-4.3.1-2.fc20

15940 - Ruby on Rails Action Mailer Log Subscriber Component Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-4389

Description

A denial of service vulnerability exists in some versions of Ruby on Rails.

Observation

Ruby on Rails is web application framework.

A denial of service vulnerability exists in some versions of Ruby on Rails. The flaw lies in the log subscriber component of Action Mailer. Successful exploitation by a remote attacker could cause a denial of service.

15951 - IBM Domino Web Administrator Cross-Site Scripting and Request Forgery Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2013-4050, CVE-2013-4051, CVE-2013-4055

Description

Multiple cross-site scripting and request forgery vulnerabilities are present in some versions of IBM Domino Web Administrator.

Observation

IBM Domino is a product that provides enterprise-grade e-mail, collaboration capabilities, and a custom application platform. IBM Domino Web Administrator allows users to manage and view settings for an IBM Domino server.

Multiple cross-site scripting and request forgery vulnerabilities are present in some versions of IBM Domino Web Administrator. The flaws are due to the Web Administrator component which does not properly sanitize user input or perform proper validity checks on certain HTTP requests. Successful exploitation by a remote attacker could result in the execution of arbitrary code or the disclosure of sensitive information.

15952 - IBM Domino Web Administrator Cross-Site Scripting and Request Forgery Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2013-4050, CVE-2013-4051, CVE-2013-4055

Description

Multiple cross-site scripting and request forgery vulnerabilities are present in some versions of IBM Domino Web Administrator.

Observation

IBM Domino is a product that provides enterprise-grade e-mail, collaboration capabilities, and a custom application platform. IBM Domino Web Administrator allows users to manage and view settings for an IBM Domino server.

Multiple cross-site scripting and request forgery vulnerabilities are present in some versions of IBM Domino Web Administrator. The flaws are due to the Web Administrator component which does not properly sanitize user input or perform proper validity checks on certain HTTP requests. Successful exploitation by a remote attacker could result in the execution of arbitrary code or the disclosure of sensitive information.

15956 - Apple iOS App and In-App Purchases Security Bypass Vulnerability

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Medium

CVE: CVE-2013-5193

Description

A security bypass vulnerability is present in some versions of Apple iOS.

Observation

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

A security bypass vulnerability is present in some versions of Apple iOS. The App Store in Apple iOS does not properly enforce an intended transaction-time password requirement, it allows local users to complete a purchase by leveraging previous entry of Apple ID credentials.

15957 - Cisco IOS Software SSL VPN Interface Queue Wedge Denial of Service

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

Risk Level: Medium

CVE: CVE-2013-6686

Description

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

Observation

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

The flaw lies in the Datagram Transport Layer Security function. Successful exploitation by a remote attacker could result in a denial of service condition.

15959 - VMware Workstation/Player Shared Library Privilege Escalation

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-5972

Description

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

Observation

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

The flaw is due to how shared libraries are handled. Successful exploitation could allow a local user to gain elevated privileges.

15961 - BlackBerry Link Peer Manager Component Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-3694

Description

A security bypass is present in some versions of BlackBerry Link.

Observation

BlackBerry Link is BlackBerry Limited software which allows management of data between BlackBerry 10 devices and personal computers.

A security bypass is present in some versions of BlackBerry Link. The flaw lies in the Peer Manager component. Successful exploitation by a remote attacker could result in a disclosure of the BlackBerry Link remote file access folder contents or a remote code execution.

15962 - Cisco Adaptive Security Appliance Software Phone Proxy Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-6682

Description

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

Observation

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

The flaw lies in the phone proxy feature. Successful exploitation by a remote attacker could result in a denial of service condition.

15963 - Cisco Adaptive Security Appliance Software Auto-Update Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-5568

Description

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

Observation

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

The flaw lies in the auto-update feature. Successful exploitation by a remote attacker could result in a denial of service condition.

15967 - Cisco NX-OS Nexus 4000 Series Switches IPv6 Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-6683

Description

A denial of service vulnerability is present in some versions of Cisco NX-OS Software.

Observation

A denial of service vulnerability is present in some versions of Cisco NX-OS Software.

The flaw lies in the IPv6 packet handling routine. Successful exploitation by a remote attacker could result in a denial of service condition.

15968 - Cisco MDS 9000 NX-OS Software Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-5566

Description

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

Observation

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

The flaw is due to improper handling of Virtual Router Redundancy Protocol (VRRP) frames. Successful exploitation by a remote attacker could result in a denial of service condition.

88560 - Slackware Linux 14.0, 14.1 SSA:2013-322-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4475, CVE-2013-4476

Description

The scan detected that the host is missing the following update: SSA:2013-322-03

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=2013&m=slackware-security.420125

Slackware 14.0
x86_64
samba-3.6.20-x86_64-1

Slackware 14.1
x86_64
samba-4.1.1-x86_64-1

88561 - Slackware Linux 14.1 SSA:2013-322-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4548

Description

The scan detected that the host is missing the following update: SSA:2013-322-02

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=2013&m=slackware-security.356319

Slackware 14.1
x86_64
openssh-6.4p1-x86_64-1

95842 - SuSE Linux 13.1 openSUSE-SU-2013:1726-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4548

Description

The scan detected that the host is missing the following update: openSUSE-SU-2013:1726-1

Observation

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

http://lists.opensuse.org/opensuse-security-announce/2013-11/msg00017.html

SuSE Linux 13.1
i586
openssh-askpass-gnome-6.2p2-3.4.1
openssh-6.2p2-3.4.1
openssh-askpass-gnome-debuginfo-6.2p2-3.4.1
openssh-debugsource-6.2p2-3.4.1
openssh-debuginfo-6.2p2-3.4.1

95843 - SuSE Linux 11.4 openSUSE-SU-2013:1717-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5329, CVE-2013-5330

Description

The scan detected that the host is missing the following update: openSUSE-SU-2013:1717-1

Observation

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

For more information see:

http://lists.opensuse.org/opensuse-security-announce/2013-11/msg00016.html

SuSE Linux 11.4
i586
flash-player-kde4-11.2.202.327-79.1
flash-player-gnome-11.2.202.327-79.1
flash-player-11.2.202.327-79.1

170217 - Amazon Linux AMI ALAS-2013-236 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4351, CVE-2013-4402

Description

The scan detected that the host is missing the following update: ALAS-2013-236

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-236

Amazon Linux AMI
i686
gnupg-1.4.15-1.21.amzn1
gnupg-debuginfo-1.4.15-1.21.amzn1

x86_64
gnupg-1.4.15-1.21.amzn1
gnupg-debuginfo-1.4.15-1.21.amzn1

170218 - Amazon Linux AMI ALAS-2013-237 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4351, CVE-2013-4402

Description

The scan detected that the host is missing the following update: ALAS-2013-237

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-237

Amazon Linux AMI
i686
gnupg2-2.0.22-1.24.amzn1
gnupg2-smime-2.0.22-1.24.amzn1
gnupg2-debuginfo-2.0.22-1.24.amzn1

x86_64
gnupg2-debuginfo-2.0.22-1.24.amzn1
gnupg2-2.0.22-1.24.amzn1
gnupg2-smime-2.0.22-1.24.amzn1

170222 - Amazon Linux AMI ALAS-2013-241 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-2408, CVE-2013-4238

Description

The scan detected that the host is missing the following update: ALAS-2013-241

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-241

Amazon Linux AMI
i686
python26-tools-2.6.9-1.40.amzn1
python26-devel-2.6.9-1.40.amzn1
python26-test-2.6.9-1.40.amzn1
python26-2.6.9-1.40.amzn1
python26-libs-2.6.9-1.40.amzn1
python26-debuginfo-2.6.9-1.40.amzn1

x86_64
python26-tools-2.6.9-1.40.amzn1
python26-devel-2.6.9-1.40.amzn1
python26-libs-2.6.9-1.40.amzn1
python26-test-2.6.9-1.40.amzn1
python26-2.6.9-1.40.amzn1
python26-debuginfo-2.6.9-1.40.amzn1

170223 - Amazon Linux AMI ALAS-2013-242 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4251

Description

The scan detected that the host is missing the following update: ALAS-2013-242

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-242

Amazon Linux AMI
i686
scipy-0.12.1-1.7.amzn1

scipy-debuginfo-0.12.1-1.7.amzn1

x86_64
scipy-0.12.1-1.7.amzn1
scipy-debuginfo-0.12.1-1.7.amzn1

170225 - Amazon Linux AMI ALAS-2013-244 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0255, CVE-2013-1900

Description

The scan detected that the host is missing the following update: ALAS-2013-244

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-244

Amazon Linux AMI
i686
postgresql8-docs-8.4.18-1.39.amzn1
postgresql8-8.4.18-1.39.amzn1
postgresql8-plperl-8.4.18-1.39.amzn1
postgresql8-plpython-8.4.18-1.39.amzn1
postgresql8-debuginfo-8.4.18-1.39.amzn1
postgresql8-libs-8.4.18-1.39.amzn1
postgresql8-pltcl-8.4.18-1.39.amzn1
postgresql8-contrib-8.4.18-1.39.amzn1
postgresql8-server-8.4.18-1.39.amzn1
postgresql8-test-8.4.18-1.39.amzn1
postgresql8-devel-8.4.18-1.39.amzn1

x86_64
postgresql8-docs-8.4.18-1.39.amzn1
postgresql8-8.4.18-1.39.amzn1
postgresql8-plperl-8.4.18-1.39.amzn1
postgresql8-plpython-8.4.18-1.39.amzn1
postgresql8-debuginfo-8.4.18-1.39.amzn1
postgresql8-libs-8.4.18-1.39.amzn1
postgresql8-pltcl-8.4.18-1.39.amzn1
postgresql8-contrib-8.4.18-1.39.amzn1
postgresql8-server-8.4.18-1.39.amzn1
postgresql8-test-8.4.18-1.39.amzn1
postgresql8-devel-8.4.18-1.39.amzn1

170226 - Amazon Linux AMI ALAS-2013-245 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2673

Description

The scan detected that the host is missing the following update: ALAS-2013-245

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-245

Amazon Linux AMI
i686
gc-7.1-12.6.amzn1
gc-debuginfo-7.1-12.6.amzn1
gc-devel-7.1-12.6.amzn1

x86_64
gc-7.1-12.6.amzn1
gc-debuginfo-7.1-12.6.amzn1
gc-devel-7.1-12.6.amzn1

177776 - Gentoo Linux GLSA-201311-07 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2008-1102, CVE-2008-1103, CVE-2009-3850

Description

The scan detected that the host is missing the following update: GLSA-201311-07

Observation

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

http://security.gentoo.org/glsa/glsa-201311-07.xml

Affected packages:
media-gfx/blender < 2.49b-r2

177777 - Gentoo Linux GLSA-201311-10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2008-1097, CVE-2009-1882, CVE-2009-3736, CVE-2013-4589

Description

The scan detected that the host is missing the following update: GLSA-201311-10

Observation

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

http://security.gentoo.org/glsa/glsa-201311-10.xml

Affected packages:
media-gfx/graphicsmagick < 1.3.18

177779 - Gentoo Linux GLSA-201311-08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-4274

Description

The scan detected that the host is missing the following update: GLSA-201311-08

Observation

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

http://security.gentoo.org/glsa/glsa-201311-08.xml

Affected packages:
media-libs/netpbm < 10.49.00

181110 - FreeBSD samba ACLs Are Not Checked On Opening An Alternate Data Stream On A File Or Directory (a4f08579-516c-11e3-9b62-000c292e4

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

Risk Level: Medium

CVE: CVE-2013-4475

Description

The scan detected that the host is missing the following update: samba -- ACLs are not checked on opening an alternate data stream on a file or directory (a4f08579-516c-11e3-9b62-000c292e4fd8)

Observation

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

http://www.vuxml.org/freebsd/a4f08579-516c-11e3-9b62-000c292e4fd8.html

Affected packages:
3.6.* < samba36 < 3.6.20
4.0.* < samba4 < 4.0.11
4.1.* < samba41 < 4.1.1

187326 - Fedora Linux 19 FEDORA-2013-14814 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4111

Description

The scan detected that the host is missing the following update: FEDORA-2013-14814

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/121876.html

Fedora Core 19

python-glanceclient-0.9.0-3.fc19

33234 - Sun Solaris 146697-04 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: 146697-04

Observation

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

https://getupdates.oracle.com/readme/146697-04

SunOS 5.10(x86): ksh patch

SOLARIS_10_x86

SUNWxcu6:11.10.0,REV=2005.01.21.16.34
SUNWcsu:11.10.0,REV=2005.01.21.16.34

33235 - Sun Solaris 146696-04 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: 146696-04

Observation

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

https://getupdates.oracle.com/readme/146696-04

SunOS 5.10: ksh patch

SOLARIS_10

SUNWxcu6:11.10.0,REV=2005.01.21.15.53
SUNWcsu:11.10.0,REV=2005.01.21.15.53

33236 - Sun Solaris 113911-02 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: 113911-02

Observation

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

https://getupdates.oracle.com/readme/113911-02

SunOS 5.9: Asian SunOS 4.x Binary Compatibility(BCP) patch

SOLARIS_9

SUNWcbcp:9.0,REV=2001.11.06.10.49
SUNWhbcp:9.0,REV=2001.11.06.10.45
SUNWkbcp:9.0,REV=2001.11.06.10.42

58724 - Debian Linux 6.0, 7.0 DSA-2795-2 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: DSA-2795-2

Observation

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

http://lists.debian.org/debian-security-announce/2013/msg00210.html

Debian 7.0
i386
lighttpd-mod-webdav_1.4.31-4+deb7u2
lighttpd-mod-mysql-vhost_1.4.31-4+deb7u2
lighttpd-mod-magnet_1.4.31-4+deb7u2
lighttpd-mod-trigger-b4-dl_1.4.31-4+deb7u2
lighttpd_1.4.31-4+deb7u2
lighttpd-mod-cml_1.4.31-4+deb7u2

Debian 6.0
i386
lighttpd_1.4.28-2+squeeze1.5
lighttpd-mod-webdav_1.4.28-2+squeeze1.5
lighttpd-mod-mysql-vhost_1.4.28-2+squeeze1.5
lighttpd-mod-trigger-b4-dl_1.4.28-2+squeeze1.5
lighttpd-mod-cml_1.4.28-2+squeeze1.5
lighttpd-mod-magnet_1.4.28-2+squeeze1.5

58726 - Debian Linux 6.0, 7.0 DSA-2798-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4545

Description

The scan detected that the host is missing the following update: DSA-2798-1

Observation

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

http://lists.debian.org/debian-security-announce/2013/msg00212.html

Debian 7.0
i386
libcurl3_7.26.0-1+wheezy5
libcurl4-nss-dev_7.26.0-1+wheezy5
libcurl3-dbg_7.26.0-1+wheezy5
libcurl3-gnutls_7.26.0-1+wheezy5
libcurl4-openssl-dev_7.26.0-1+wheezy5
curl_7.26.0-1+wheezy5
libcurl4-gnutls-dev_7.26.0-1+wheezy5
libcurl3-nss_7.26.0-1+wheezy5

Debian 6.0
i386
libcurl3-gnutls_7.21.0-2.1+squeeze5
libcurl3-dbg_7.21.0-2.1+squeeze5
libcurl4-openssl-dev_7.21.0-2.1+squeeze5
libcurl3_7.21.0-2.1+squeeze5
curl_7.21.0-2.1+squeeze5
libcurl4-gnutls-dev_7.21.0-2.1+squeeze5

58727 - Debian Linux 6.0, 7.0 DSA-2796-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4495

Description

The scan detected that the host is missing the following update: DSA-2796-1

Observation

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

http://lists.debian.org/debian-security-announce/2013/msg00208.html

Debian 7.0
i386
torque-scheduler_2.4.16+dfsg-1+deb7u2
libtorque2-dev_2.4.16+dfsg-1+deb7u2
libtorque2_2.4.16+dfsg-1+deb7u2
torque-server_2.4.16+dfsg-1+deb7u2
torque-pam_2.4.16+dfsg-1+deb7u2
torque-client-x11_2.4.16+dfsg-1+deb7u2
torque-common_2.4.16+dfsg-1+deb7u2
torque-client_2.4.16+dfsg-1+deb7u2
torque-mom_2.4.16+dfsg-1+deb7u2

Debian 6.0
i386
torque-client-x11_2.4.8+dfsg-9squeeze3
libtorque2_2.4.8+dfsg-9squeeze3

torque-mom_2.4.8+dfsg-9squeeze3
torque-pam_2.4.8+dfsg-9squeeze3
torque-common_2.4.8+dfsg-9squeeze3
torque-server_2.4.8+dfsg-9squeeze3
libtorque2-dev_2.4.8+dfsg-9squeeze3
torque-scheduler_2.4.8+dfsg-9squeeze3
torque-client_2.4.8+dfsg-9squeeze3

88558 - Slackware Linux 13.37, 14.0, 14.1 SSA:2013-322-01 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: SSA:2013-322-01

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=2013&m=slackware-security.446719

Slackware 14.0
x86_64
mozilla-firefox-17.0.11esr-x86_64-1

Slackware 13.37
x86_64
mozilla-firefox-17.0.11esr-x86_64-1

Slackware 14.1
x86_64
mozilla-firefox-24.1.1esr-x86_64-1

88559 - Slackware Linux 14.0, 14.1 SSA:2013-322-04 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: SSA:2013-322-04

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=2013&m=slackware-security.491955

Slackware 14.0
x86_64
seamonkey-2.22-x86_64-1
seamonkey-solibs-2.22-x86_64-1

Slackware 14.1
x86_64
seamonkey-2.22-x86_64-1

seamonkey-solibs-2.22-x86_64-1

93208 - Mandriva Linux MBS1 MDVSA-2013-268 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4495

Description

The scan detected that the host is missing the following update: MDVSA-2013-268

Observation

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

https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2013:268/

Mandriva Linux mbs1
x86_64
torque-server-4.1.5.1-1.1
torque-client-4.1.5.1-1.1
torque-sched-4.1.5.1-1.1
lib64torque-devel-4.1.5.1-1.1
torque-mom-4.1.5.1-1.1
torque-gui-4.1.5.1-1.1
torque-4.1.5.1-1.1

170221 - Amazon Linux AMI ALAS-2013-240 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-3839

Description

The scan detected that the host is missing the following update: ALAS-2013-240

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-240

Amazon Linux AMI
i686
mysql51-bench-5.1.72-1.64.amzn1
mysql51-server-5.1.72-1.64.amzn1
mysql51-libs-5.1.72-1.64.amzn1
mysql51-embedded-5.1.72-1.64.amzn1
mysql51-embedded-devel-5.1.72-1.64.amzn1
mysql51-common-5.1.72-1.64.amzn1
mysql51-debuginfo-5.1.72-1.64.amzn1
mysql51-5.1.72-1.64.amzn1
mysql51-test-5.1.72-1.64.amzn1
mysql51-devel-5.1.72-1.64.amzn1

x86_64
mysql51-bench-5.1.72-1.64.amzn1
mysql51-server-5.1.72-1.64.amzn1
mysql51-embedded-5.1.72-1.64.amzn1
mysql51-embedded-devel-5.1.72-1.64.amzn1
mysql51-common-5.1.72-1.64.amzn1
mysql51-devel-5.1.72-1.64.amzn1
mysql51-debuginfo-5.1.72-1.64.amzn1
mysql51-5.1.72-1.64.amzn1
mysql51-test-5.1.72-1.64.amzn1
mysql51-libs-5.1.72-1.64.amzn1

170224 - Amazon Linux AMI ALAS-2013-243 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-1445

Description

The scan detected that the host is missing the following update: ALAS-2013-243

Observation

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

http://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2013-243

Amazon Linux AMI
i686
python-crypto-debuginfo-2.6.1-1.7.amzn1
python-crypto-2.6.1-1.7.amzn1

x86_64
python-crypto-debuginfo-2.6.1-1.7.amzn1
python-crypto-2.6.1-1.7.amzn1

181108 - FreeBSD nginx Request Line Parsing Vulnerability (94b6264a-5140-11e3-8b22-f0def16c5c1b)

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

Risk Level: Low

CVE: CVE-2013-4547

Description

The scan detected that the host is missing the following update: nginx -- Request line parsing vulnerability (94b6264a-5140-11e3-8b22-f0def16c5c1b)

Observation

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

http://www.vuxml.org/freebsd/94b6264a-5140-11e3-8b22-f0def16c5c1b.html

Affected packages:
0.8.41 <= nginx < 1.4.4,1
0.8.41 <= nginx-devel < 1.5.7

181109 - FreeBSD samba Private Key In Key.pem World Readable (479efd57-516e-11e3-9b62-000c292e4fd8)

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

Risk Level: Low

CVE: CVE-2013-4476

Description

The scan detected that the host is missing the following update: samba -- Private key in key.pem world readable (479efd57-516e-11e3-9b62-000c292e4fd8)

Observation

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

http://www.vuxml.org/freebsd/479efd57-516e-11e3-9b62-000c292e4fd8.html

Affected packages:
4.0.* < samba4 < 4.0.11
4.1.* < samba41 < 4.1.1

187313 - Fedora Linux 19 FEDORA-2013-20814 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4519

Description

The scan detected that the host is missing the following update: FEDORA-2013-20814

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/121923.html
http://lists.fedoraproject.org/pipermail/package-announce/2013-November/121922.html

Fedora Core 19

ReviewBoard-1.7.18-1.fc19
python-djblets-0.7.23-1.fc19

187314 - Fedora Linux 19 FEDORA-2013-18794 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: FEDORA-2013-18794

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/121929.html

Fedora Core 19

phpMyAdmin-3.5.8.2-1.fc19

187315 - Fedora Linux 20 FEDORA-2013-21006 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4550

Description

The scan detected that the host is missing the following update: FEDORA-2013-21006

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/121868.html

Fedora Core 20

bip-0.8.9-1.fc20

187316 - Fedora Linux 18 FEDORA-2013-20410 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4473, CVE-2013-4474

Description

The scan detected that the host is missing the following update: FEDORA-2013-20410

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122126.html

Fedora Core 18

poppler-0.20.2-17.fc18

187318 - Fedora Linux 19 FEDORA-2013-20628 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4466, CVE-2013-4487

Description

The scan detected that the host is missing the following update: FEDORA-2013-20628

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122155.html

Fedora Core 19

gnutls-3.1.16-1.fc19

187319 - Fedora Linux 20 FEDORA-2013-21456 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-1417

Description

The scan detected that the host is missing the following update: FEDORA-2013-21456

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122175.html

Fedora Core 20

krb5-1.11.3-32.fc20

187320 - Fedora Linux 18 FEDORA-2013-18802 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: FEDORA-2013-18802

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/121909.html

Fedora Core 18

phpMyAdmin-3.5.8.2-1.fc18

187321 - Fedora Linux 20 FEDORA-2013-20929 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4509

Description

The scan detected that the host is missing the following update: FEDORA-2013-20929

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/121897.html

Fedora Core 20

ibus-pinyin-1.5.0-5.fc20

187322 - Fedora Linux 19 FEDORA-2013-20993 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4509

Description

The scan detected that the host is missing the following update: FEDORA-2013-20993

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122205.html

Fedora Core 19

ibus-pinyin-1.5.0-5.fc19

187323 - Fedora Linux 20 FEDORA-2013-20940 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: FEDORA-2013-20940

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122168.html

Fedora Core 20

prboom-plus-2.5.1.3-3.fc20

187324 - Fedora Linux 19 FEDORA-2013-20988 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: FEDORA-2013-20988

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122214.html

Fedora Core 19

prboom-plus-2.5.1.3-3.fc19

187325 - Fedora Linux 20 FEDORA-2013-18705 Update Is Not Installed

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: FEDORA-2013-18705

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122059.html

Fedora Core 20

phpMyAdmin-3.5.8.2-1.fc20

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.

2684 - OpenSSH buffer_init Buffer Management Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1156

CVE: CVE-2003-0693, CVE-2003-0695

DISA IAVA: 2003-T-0020,2001-T-0017,2001-A-0013

Update Details

Description is updated.
Observation is updated.

13973 - BlackBerry Browser Null Ptr Denial Of Service Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Blackberry

Risk Level: High

CVE: CVE-2009-2575

Update Details

Name is updated.

15689 - Mitsubishi MC-WorkX IcoLaunch ActiveX Control Remote Code Execution Vulnerability

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

Risk Level: High

Update Details

Recommendation is updated.

15845 - NETGEAR WNDR3700v4 ping6 Diagnostic Page Command Injection Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: High

Update Details

Recommendation is updated.

2217 - OpenSSH PKCS Session Key Retrieval

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

CVE: CVE-2001-0361

DISA IAVA: 2001-A-0013

Update Details

Observation is updated.

13972 - BlackBerry Browser Insufficient Certificate Warning Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Blackberry

Risk Level: Medium

CVE: CVE-2009-3477

Update Details

Name is updated.

15423 - DotNetNuke DNNArticle Module "categoryid" SQL Injection Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-5117

Update Details

Recommendation is updated.

15600 - TP-LINK TD-W8951ND Router Cross-Site Scripting and Request Forgery Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

Update Details

Recommendation is updated.

15619 - Cisco Prime Network Control System (NCS) Health Monitor Login Page Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2012-5990

Update Details

Recommendation is updated.

15758 - WordPress WP Ultimate Email Marketer Plugin Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2013-3263, CVE-2013-3264

Update Details

Recommendation is updated.

95825 - SuSE SLES 10 libxslt-8733 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2011-3970, CVE-2012-2825, CVE-2012-6139, CVE-2013-4520

Update Details

FASLScript is updated.

33153 - Sun Solaris 150584-02 Update Is Not Installed

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

Risk Level: Low

Update Details

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

33155 - Sun Solaris 150585-02 Update Is Not Installed

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

Risk Level: Low

Update Details

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

181104 - FreeBSD OpenSSH Memory Corruption In Sshd (5709d244-4873-11e3-8a46-000d601460a4)

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

Risk Level: Low

Update Details

FASLScript is updated.

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

Update Details

FASLScript is updated.

70087 - hp.fasl3.inc

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

Risk Level: Informational

Update Details

FASLScript is updated.

DELETED CHECKS

32851 - Sun Solaris 146055-07 Update Is Not Installed

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

Risk Level: Low

32853 - Sun Solaris 146054-07 Update Is Not Installed

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

Risk Level: Low

ADDITIONAL NOTES

32851, 32853 - were flagged as obsolete by the vendor.

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.