

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

15763 - (APSB13-24) Vulnerability In Adobe RoboHelp

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

Risk Level: High

CVE: CVE-2013-5327

Description

A remote code execution vulnerability is present in Adobe RoboHelp.

Observation

Adobe RoboHelp is a tool used to create help document.

A remote code execution vulnerability is present in Adobe RoboHelp. The flaw occurs due to a memory corruption issue. Successful exploitation could allow an attacker to execute arbitrary code or cause denial of service.

The update provided by Adobe bulletin APSB13-24 resolves this issue. The target system appears to be missing this update.

15782 - Moore Industries NCS Configuration Denial of Service

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

Risk Level: High

Description

A denial of service vulnerability is present in some versions of Moore Industries NCS Configuration.

Observation

A denial of service vulnerability is present in some versions of Moore Industries NCS Configuration.

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

15793 - Cisco NX-OS Pipe Handling OS Command Injection Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2012-4076

Description

An arbitrary command execute vulnerability is present in some versions of Cisco NX-OS.

Observation

Cisco NX-OS is networking software.

An arbitrary command execute vulnerability is present in some versions of Cisco NX-OS. The flaw lies in VSH parsing of pipe. Successful exploitation by an authenticated local attacker may result in the execution of arbitrary commands.

15794 - McAfee Web Reporter Tomcat EJBServlet Marshalled Object Remote Code Execution

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

Risk Level: High

Description

A remote code execution vulnerability is present in some versions of McAfee Web Reporter.

Observation

A remote code execution vulnerability is present in some versions of McAfee Web Reporter.

The flaw is due to how certain HTTP requests containing marshalled Java objects are handled. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

15795 - Cisco NX-OS sed "e" Option Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2012-4077

Description

A privilege escalation vulnerability is present in some versions of Cisco NX-OS.

Observation

Cisco NX-OS is networking software.

A privilege escalation vulnerability is present in some versions of Cisco NX-OS. The flaw lies in VSH parsing of SED parameters. Successful exploitation by an authenticated local attacker may result in the execution of arbitrary commands.

15797 - BlackBerry Enterprise Service JBoss RMI Arbitrary Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2013-3693

Description

A remote code execution vulnerability is present in some versions of BlackBerry Enterprise Service.

Observation

BlackBerry Enterprise Service is RIM multi-platform device management.

A remote code execution vulnerability is present in some versions of BlackBerry Enterprise Service. The flaw is due to an unrestricted access to JBoss Remote Method Invocation (RMI). Successful exploitation by a remote attacker could result in the execution of arbitrary code.

15798 - D-Link Router User Agent Backdoor Security Bypass Vulnerability

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

Risk Level: High

Description

A security bypass vulnerability is present in some versions of D-Link Router firmware.

Observation

D-Link Router is the device used to route network data packets.

A security bypass vulnerability is present in some versions of D-Link Router. The flaw occurs due to a backdoor string used in User-Agent. Successful exploitation could allow an attacker to bypass web interface authentication.

15803 - (VMSA-2013-0012) VMware ESXi Server hostd-vmdb Service Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-5970

Description

A denial of service vulnerability is present in some versions of VMware ESXi.

Observation

VMware ESXi is a popular virtualization platform.

A denial of service vulnerability is present in some versions of VMware ESXi. The flaw resides in the handling of management traffic by hostd-vmdb service. An attacker may exploit this vulnerability to trigger a denial of service.

15804 - (VMSA-2013-0012) VMware ESX Server hostd-vmdb Service Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-5970

Description

A denial of service vulnerability is present in some versions of VMware ESX.

Observation

VMware ESX is a popular virtualization platform.

A denial of service vulnerability is present in some versions of VMware ESX. The flaw resides in the handling of management traffic by hostd-vmdb service. An attacker may exploit this vulnerability to trigger a denial of service.

15807 - (HT5982) Apple Mac OS X Java Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5776, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5787, CVE-2013-5789, CVE-2013-5790, CVE-2013-5797, CVE-2013-5801, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5812, CVE-2013-5814, CVE-2013-5817, CVE-2013-5818, CVE-2013-5819, CVE-2013-5820, CVE-2013-5823, CVE-2013-5824, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5831, CVE-2013-5832, CVE-2013-5840, CVE-2013-5842, CVE-2013-5843, CVE-2013-5848, CVE-2013-5849, CVE-2013-5850

Description

Multiple vulnerabilities are present in some versions of Apple Mac OS X Java.

Observation

Apple Mac OS X is a popular operating system.

Multiple vulnerabilities are present in some versions of Apple Mac OS X Java. The flaws lie in several Java components. Successful exploitation could allow remote attackers to execute arbitrary code outside the Java sandbox.

15813 - Google Chrome Multiple Vulnerabilities Prior To 30.0.1599.101

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

Risk Level: High

CVE: CVE-2013-2925, CVE-2013-2926, CVE-2013-2927, CVE-2013-2928

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 are due to multiple memory usage errors. Successful exploitation could allow a remote attacker to execute arbitrary code.

15814 - VideoLAN VLC Media Player mp4a Packetizer Remote Code Execution

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

Risk Level: High

CVE: CVE-2013-4388

Description

A remote code execution vulnerability is present in some versions of VideoLAN VLC Media Player.

Observation

A remote code execution vulnerability is present in some versions of VideoLAN VLC Media Player.

The flaw is due to a buffer overflow in the mp4a packetizer. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

58711 - Debian Linux 6.0 DSA-2780-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-2750, CVE-2013-3839

Description

The scan detected that the host is missing the following update: DSA-2780-1

Observation

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

<http://lists.debian.org/debian-security-announce/2013/msg00191.html>

Debian 6.0

i386

libmysqld-dev_5.1.72-2

libmysqld-pic_5.1.72-2

libmysqlclient16_5.1.72-2

mysql-server-5.1_5.1.72-2

libmysqlclient-dev_5.1.72-2

mysql-server-core-5.1_5.1.72-2

mysql-client-5.1_5.1.72-2

85626 - CentOS 6 CESA-2013-1426 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4396

Description

The scan detected that the host is missing the following update: CESA-2013-1426

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2013-October/019973.html>

CentOS 6

noarch

xorg-x11-server-source-1.13.0-11.1.el6.centos.2

i686

xorg-x11-server-devel-1.13.0-11.1.el6.centos.2

xorg-x11-server-common-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xephyr-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xnest-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xvfb-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xorg-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xdmx-1.13.0-11.1.el6.centos.2

x86_64

xorg-x11-server-devel-1.13.0-11.1.el6.centos.2

xorg-x11-server-common-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xephyr-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xnest-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xvfb-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xorg-1.13.0-11.1.el6.centos.2

xorg-x11-server-Xdmx-1.13.0-11.1.el6.centos.2

85627 - CentOS 5 CESA-2013-1447 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS 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: CESA-2013-1447

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2013-October/019980.html>

CentOS 5

x86_64

java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.el5_10

i386

java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.el5_10

88555 - Slackware Linux 12.1, 12.2, 13.0, 13.1, 13.37, 14.0 SSA:2013-290-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-2088, CVE-2012-2113, CVE-2012-4447, CVE-2012-4564, CVE-2013-1960, CVE-2013-1961, CVE-2013-4231, CVE-2013-4232, CVE-2013-4244

Description

The scan detected that the host is missing the following update: SSA:2013-290-01

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.543193>

Slackware 13.1

x86_64

libtiff-3.9.7-x86_64-1

Slackware 13.37

x86_64

libtiff-3.9.7-x86_64-1

Slackware 12.1

i486

libtiff-3.9.7-i486-1

Slackware 14.0
x86_64
libtiff-3.9.7-x86_64-1

Slackware 13.0
x86_64
libtiff-3.9.7-x86_64-1

Slackware 12.2
i486
libtiff-3.9.7-i486-1

91367 - Oracle Enterprise Linux ELSA-2013-1451 Update Is Not Installed

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

Risk Level: High

Description

The scan detected that the host is missing the following update: ELSA-2013-1451

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-October/003754.html>

OEL6
x86_64
java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.2.0.1.el6_4
java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.2.0.1.el6_4
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.2.0.1.el6_4
java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.2.0.1.el6_4
java-1.7.0-openjdk-1.7.0.45-2.4.3.2.0.1.el6_4

i386
java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.2.0.1.el6_4
java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.2.0.1.el6_4
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.2.0.1.el6_4
java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.2.0.1.el6_4
java-1.7.0-openjdk-1.7.0.45-2.4.3.2.0.1.el6_4

91368 - Oracle Enterprise Linux ELSA-2013-1447 Update Is Not Installed

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

Risk Level: High

Description

The scan detected that the host is missing the following update: ELSA-2013-1447

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-October/003751.html>

OEL5

x86_64

java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.0.1.el5_10

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.0.1.el5_10

java-1.7.0-openjdk-1.7.0.45-2.4.3.1.0.1.el5_10

java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.0.1.el5_10

java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.0.1.el5_10

i386

java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.0.1.el5_10

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.0.1.el5_10

java-1.7.0-openjdk-1.7.0.45-2.4.3.1.0.1.el5_10

java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.0.1.el5_10

java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.0.1.el5_10

93197 - Mandriva Linux MES5 MDVSA-2013-250 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-1689, CVE-2012-2750, CVE-2013-3839

Description

The scan detected that the host is missing the following update: MDVSA-2013-250

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-2013:250/>

Mandriva Linux mes5

i586

mysql-common-5.1.72-0.1

mysql-5.1.72-0.1

mysql-client-5.1.72-0.1

mysql-bench-5.1.72-0.1

libmysql-static-devel-5.1.72-0.1

libmysql-devel-5.1.72-0.1

x86_64

mysql-common-5.1.72-0.1

mysql-5.1.72-0.1

mysql-client-5.1.72-0.1

mysql-bench-5.1.72-0.1

lib64mysql-static-devel-5.1.72-0.1

lib64mysql-devel-5.1.72-0.1

93198 - Mandriva Linux MBS1 MDVSA-2013-252 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4319

Description

The scan detected that the host is missing the following update: MDVSA-2013-252

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-2013:252/>

Mandriva Linux mbs1
x86_64
torque-4.1.5.1-1
torque-sched-4.1.5.1-1
torque-gui-4.1.5.1-1
torque-mom-4.1.5.1-1
lib64torque-devel-4.1.5.1-1
torque-client-4.1.5.1-1
torque-server-4.1.5.1-1

140322 - Red Hat Enterprise Linux RHSA-2013-1447 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise 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: RHSA-2013-1447

Observation

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

<https://rhn.redhat.com/errata/RHSA-2013-1447.html>

RHEL5D

x86_64
java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.el5_10

i386

java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.el5_10

RHEL5S

x86_64
java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.1.el5_10

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.el5_10

i386

java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.el5_10

140323 - Red Hat Enterprise Linux RHSA-2013-1440 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5775, CVE-2013-5776, CVE-2013-5777, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5787, CVE-2013-5788, CVE-2013-5789, CVE-2013-5790, CVE-2013-5797, CVE-2013-5800, CVE-2013-5801, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5810, CVE-2013-5812, CVE-2013-5814, CVE-2013-5817, CVE-2013-5818, CVE-2013-5819, CVE-2013-5820, CVE-2013-5823, CVE-2013-5824, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5831, CVE-2013-5832, CVE-2013-5838, CVE-2013-5840, CVE-2013-5842, CVE-2013-5843, CVE-2013-5844, CVE-2013-5846, CVE-2013-5848, CVE-2013-5849, CVE-2013-5850, CVE-2013-5851, CVE-2013-5852, CVE-2013-5854

Description

The scan detected that the host is missing the following update: RHSA-2013-1440

Observation

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

<https://rhn.redhat.com/errata/RHSA-2013-1440.html>

RHEL6WS

x86_64
java-1.7.0-oracle-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-jdbc-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-javafx-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-plugin-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-src-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-devel-1.7.0.45-1jpp.2.el6_4

i386

java-1.7.0-oracle-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-jdbc-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-javafx-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-plugin-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-src-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-devel-1.7.0.45-1jpp.2.el6_4

RHEL6D

x86_64
java-1.7.0-oracle-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-javafx-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-src-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-devel-1.7.0.45-1jpp.2.el6_4

RHEL5S

x86_64

java-1.7.0-oracle-plugin-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-javafx-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-devel-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-src-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-jdbc-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-1.7.0.45-1jpp.1.el5_10

i386

java-1.7.0-oracle-plugin-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-javafx-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-devel-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-src-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-jdbc-1.7.0.45-1jpp.1.el5_10
java-1.7.0-oracle-1.7.0.45-1jpp.1.el5_10

RHEL6S

x86_64

java-1.7.0-oracle-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-jdbc-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-javafx-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-plugin-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-src-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-devel-1.7.0.45-1jpp.2.el6_4

i386

java-1.7.0-oracle-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-jdbc-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-javafx-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-plugin-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-src-1.7.0.45-1jpp.2.el6_4
java-1.7.0-oracle-devel-1.7.0.45-1jpp.2.el6_4

140326 - Red Hat Enterprise Linux RHSA-2013-1451 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise 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: RHSA-2013-1451

Observation

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

<https://rhn.redhat.com/errata/RHSA-2013-1451.html>

RHEL6WS

x86_64

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.2.el6_4

i386

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.2.el6_4

java-1.7.0-openjdk-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.2.el6_4

RHEL6D
x86_64

java-1.7.0-openjdk-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.2.el6_4

i386

java-1.7.0-openjdk-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.2.el6_4

RHEL6S
x86_64

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.2.el6_4

i386

java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-1.7.0.45-2.4.3.2.el6_4
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.2.el6_4

174372 - Scientific Linux Security ERRATA Important: xorg-x11-server on SL5.x, SL6.x i386/x86_64 (1310-1412)

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

Risk Level: High

CVE: CVE-2013-4396

Description

The scan detected that the host is missing the following update: Security ERRATA Important: xorg-x11-server on SL5.x, SL6.x i386/x86_64 (1310-1412)

Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1310&L=scientific-linux-errata&T=0&P=1412>

SL5

x86_64

xorg-x11-drv-sis-0.9.1-7.3.el5_7.1
xorg-x11-drv-nv-2.1.15-4.el5
xorg-x11-drv-i810-1.6.5-9.40.el5
xorg-x11-xfs-utils-1.0.2-5.el5_6.1
xorg-x11-drv-mga-1.4.13-5.el5
xorg-x11-server-Xvfb-1.1.1-48.101.el5_10.1
xorg-x11-drivers-7.1-4.2.el5
xorg-x11-drv-i810-devel-1.6.5-9.40.el5
xorg-x11-xinit-1.0.2-15.el5
xorg-x11-drv-vesa-1.3.0-8.3.el5
xorg-x11-drv-evdev-1.0.0.5-5.el5
xorg-x11-server-Xnest-1.1.1-48.101.el5_10.1
xorg-x11-server-sdk-1.1.1-48.101.el5_10.1
xorg-x11-proto-devel-7.1-13.el5
xorg-x11-drv-qxl-0.0.12-2.el5
xorg-x11-xfs-1.0.2-5.el5_6.1

xorg-x11-drv-fbdev-0.3.0-3
xorg-x11-server-debuginfo-1.1.1-48.101.el5_10.1
xorg-x11-server-Xephyr-1.1.1-48.101.el5_10.1
xorg-x11-drv-mutouch-1.1.0-3
xorg-x11-drv-keyboard-1.1.0-3
xorg-x11-server-utils-7.1-5.el5_6.2
xorg-x11-server-Xvnc-source-1.1.1-48.101.el5_10.1
xorg-x11-server-Xorg-1.1.1-48.101.el5_10.1
xorg-x11-xdm-1.0.5-7.el5
xorg-x11-server-Xdmx-1.1.1-48.101.el5_10.1
xorg-x11-drv-ast-0.89.9-1.el5
xorg-x11-font-utils-7.1-3

i386

xorg-x11-drv-sis-0.9.1-7.3.el5_7.1
xorg-x11-drv-nv-2.1.15-4.el5
xorg-x11-drv-i810-1.6.5-9.40.el5
xorg-x11-xfs-utils-1.0.2-5.el5_6.1
xorg-x11-drv-mga-1.4.13-5.el5
xorg-x11-server-Xvfb-1.1.1-48.101.el5_10.1
xorg-x11-drivers-7.1-4.2.el5
xorg-x11-drv-i810-devel-1.6.5-9.40.el5
xorg-x11-xinit-1.0.2-15.el5
xorg-x11-drv-vesa-1.3.0-8.3.el5
xorg-x11-drv-evdev-1.0.0.5-5.el5
xorg-x11-server-Xnest-1.1.1-48.101.el5_10.1
xorg-x11-server-sdk-1.1.1-48.101.el5_10.1
xorg-x11-proto-devel-7.1-13.el5
xorg-x11-drv-qxl-0.0.12-2.el5
xorg-x11-xfs-1.0.2-5.el5_6.1
xorg-x11-drv-fbdev-0.3.0-3
xorg-x11-server-debuginfo-1.1.1-48.101.el5_10.1
xorg-x11-server-Xephyr-1.1.1-48.101.el5_10.1
xorg-x11-drv-mutouch-1.1.0-3
xorg-x11-drv-keyboard-1.1.0-3
xorg-x11-server-utils-7.1-5.el5_6.2
xorg-x11-server-Xvnc-source-1.1.1-48.101.el5_10.1
xorg-x11-server-Xorg-1.1.1-48.101.el5_10.1
xorg-x11-xdm-1.0.5-7.el5
xorg-x11-server-Xdmx-1.1.1-48.101.el5_10.1
xorg-x11-drv-ast-0.89.9-1.el5
xorg-x11-font-utils-7.1-3

SL6

noarch
xorg-x11-server-source-1.13.0-11.1.sl6.2

x86_64

xorg-x11-server-common-1.13.0-11.1.sl6.2
xorg-x11-server-Xephyr-1.13.0-11.1.sl6.2
xorg-x11-drv-mga-1.6.1-8.el6_4
xorg-x11-server-devel-1.13.0-11.1.sl6.2
xorg-x11-server-debuginfo-1.13.0-11.1.sl6.2
xorg-x11-server-Xvfb-1.13.0-11.1.sl6.2
xorg-x11-server-Xdmx-1.13.0-11.1.sl6.2
xorg-x11-server-Xorg-1.13.0-11.1.sl6.2
xorg-x11-drv-synaptics-devel-1.6.2-11.el6_4.1
xorg-x11-drv-mach64-6.9.3-4.1.el6_4
xorg-x11-drv-synaptics-1.6.2-11.el6_4.1
xorg-x11-server-Xnest-1.13.0-11.1.sl6.2

i386

xorg-x11-server-common-1.13.0-11.1.sl6.2
xorg-x11-server-Xephyr-1.13.0-11.1.sl6.2
xorg-x11-drv-mga-1.6.1-8.el6_4
xorg-x11-server-devel-1.13.0-11.1.sl6.2
xorg-x11-server-debuginfo-1.13.0-11.1.sl6.2
xorg-x11-server-Xvfb-1.13.0-11.1.sl6.2
xorg-x11-server-Xdmx-1.13.0-11.1.sl6.2
xorg-x11-server-Xorg-1.13.0-11.1.sl6.2
xorg-x11-drv-synaptics-devel-1.6.2-11.el6_4.1
xorg-x11-drv-mach64-6.9.3-4.1.el6_4
xorg-x11-drv-synaptics-1.6.2-11.el6_4.1
xorg-x11-server-Xnest-1.13.0-11.1.sl6.2

174374 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL5.x i386/x86_64 (1310-1969)

Category: SSH Module -> NonIntrusive -> Scientific 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: Security ERRATA Important: java-1.7.0-openjdk on SL5.x i386/x86_64 (1310-1969)

Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1310&L=scientific-linux-errata&T=0&P=1969>

SL5

x86_64

java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.el5_10

i386

java-1.7.0-openjdk-demo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-javadoc-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-debuginfo-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-devel-1.7.0.45-2.4.3.1.el5_10
java-1.7.0-openjdk-src-1.7.0.45-2.4.3.1.el5_10

181097 - FreeBSD wordpress Multiple Vulnerabilities (043d3a78-f245-4938-9bc7-3d0d35dd94bf)

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

Risk Level: High

CVE: CVE-2013-4338, CVE-2013-4339, CVE-2013-4340, CVE-2013-5738, CVE-2013-5739

Description

The scan detected that the host is missing the following update: wordpress -- multiple vulnerabilities (043d3a78-f245-4938-9bc7-3d0d35dd94bf)

Observation

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

<http://www.vuxml.org/freebsd/043d3a78-f245-4938-9bc7-3d0d35dd94bf.html>

Affected packages:

zh-wordpress-zh_CN < 3.6.1

zh-wordpress-zh_TW < 3.6.1

de-wordpress < 3.6.1

ja-wordpress < 3.6.1

ru-wordpress < 3.6.1

wordpress < 3.6.1

184179 - Ubuntu Linux 13.04 USN-1998-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2237, CVE-2013-2888, CVE-2013-2892, CVE-2013-2896, CVE-2013-2898, CVE-2013-2899, CVE-2013-4300

Description

The scan detected that the host is missing the following update: USN-1998-1

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-October/002286.html>

Ubuntu 13.04

linux-image-3.8.0-32-generic_3.8.0-32.47

184186 - Ubuntu Linux 12.04 USN-1995-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2237, CVE-2013-2888, CVE-2013-2892, CVE-2013-2896, CVE-2013-2898, CVE-2013-2899, CVE-2013-4300

Description

The scan detected that the host is missing the following update: USN-1995-1

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-October/002282.html>

Ubuntu 12.04

15785 - (SOL14741) F5 OpenSSH Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2010-5107

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 default configuration of OpenSSH in F5 BIG-IP products enforces a fixed time limit between establishing a TCP connection and completing a login, which could allow remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

15786 - Cisco IOS Software OSPF Opaque LSA Denial of Service

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

Risk Level: Medium

CVE: CVE-2013-5527

Description

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

Observation

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

The flaw lies in the OSPF implementation. Successful exploitation by a remote attacker could result in a denial of service condition.

15789 - (SYM13-012) Symantec Management Platform Static Key Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-5008

Description

An information disclosure vulnerability is present in some versions of Symantec Management Platform.

Observation

Symantec Management Platform is Symantec web services, security and systems management product.

An information disclosure vulnerability is present in some versions of Symantec Management Platform. The flaw lies in product agents which installs a locally accessible registry service key. An attacker accessing this key could disclose information.

15790 - Cisco NX-OS Configuration File Password Hashes Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2012-4090

Description

A information disclosure vulnerability is present in some versions of Cisco NX-OS.

Observation

Cisco NX-OS is networking software.

A information disclosure vulnerability is present in some versions of Cisco NX-OS. The flaw is due to improper sanitization of configuration files. Successful exploitation by an authenticated local attacker could allow him to gain access to sensitive information.

15791 - Cisco NX-OS Software Routing Information Protocol Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2012-4091

Description

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

Observation

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

The flaw lies in the RIP service engine. Successful exploitation by a remote attacker could result in a denial of service condition.

15796 - (HT5964) Apple Mac OS X Directory Services Authentication Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-5163

Description

A security bypass vulnerability present in some versions of Apple Mac OS X.

Observation

Apple Mac OS X is a popular operating system.

A security bypass vulnerability present in some versions of Apple Mac OS X. The flaw is due to the lack of verifications when processing user's authentications within the Directory Services component. Successful exploitation could allow an attacker to execute arbitrary code.

15799 - IBM DB2 Fast Communications Manager Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-4032

Description

A denial of service vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A buffer overflow vulnerability is present in some versions of IBM DB2. The flaw lies in the Fast Communications Manager (FCM). Successful exploitation could allow an attacker to cause a denial of service condition.

15800 - Oracle WebLogic Server Web Container Java Server Faces Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-3827

Description

An information disclosure vulnerability is present in some versions of Oracle Fusion Middleware WebLogic Server.

Observation

An information disclosure vulnerability is present in some versions of Oracle Fusion Middleware WebLogic Server.

The flaw lies in the Java Server Faces and Web Container sub-components. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

15801 - Oracle Database Critical Patch Update October 2013

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

Risk Level: Medium

CVE: CVE-2011-3389, CVE-2013-0169, CVE-2013-3826, CVE-2013-5771

Description

Multiple vulnerabilities are present in some versions of Oracle Database.

Observation

Oracle Database is one of the most popular database management system.

Multiple vulnerabilities are present in some versions of Oracle Database. The flaws lie in Core RDBMS and Oracle Security Service components. Successful exploitation could allow an attacker to obtain sensitive information.

15802 - McAfee SiteAdvisor Unquoted Path Privilege Escalation

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

Risk Level: Medium

Description

A privilege escalation vulnerability is present in some versions of McAfee SiteAdvisor.

Observation

McAfee SiteAdvisor software that provides simple Web site safety ratings.

A privilege escalation vulnerability is present in some versions of McAfee SiteAdvisor. The flaw lies in a shared component which does not properly handles unquoted paths. Successful exploitation could allow an attacker to escalate privileges.

15805 - Oracle MySQL Multiple Vulnerabilities Prior To 5.6.13

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

Risk Level: Medium

CVE: CVE-2013-3839, CVE-2013-5767, CVE-2013-5786, CVE-2013-5793, CVE-2013-5807

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL.

Observation

Oracle MySQL is a widely used relational database management system.

Multiple vulnerabilities are present in some versions of Oracle MySQL. The flaws are due to errors in multiple components. A successful exploitation could result in a Denial of Service (DoS) or the disclosure of sensitive information.

15806 - Oracle MySQL Multiple Vulnerabilities Prior To 5.5.33

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

Risk Level: Medium

CVE: CVE-2013-3839, CVE-2013-5807

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL.

Observation

Oracle MySQL is a widely used relational database management system.

Multiple vulnerabilities are present in some versions of Oracle MySQL. The flaws are due to errors in multiple components. A successful exploitation could result in a Denial of Service (DoS) or the disclosure of sensitive information.

15809 - Oracle GlassFish Server Critical Patch Update October 2013

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

Risk Level: Medium

CVE: CVE-2013-2172, CVE-2013-3827, CVE-2013-5816

Description

Multiple vulnerabilities are present in some versions of Oracle GlassFish Server.

Observation

Oracle GlassFish Server supports lightweight Java EE 6 Web Profile and the Java EE 6 platform.

Multiple vulnerabilities are present in some versions of Oracle GlassFish Server. The flaws lie in the Java Server Faces and the Metro components. It could allow remote attackers to disclose potentially sensitive information, manipulate certain data, and cause a Denial of Service.

15816 - Oracle MySQL Locking Denial of Service

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

Risk Level: Medium

CVE: CVE-2013-5770

Description

A denial of service vulnerability is present in some versions of Oracle MySQL.

Observation

A denial of service vulnerability is present in some versions of Oracle MySQL.

The flaw lies in the Locking sub-component. Successful exploitation by a remote attacker could result in a denial of service condition.

58707 - Debian Linux 6.0 DSA-2783-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2011-5036, CVE-2013-0184, CVE-2013-0263

Description

The scan detected that the host is missing the following update: DSA-2783-1

Observation

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

<http://lists.debian.org/debian-security-announce/2013/msg00194.html>

Debian 6.0

all

librack-ruby1.9.1_1.1.0-4+squeeze1

librack-ruby_1.1.0-4+squeeze1

librack-ruby1.8_1.1.0-4+squeeze1

58708 - Debian Linux 6.0, 7.0 DSA-2784-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4396

Description

The scan detected that the host is missing the following update: DSA-2784-1

Observation

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

<http://lists.debian.org/debian-security-announce/2013/msg00195.html>

Debian 7.0

i386

xserver-xephyr_1.12.4-6+deb7u1
xdmx_1.12.4-6+deb7u1
xserver-xorg-core-dbg_1.12.4-6+deb7u1
xdmx-tools_1.12.4-6+deb7u1
xserver-xorg-dev_1.12.4-6+deb7u1
xvfb_1.12.4-6+deb7u1
xnest_1.12.4-6+deb7u1
xserver-xfbdev_1.12.4-6+deb7u1
xserver-xorg-core_1.12.4-6+deb7u1

Debian 6.0

i386

xserver-xorg-core-dbg_1.7.7-17
xvfb_1.7.7-17
xserver-xfbdev_1.7.7-17
xserver-xorg-dev_1.7.7-17
xdmx-tools_1.7.7-17
xserver-xorg-core_1.7.7-17
xdmx_1.7.7-17
xserver-xephyr_1.7.7-17
xnest_1.7.7-17

58710 - Debian Linux 6.0, 7.0 DSA-2782-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4623, CVE-2013-5914, CVE-2013-5915

Description

The scan detected that the host is missing the following update: DSA-2782-1

Observation

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

For more information see:

<http://lists.debian.org/debian-security-announce/2013/msg00193.html>

Debian 7.0

i386

libpolarssl-dev_1.2.9-1~deb7u1
libpolarssl0_1.2.9-1~deb7u1
libpolarssl-runtime_1.2.9-1~deb7u1

Debian 6.0

i386

libpolarssl0_1.2.9-1~deb6u1
libpolarssl-runtime_1.2.9-1~deb6u1
libpolarssl-dev_1.2.9-1~deb6u1

85625 - CentOS 6 CESA-2013-1436 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4162, CVE-2013-4299

Description

The scan detected that the host is missing the following update: CESA-2013-1436

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2013-October/019976.html>

CentOS 6

noarch

kernel-doc-2.6.32-358.23.2.el6

kernel-firmware-2.6.32-358.23.2.el6

i686

python-perf-2.6.32-358.23.2.el6

kernel-debug-2.6.32-358.23.2.el6

kernel-devel-2.6.32-358.23.2.el6

kernel-2.6.32-358.23.2.el6

kernel-headers-2.6.32-358.23.2.el6

kernel-debug-devel-2.6.32-358.23.2.el6

perf-2.6.32-358.23.2.el6

x86_64

python-perf-2.6.32-358.23.2.el6

kernel-debug-2.6.32-358.23.2.el6

kernel-devel-2.6.32-358.23.2.el6

kernel-2.6.32-358.23.2.el6

kernel-headers-2.6.32-358.23.2.el6

kernel-debug-devel-2.6.32-358.23.2.el6

perf-2.6.32-358.23.2.el6

85628 - CentOS 6 CESA-2013-1441 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2125, CVE-2012-2126, CVE-2013-4287

Description

The scan detected that the host is missing the following update: CESA-2013-1441

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2013-October/019977.html>

CentOS 6

noarch

rubygems-1.3.7-4.el6_4

88556 - Slackware Linux 13.1, 13.37, 14.0 SSA:2013-291-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4325

Description

The scan detected that the host is missing the following update: SSA:2013-291-01

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.422319>

Slackware 13.1
x86_64
hplip-3.10.2-x86_64-4

Slackware 14.0
x86_64
hplip-3.12.9-x86_64-3

Slackware 13.37
x86_64
hplip-3.11.3a-x86_64-3

91365 - Oracle Enterprise Linux ELSA-2013-1436 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4162, CVE-2013-4299

Description

The scan detected that the host is missing the following update: ELSA-2013-1436

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-October/003733.html>

OEL6
x86_64
kernel-doc-2.6.32-358.23.2.el6
kernel-debug-2.6.32-358.23.2.el6
kernel-devel-2.6.32-358.23.2.el6
kernel-2.6.32-358.23.2.el6
kernel-firmware-2.6.32-358.23.2.el6
kernel-headers-2.6.32-358.23.2.el6
kernel-debug-devel-2.6.32-358.23.2.el6

i386
kernel-doc-2.6.32-358.23.2.el6
kernel-debug-2.6.32-358.23.2.el6
kernel-devel-2.6.32-358.23.2.el6
kernel-2.6.32-358.23.2.el6
kernel-firmware-2.6.32-358.23.2.el6
kernel-headers-2.6.32-358.23.2.el6
kernel-debug-devel-2.6.32-358.23.2.el6

91366 - Oracle Enterprise Linux ELSA-2013-1441 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2125, CVE-2012-2126, CVE-2013-4287, CVE-2013-4363

Description

The scan detected that the host is missing the following update: ELSA-2013-1441

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-October/003734.html>

OEL6
x86_64
rubygems-1.3.7-4.el6_4

i386
rubygems-1.3.7-4.el6_4

91369 - Oracle Enterprise Linux ELSA-2013-1452 Update Is Not Installed

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

Risk Level: Medium

Description

The scan detected that the host is missing the following update: ELSA-2013-1452

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-October/003752.html>
<http://oss.oracle.com/pipermail/el-errata/2013-October/003753.html>

OEL6
x86_64
vino-2.28.1-9.el6_4

i386
vino-2.28.1-9.el6_4

OEL5
x86_64
vino-2.13.5-10.el5_10

i386
vino-2.13.5-10.el5_10

91370 - Oracle Enterprise Linux ELSA-2013-2576 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4299

Description

The scan detected that the host is missing the following update: ELSA-2013-2576

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-October/003738.html>

<http://oss.oracle.com/pipermail/el-errata/2013-October/003737.html>

OEL6

x86_64

kernel-uek-firmware-2.6.39-400.209.2.el6uek

kernel-uek-2.6.39-400.209.2.el6uek

kernel-uek-devel-2.6.39-400.209.2.el6uek

kernel-uek-debug-devel-2.6.39-400.209.2.el6uek

kernel-uek-doc-2.6.39-400.209.2.el6uek

kernel-uek-debug-2.6.39-400.209.2.el6uek

i386

kernel-uek-firmware-2.6.39-400.209.2.el6uek

kernel-uek-debug-devel-2.6.39-400.209.2.el6uek

kernel-uek-2.6.39-400.209.2.el6uek

kernel-uek-devel-2.6.39-400.209.2.el6uek

kernel-uek-debug-2.6.39-400.209.2.el6uek

kernel-uek-doc-2.6.39-400.209.2.el6uek

OEL5

x86_64

kernel-uek-devel-2.6.39-400.209.2.el5uek

kernel-uek-2.6.39-400.209.2.el5uek

kernel-uek-debug-devel-2.6.39-400.209.2.el5uek

kernel-uek-firmware-2.6.39-400.209.2.el5uek

kernel-uek-debug-2.6.39-400.209.2.el5uek

kernel-uek-doc-2.6.39-400.209.2.el5uek

i386

kernel-uek-debug-devel-2.6.39-400.209.2.el5uek

kernel-uek-2.6.39-400.209.2.el5uek

kernel-uek-debug-2.6.39-400.209.2.el5uek

kernel-uek-devel-2.6.39-400.209.2.el5uek

kernel-uek-firmware-2.6.39-400.209.2.el5uek

kernel-uek-doc-2.6.39-400.209.2.el5uek

91371 - Oracle Enterprise Linux ELSA-2013-2575 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4162, CVE-2013-4299

Description

The scan detected that the host is missing the following update: ELSA-2013-2575

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-October/003735.html>

<http://oss.oracle.com/pipermail/el-errata/2013-October/003736.html>

OEL6

x86_64

kernel-uek-devel-2.6.32-400.33.2.el6uek
kernel-uek-headers-2.6.32-400.33.2.el6uek
mlnx_en-2.6.32-400.33.2.el6uek-1.5.7-0.1
kernel-uek-doc-2.6.32-400.33.2.el6uek
kernel-uek-debug-2.6.32-400.33.2.el6uek
kernel-uek-firmware-2.6.32-400.33.2.el6uek
mlnx_en-2.6.32-400.33.2.el6uekdebug-1.5.7-0.1
ofa-2.6.32-400.33.2.el6uek-1.5.1-4.0.58
ofa-2.6.32-400.33.2.el6uekdebug-1.5.1-4.0.58
kernel-uek-2.6.32-400.33.2.el6uek
kernel-uek-debug-devel-2.6.32-400.33.2.el6uek

i386

kernel-uek-devel-2.6.32-400.33.2.el6uek
kernel-uek-headers-2.6.32-400.33.2.el6uek
mlnx_en-2.6.32-400.33.2.el6uek-1.5.7-0.1
kernel-uek-doc-2.6.32-400.33.2.el6uek
kernel-uek-debug-2.6.32-400.33.2.el6uek
kernel-uek-firmware-2.6.32-400.33.2.el6uek
mlnx_en-2.6.32-400.33.2.el6uekdebug-1.5.7-0.1
ofa-2.6.32-400.33.2.el6uek-1.5.1-4.0.58
ofa-2.6.32-400.33.2.el6uekdebug-1.5.1-4.0.58
kernel-uek-2.6.32-400.33.2.el6uek
kernel-uek-debug-devel-2.6.32-400.33.2.el6uek

OEL5

x86_64

kernel-uek-2.6.32-400.33.2.el5uek
kernel-uek-debug-2.6.32-400.33.2.el5uek
kernel-uek-headers-2.6.32-400.33.2.el5uek
kernel-uek-doc-2.6.32-400.33.2.el5uek
ofa-2.6.32-400.33.2.el5uekdebug-1.5.1-4.0.58
kernel-uek-devel-2.6.32-400.33.2.el5uek
kernel-uek-firmware-2.6.32-400.33.2.el5uek
mlnx_en-2.6.32-400.33.2.el5uek-1.5.7-2
kernel-uek-debug-devel-2.6.32-400.33.2.el5uek
mlnx_en-2.6.32-400.33.2.el5uekdebug-1.5.7-2
ofa-2.6.32-400.33.2.el5uek-1.5.1-4.0.58

i386

kernel-uek-2.6.32-400.33.2.el5uek
kernel-uek-debug-2.6.32-400.33.2.el5uek
kernel-uek-headers-2.6.32-400.33.2.el5uek
kernel-uek-doc-2.6.32-400.33.2.el5uek
ofa-2.6.32-400.33.2.el5uekdebug-1.5.1-4.0.58
kernel-uek-devel-2.6.32-400.33.2.el5uek
kernel-uek-firmware-2.6.32-400.33.2.el5uek
mlnx_en-2.6.32-400.33.2.el5uek-1.5.7-2
kernel-uek-debug-devel-2.6.32-400.33.2.el5uek
mlnx_en-2.6.32-400.33.2.el5uekdebug-1.5.7-2
ofa-2.6.32-400.33.2.el5uek-1.5.1-4.0.58

93195 - Mandriva Linux MBS1, MES5 MDVSA-2013-253 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4397

Description

The scan detected that the host is missing the following update: MDVSA-2013-253

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-2013:253/>

<https://www.mandriva.com/en/support/security/advisories/mes5/MDVSA-2013:253/>

Mandriva Linux mbs1

x86_64

libtar-devel-1.2.11-11.1

Mandriva Linux mes5

i586

libtar-devel-1.2.11-8.1

x86_64

libtar-devel-1.2.11-8.1

95811 - SuSE Linux 12.2, 12.3 openSUSE-SU-2013:1556-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2906, CVE-2013-2907, CVE-2013-2908, CVE-2013-2909, CVE-2013-2910, CVE-2013-2911, CVE-2013-2912, CVE-2013-2913, CVE-2013-2914, CVE-2013-2915, CVE-2013-2916, CVE-2013-2917, CVE-2013-2918, CVE-2013-2919, CVE-2013-2920, CVE-2013-2921, CVE-2013-2922, CVE-2013-2923, CVE-2013-2924

Description

The scan detected that the host is missing the following update: openSUSE-SU-2013:1556-1

Observation

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

<http://lists.opensuse.org/opensuse-security-announce/2013-10/msg00002.html>

SuSE Linux 12.2

i586

chromium-ffmpegsumo-30.0.1599.66-1.46.1

chromium-debugsource-30.0.1599.66-1.46.1

chromedriver-30.0.1599.66-1.46.1

chromium-debuginfo-30.0.1599.66-1.46.1

chromium-suid-helper-30.0.1599.66-1.46.1

chromium-ffmpegsumo-debuginfo-30.0.1599.66-1.46.1

chromium-desktop-gnome-30.0.1599.66-1.46.1

chromium-30.0.1599.66-1.46.1

chromium-desktop-kde-30.0.1599.66-1.46.1

chromedriver-debuginfo-30.0.1599.66-1.46.1

chromium-suid-helper-debuginfo-30.0.1599.66-1.46.1

SuSE Linux 12.3

i586

chromedriver-debuginfo-30.0.1599.66-1.11.2

chromium-desktop-kde-30.0.1599.66-1.11.2

chromium-ffmpegsumo-debuginfo-30.0.1599.66-1.11.2

chromium-debuginfo-30.0.1599.66-1.11.2

chromium-ffmpegsumo-30.0.1599.66-1.11.2

chromedriver-30.0.1599.66-1.11.2

chromium-debugsource-30.0.1599.66-1.11.2

chromium-desktop-gnome-30.0.1599.66-1.11.2

chromium-suid-helper-debuginfo-30.0.1599.66-1.11.2

chromium-30.0.1599.66-1.11.2

chromium-suid-helper-30.0.1599.66-1.11.2

95812 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 kdelibs4-8402 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-4512, CVE-2012-4513, CVE-2012-4515

Description

The scan detected that the host is missing the following update: kdelibs4-8402

Observation

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

For more information see:

<http://download.novell.com/Download?buildid=jPQrtLKenxM~>
<http://download.novell.com/Download?buildid=hkHdYy8fPQM~>
<http://download.novell.com/Download?buildid=KhUPxUuHBAw~>
<http://download.novell.com/Download?buildid=SY9P4xJN3JM~>
<http://download.novell.com/Download?buildid=D5YkyDyr3cl~>
<http://download.novell.com/Download?buildid=B29MhSz0R1s~>
<http://download.novell.com/Download?buildid=7y6QdPiSSPQ~>
<http://download.novell.com/Download?buildid=33pbBepNAoQ~>
<http://download.novell.com/Download?buildid=6pQsYqf2gus~>

SuSE SLES 11 SP3

i586

libkde4-4.3.5-0.12.1

kdelibs4-doc-4.3.5-0.12.1

kdelibs4-4.3.5-0.12.1

kdelibs4-core-4.3.5-0.12.1

libkdecore4-4.3.5-0.12.1

x86_64

libkde4-4.3.5-0.12.1

kdelibs4-doc-4.3.5-0.12.1

libkde4-32bit-4.3.5-0.12.1

kdelibs4-4.3.5-0.12.1

libkdecore4-32bit-4.3.5-0.12.1

kdelibs4-core-4.3.5-0.12.1

libkdecore4-4.3.5-0.12.1

SuSE SLED 11

i586

libkde4-4.3.5-0.12.1
kdelibs4-doc-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

x86_64
libkde4-4.3.5-0.12.1
kdelibs4-doc-4.3.5-0.12.1
libkde4-32bit-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
libkdecore4-32bit-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

SuSE SLED 11 SP3
i586
libkde4-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

x86_64
libkde4-4.3.5-0.12.1
libkde4-32bit-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
libkdecore4-32bit-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

SuSE SLES 11
i586
libkde4-4.3.5-0.12.1
kdelibs4-doc-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

x86_64
libkde4-4.3.5-0.12.1
kdelibs4-doc-4.3.5-0.12.1
libkde4-32bit-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
libkdecore4-32bit-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

95813 - SuSE SLES 11, 11 SP2, SLED 11, 11 SP2 kdelibs4-8401 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-4512, CVE-2012-4513, CVE-2012-4515

Description

The scan detected that the host is missing the following update: kdelibs4-8401

Observation

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

For more information see:

<http://download.novell.com/Download?buildid=6qdFIBYife4~>
http://download.novell.com/Download?buildid=dAa_SuAnsMQ~
<http://download.novell.com/Download?buildid=Zk1MsnmDxnA~>
<http://download.novell.com/Download?buildid=HK9fZBOc0bE~>
<http://download.novell.com/Download?buildid=uAyeZfZEURE~>
http://download.novell.com/Download?buildid=E7_rekZeqkg~
<http://download.novell.com/Download?buildid=81NbtIINKtM~>
<http://download.novell.com/Download?buildid=2dYTmiXZegw~>
<http://download.novell.com/Download?buildid=mPu8xYTzU7c~>

SuSE SLED 11 SP2

i586

libkde4-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

x86_64

libkde4-4.3.5-0.12.1
libkde4-32bit-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
libkdecore4-32bit-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

SuSE SLED 11

i586

libkde4-4.3.5-0.12.1
kdelibs4-doc-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

x86_64

libkde4-4.3.5-0.12.1
kdelibs4-doc-4.3.5-0.12.1
libkde4-32bit-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
libkdecore4-32bit-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

SuSE SLES 11 SP2

i586

libkde4-4.3.5-0.12.1
kdelibs4-doc-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

x86_64

libkde4-4.3.5-0.12.1
kdelibs4-doc-4.3.5-0.12.1
libkde4-32bit-4.3.5-0.12.1
kdelibs4-4.3.5-0.12.1
libkdecore4-32bit-4.3.5-0.12.1
kdelibs4-core-4.3.5-0.12.1
libkdecore4-4.3.5-0.12.1

SuSE SLES 11

i586

libkde4-4.3.5-0.12.1

kdelibs4-doc-4.3.5-0.12.1

kdelibs4-4.3.5-0.12.1

kdelibs4-core-4.3.5-0.12.1

libkdecore4-4.3.5-0.12.1

x86_64

libkde4-4.3.5-0.12.1

kdelibs4-doc-4.3.5-0.12.1

libkde4-32bit-4.3.5-0.12.1

kdelibs4-4.3.5-0.12.1

libkdecore4-32bit-4.3.5-0.12.1

kdelibs4-core-4.3.5-0.12.1

libkdecore4-4.3.5-0.12.1

140321 - Red Hat Enterprise Linux RHSA-2013-1449 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0343, CVE-2013-4299, CVE-2013-4345, CVE-2013-4368

Description

The scan detected that the host is missing the following update: RHSA-2013-1449

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2013-1449.html>

RHEL5D

noarch

kernel-doc-2.6.18-371.1.2.el5

x86_64

kernel-devel-2.6.18-371.1.2.el5

kernel-debug-devel-2.6.18-371.1.2.el5

kernel-headers-2.6.18-371.1.2.el5

kernel-debuginfo-common-2.6.18-371.1.2.el5

kernel-xen-debuginfo-2.6.18-371.1.2.el5

kernel-xen-devel-2.6.18-371.1.2.el5

kernel-xen-2.6.18-371.1.2.el5

kernel-debuginfo-2.6.18-371.1.2.el5

kernel-debug-2.6.18-371.1.2.el5

kernel-2.6.18-371.1.2.el5

kernel-debug-debuginfo-2.6.18-371.1.2.el5

i386

kernel-devel-2.6.18-371.1.2.el5

kernel-debug-devel-2.6.18-371.1.2.el5

kernel-headers-2.6.18-371.1.2.el5

kernel-debuginfo-common-2.6.18-371.1.2.el5

kernel-xen-debuginfo-2.6.18-371.1.2.el5

kernel-xen-devel-2.6.18-371.1.2.el5

kernel-PAE-debuginfo-2.6.18-371.1.2.el5

kernel-debuginfo-2.6.18-371.1.2.el5
kernel-xen-2.6.18-371.1.2.el5
kernel-debug-2.6.18-371.1.2.el5
kernel-2.6.18-371.1.2.el5
kernel-debug-debuginfo-2.6.18-371.1.2.el5
kernel-PAE-2.6.18-371.1.2.el5
kernel-PAE-devel-2.6.18-371.1.2.el5

RHEL5S

noarch
kernel-doc-2.6.18-371.1.2.el5

x86_64

kernel-devel-2.6.18-371.1.2.el5
kernel-debug-devel-2.6.18-371.1.2.el5
kernel-headers-2.6.18-371.1.2.el5
kernel-debuginfo-common-2.6.18-371.1.2.el5
kernel-xen-debuginfo-2.6.18-371.1.2.el5
kernel-xen-devel-2.6.18-371.1.2.el5
kernel-xen-2.6.18-371.1.2.el5
kernel-debuginfo-2.6.18-371.1.2.el5
kernel-debug-2.6.18-371.1.2.el5
kernel-2.6.18-371.1.2.el5
kernel-debug-debuginfo-2.6.18-371.1.2.el5

i386

kernel-devel-2.6.18-371.1.2.el5
kernel-debug-devel-2.6.18-371.1.2.el5
kernel-headers-2.6.18-371.1.2.el5
kernel-debuginfo-common-2.6.18-371.1.2.el5
kernel-xen-debuginfo-2.6.18-371.1.2.el5
kernel-xen-devel-2.6.18-371.1.2.el5
kernel-PAE-debuginfo-2.6.18-371.1.2.el5
kernel-debuginfo-2.6.18-371.1.2.el5
kernel-xen-2.6.18-371.1.2.el5
kernel-debug-2.6.18-371.1.2.el5
kernel-2.6.18-371.1.2.el5
kernel-debug-debuginfo-2.6.18-371.1.2.el5
kernel-PAE-2.6.18-371.1.2.el5
kernel-PAE-devel-2.6.18-371.1.2.el5

140324 - Red Hat Enterprise Linux RHSA-2013-1436 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4162, CVE-2013-4299

Description

The scan detected that the host is missing the following update: RHSA-2013-1436

Observation

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

<https://rhn.redhat.com/errata/RHSA-2013-1436.html>

RHEL6WS

noarch

kernel-doc-2.6.32-358.23.2.el6
kernel-firmware-2.6.32-358.23.2.el6

x86_64

kernel-debuginfo-2.6.32-358.23.2.el6
kernel-2.6.32-358.23.2.el6
python-perf-debuginfo-2.6.32-358.23.2.el6
perf-debuginfo-2.6.32-358.23.2.el6
kernel-headers-2.6.32-358.23.2.el6
kernel-debug-debuginfo-2.6.32-358.23.2.el6
perf-2.6.32-358.23.2.el6
kernel-debug-2.6.32-358.23.2.el6
kernel-devel-2.6.32-358.23.2.el6
kernel-debuginfo-common-x86_64-2.6.32-358.23.2.el6
kernel-debug-devel-2.6.32-358.23.2.el6

i386

kernel-debuginfo-2.6.32-358.23.2.el6
kernel-2.6.32-358.23.2.el6
python-perf-debuginfo-2.6.32-358.23.2.el6
perf-debuginfo-2.6.32-358.23.2.el6
kernel-debug-debuginfo-2.6.32-358.23.2.el6
kernel-debuginfo-common-i686-2.6.32-358.23.2.el6
kernel-debug-2.6.32-358.23.2.el6
perf-2.6.32-358.23.2.el6
kernel-devel-2.6.32-358.23.2.el6
kernel-headers-2.6.32-358.23.2.el6
kernel-debug-devel-2.6.32-358.23.2.el6

RHEL6D

noarch
kernel-doc-2.6.32-358.23.2.el6
kernel-firmware-2.6.32-358.23.2.el6

x86_64

kernel-debuginfo-2.6.32-358.23.2.el6
kernel-2.6.32-358.23.2.el6
python-perf-debuginfo-2.6.32-358.23.2.el6
perf-debuginfo-2.6.32-358.23.2.el6
kernel-headers-2.6.32-358.23.2.el6
kernel-debug-debuginfo-2.6.32-358.23.2.el6
perf-2.6.32-358.23.2.el6
kernel-debug-2.6.32-358.23.2.el6
kernel-devel-2.6.32-358.23.2.el6
kernel-debuginfo-common-x86_64-2.6.32-358.23.2.el6
kernel-debug-devel-2.6.32-358.23.2.el6

i386

kernel-debuginfo-2.6.32-358.23.2.el6
kernel-2.6.32-358.23.2.el6
python-perf-debuginfo-2.6.32-358.23.2.el6
perf-debuginfo-2.6.32-358.23.2.el6
kernel-debug-debuginfo-2.6.32-358.23.2.el6
kernel-debuginfo-common-i686-2.6.32-358.23.2.el6
kernel-debug-2.6.32-358.23.2.el6
perf-2.6.32-358.23.2.el6
kernel-devel-2.6.32-358.23.2.el6
kernel-headers-2.6.32-358.23.2.el6
kernel-debug-devel-2.6.32-358.23.2.el6

RHEL6S

noarch

kernel-doc-2.6.32-358.23.2.el6

kernel-firmware-2.6.32-358.23.2.el6

x86_64

kernel-debuginfo-2.6.32-358.23.2.el6

kernel-2.6.32-358.23.2.el6

python-perf-debuginfo-2.6.32-358.23.2.el6

perf-debuginfo-2.6.32-358.23.2.el6

kernel-headers-2.6.32-358.23.2.el6

kernel-debug-debuginfo-2.6.32-358.23.2.el6

perf-2.6.32-358.23.2.el6

kernel-debug-2.6.32-358.23.2.el6

kernel-devel-2.6.32-358.23.2.el6

kernel-debuginfo-common-x86_64-2.6.32-358.23.2.el6

kernel-debug-devel-2.6.32-358.23.2.el6

i386

kernel-debuginfo-2.6.32-358.23.2.el6

kernel-2.6.32-358.23.2.el6

python-perf-debuginfo-2.6.32-358.23.2.el6

perf-debuginfo-2.6.32-358.23.2.el6

kernel-debug-debuginfo-2.6.32-358.23.2.el6

kernel-debuginfo-common-i686-2.6.32-358.23.2.el6

kernel-debug-2.6.32-358.23.2.el6

perf-2.6.32-358.23.2.el6

kernel-devel-2.6.32-358.23.2.el6

kernel-headers-2.6.32-358.23.2.el6

kernel-debug-devel-2.6.32-358.23.2.el6

140325 - Red Hat Enterprise Linux RHSA-2013-1452 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5745

Description

The scan detected that the host is missing the following update: RHSA-2013-1452

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2013-1452.html>

RHEL5D

x86_64

vino-2.13.5-10.el5_10

vino-debuginfo-2.13.5-10.el5_10

i386

vino-2.13.5-10.el5_10

vino-debuginfo-2.13.5-10.el5_10

RHEL6D

x86_64

vino-2.28.1-9.el6_4

vino-debuginfo-2.28.1-9.el6_4

i386

vino-2.28.1-9.el6_4

vino-debuginfo-2.28.1-9.el6_4

RHEL6WS

x86_64

vino-2.28.1-9.el6_4

vino-debuginfo-2.28.1-9.el6_4

i386

vino-2.28.1-9.el6_4

vino-debuginfo-2.28.1-9.el6_4

RHEL5S

x86_64

vino-2.13.5-10.el5_10

vino-debuginfo-2.13.5-10.el5_10

i386

vino-2.13.5-10.el5_10

vino-debuginfo-2.13.5-10.el5_10

RHEL6S

x86_64

vino-2.28.1-9.el6_4

vino-debuginfo-2.28.1-9.el6_4

i386

vino-2.28.1-9.el6_4

vino-debuginfo-2.28.1-9.el6_4

140327 - Red Hat Enterprise Linux RHSA-2013-1441 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2125, CVE-2012-2126, CVE-2013-4287

Description

The scan detected that the host is missing the following update: RHSA-2013-1441

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2013-1441.html>

RHEL6D

noarch

rubygems-1.3.7-4.el6_4

RHEL6S

noarch

rubygems-1.3.7-4.el6_4

174371 - Scientific Linux Security ERRATA Moderate: kernel on SL6.x i386/srpm/x86_64 (1310-1714)

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

Risk Level: Medium

CVE: CVE-2013-4162, CVE-2013-4299

Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: kernel on SL6.x i386/srpm/x86_64 (1310-1714)

Observation

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

For more information see:

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1310&L=scientific-linux-errata&T=0&P=1714>

SL6

noarch

kernel-debuginfo-2.6.32-358.23.2.el6
kernel-debug-debuginfo-2.6.32-358.23.2.el6
kernel-debuginfo-common-i686-2.6.32-358.23.2.el6
python-perf-debuginfo-2.6.32-358.23.2.el6
kernel-doc-2.6.32-358.23.2.el6
kernel-firmware-2.6.32-358.23.2.el6
kernel-debuginfo-common-x86_64-2.6.32-358.23.2.el6
perf-debuginfo-2.6.32-358.23.2.el6

x86_64

kernel-2.6.32-358.23.2.el6
python-perf-2.6.32-358.23.2.el6
python-perf-debuginfo-2.6.32-358.23.2.el6
perf-debuginfo-2.6.32-358.23.2.el6
kernel-debuginfo-common-x86_64-2.6.32-358.23.2.el6
kernel-debug-debuginfo-2.6.32-358.23.2.el6
perf-2.6.32-358.23.2.el6
kernel-debug-2.6.32-358.23.2.el6
kernel-debuginfo-2.6.32-358.23.2.el6
kernel-doc-2.6.32-358.23.2.el6
kernel-firmware-2.6.32-358.23.2.el6
kernel-devel-2.6.32-358.23.2.el6
kernel-headers-2.6.32-358.23.2.el6
kernel-debug-devel-2.6.32-358.23.2.el6

i386

kernel-2.6.32-358.23.2.el6
python-perf-2.6.32-358.23.2.el6
python-perf-debuginfo-2.6.32-358.23.2.el6
perf-debuginfo-2.6.32-358.23.2.el6
kernel-debug-debuginfo-2.6.32-358.23.2.el6
perf-2.6.32-358.23.2.el6
kernel-debug-2.6.32-358.23.2.el6
kernel-debuginfo-common-i686-2.6.32-358.23.2.el6
kernel-debuginfo-2.6.32-358.23.2.el6
kernel-doc-2.6.32-358.23.2.el6
kernel-firmware-2.6.32-358.23.2.el6
kernel-devel-2.6.32-358.23.2.el6
kernel-headers-2.6.32-358.23.2.el6
kernel-debug-devel-2.6.32-358.23.2.el6

174373 - Scientific Linux Security ERRATA Moderate: rubygems on SL6.x (noarch) (1310-1844)

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

Risk Level: Medium

CVE: CVE-2012-2125, CVE-2012-2126, CVE-2013-4287

Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: rubygems on SL6.x (noarch) (1310-1844)

Observation

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

For more information see:

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1310&L=scientific-linux-errata&T=0&P=1844>

SL6

noarch

rubygems-1.3.7-4.el6_4

174375 - Scientific Linux Security ERRATA Moderate: Red Hat Enterprise Linux 5 kernel update on SL5.x i386/x86_64 (1310-1555)

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

Risk Level: Medium

CVE: CVE-2012-4398

Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: Red Hat Enterprise Linux 5 kernel update on SL5.x i386/x86_64 (1310-1555)

Observation

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

For more information see:

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1310&L=scientific-linux-errata&T=0&P=1555>

SL5

noarch

kernel-doc-2.6.18-371.el5

x86_64

kernel-debug-devel-2.6.18-371.el5

kernel-debug-2.6.18-371.el5

kernel-debuginfo-common-2.6.18-371.el5

kernel-2.6.18-371.el5

kernel-xen-devel-2.6.18-371.el5

kernel-xen-debuginfo-2.6.18-371.el5

kernel-debuginfo-2.6.18-371.el5

kernel-devel-2.6.18-371.el5

kernel-headers-2.6.18-371.el5

kernel-xen-2.6.18-371.el5

kernel-debug-debuginfo-2.6.18-371.el5

i386

kernel-PAE-2.6.18-371.el5

kernel-xen-2.6.18-371.el5
kernel-debuginfo-common-2.6.18-371.el5
kernel-debug-2.6.18-371.el5
kernel-2.6.18-371.el5
kernel-xen-devel-2.6.18-371.el5
kernel-headers-2.6.18-371.el5
kernel-debuginfo-2.6.18-371.el5
kernel-PAE-debuginfo-2.6.18-371.el5
kernel-devel-2.6.18-371.el5
kernel-PAE-devel-2.6.18-371.el5
kernel-debug-devel-2.6.18-371.el5
kernel-xen-debuginfo-2.6.18-371.el5
kernel-debug-debuginfo-2.6.18-371.el5

177758 - Gentoo Linux GLSA-201310-11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2011-4115

Description

The scan detected that the host is missing the following update: GLSA-201310-11

Observation

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

<http://security.gentoo.org/glsa/glsa-201310-11.xml>

Affected packages:

dev-perl/Parallel-ForkManager < 1.20.0

177759 - Gentoo Linux GLSA-201310-10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2011-1923, CVE-2012-2130, CVE-2013-0169, CVE-2013-1621, CVE-2013-4623, CVE-2013-5915

Description

The scan detected that the host is missing the following update: GLSA-201310-10

Observation

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

<http://security.gentoo.org/glsa/glsa-201310-10.xml>

Affected packages:

net-libs/polarssl < 1.3.0

184180 - Ubuntu Linux 12.04, 12.10, 13.04 USN-1990-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1056, CVE-2013-4396

Description

The scan detected that the host is missing the following update: USN-1990-1

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-October/002278.html>

Ubuntu 12.10

xserver-xorg-core_1.13.0-0ubuntu6.4

Ubuntu 12.04

xserver-xorg-core-lts-raring_1.13.3-0ubuntu6~precise3

xserver-xorg-core_1.11.4-0ubuntu10.14

xserver-xorg-core-lts-quantal_1.13.0-0ubuntu6.1~precise4

Ubuntu 13.04

xserver-xorg-core_1.13.3-0ubuntu6.2

184182 - Ubuntu Linux 10.04, 12.04, 12.10, 13.04 USN-1991-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-4412, CVE-2012-4424, CVE-2013-0242, CVE-2013-1914, CVE-2013-4237, CVE-2013-4332

Description

The scan detected that the host is missing the following update: USN-1991-1

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-October/002279.html>

Ubuntu 10.04

libc6_2.11.1-0ubuntu7.13

Ubuntu 12.10

libc6_2.15-0ubuntu20.2

Ubuntu 12.04

libc6_2.15-0ubuntu10.5

Ubuntu 13.04

libc6_2.17-0ubuntu5.1

187230 - Fedora Linux 18 FEDORA-2013-18686 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4365

Description

The scan detected that the host is missing the following update: FEDORA-2013-18686

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119351.html>

Fedora Core 18

mod_fcgid-2.3.9-1.fc18

187231 - Fedora Linux 18 FEDORA-2013-17112 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4325

Description

The scan detected that the host is missing the following update: FEDORA-2013-17112

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119358.html>

Fedora Core 18

hplip-3.13.9-2.fc18

187232 - Fedora Linux 19 FEDORA-2013-18808 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4397

Description

The scan detected that the host is missing the following update: FEDORA-2013-18808

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119418.html>

Fedora Core 19

libtar-1.2.11-26.fc19

187235 - Fedora Linux 18 FEDORA-2013-18785 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4397

Description

The scan detected that the host is missing the following update: FEDORA-2013-18785

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119379.html>

Fedora Core 18

libtar-1.2.11-25.fc18

187236 - Fedora Linux 18 FEDORA-2013-18822 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4387

Description

The scan detected that the host is missing the following update: FEDORA-2013-18822

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119236.html>

Fedora Core 18

kernel-3.11.4-101.fc18

187237 - Fedora Linux 19 FEDORA-2013-18638 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4365

Description

The scan detected that the host is missing the following update: FEDORA-2013-18638

Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119288.html>

Fedora Core 19

mod_fcgid-2.3.9-1.fc19

58709 - Debian Linux 6.0, 7.0 DSA-2781-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-1445

Description

The scan detected that the host is missing the following update: DSA-2781-1

Observation

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

<http://lists.debian.org/debian-security-announce/2013/msg00192.html>

Debian 7.0

i386

python3-crypto_2.6-4+deb7u3

python3-crypto-dbg_2.6-4+deb7u3

python-crypto-dbg_2.6-4+deb7u3

python-crypto_2.6-4+deb7u3

Debian 6.0

i386

python-crypto_2.1.0-2+squeeze2

python-crypto-dbg_2.1.0-2+squeeze2

93196 - Mandriva Linux MBS1 MDVSA-2013-255 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2190

Description

The scan detected that the host is missing the following update: MDVSA-2013-255

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-2013:255/>

Mandriva Linux mbs1

x86_64

lib64clutter-gir1.0-1.10.8-1

lib64clutter1.0-devel-1.10.8-1

lib64clutter1.0_0-1.10.8-1

93199 - Mandriva Linux MBS1 MDVSA-2013-254 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2236

Description

The scan detected that the host is missing the following update: MDVSA-2013-254

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-2013:254/>

Mandriva Linux mbs1
x86_64
lib64quagga-devel-0.99.20.1-4.2
quagga-0.99.20.1-4.2
quagga-contrib-0.99.20.1-4.2

181094 - FreeBSD bugzilla Multiple Vulnerabilities (e135f0c9-375f-11e3-80b7-20cf30e32f6d)

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

Risk Level: Low

CVE: CVE-2013-1733, CVE-2013-1734, CVE-2013-1742, CVE-2013-1743

Description

The scan detected that the host is missing the following update: bugzilla -- multiple vulnerabilities (e135f0c9-375f-11e3-80b7-20cf30e32f6d)

Observation

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

<http://www.vuxml.org/freebsd/e135f0c9-375f-11e3-80b7-20cf30e32f6d.html>

Affected packages:

4.0.0 <= bugzilla < 4.0.11
4.0.0 <= bugzilla40 < 4.0.11
4.0.0 <= bugzilla42 < 4.0.11
4.0.0 <= bugzilla44 < 4.0.11
4.2.0 <= bugzilla < 4.2.7
4.2.0 <= bugzilla40 < 4.2.7
4.2.0 <= bugzilla42 < 4.2.7
4.2.0 <= bugzilla44 < 4.2.7
4.4 <= bugzilla < 4.4.1
4.4 <= bugzilla40 < 4.4.1
4.4 <= bugzilla42 < 4.4.1
4.4 <= bugzilla44 < 4.4.1

181095 - FreeBSD pycrypto PRNG Reseed Race Condition (c0f122e2-3897-11e3-a084-3c970e169bc2)

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

Risk Level: Low

CVE: CVE-2013-1445

Description

The scan detected that the host is missing the following update: pycrypto -- PRNG reseed race condition (c0f122e2-3897-11e3-a084-3c970e169bc2)

Observation

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

<http://www.vuxml.org/freebsd/c0f122e2-3897-11e3-a084-3c970e169bc2.html>

Affected packages:

py26-pycrypto < 2.6.1

py27-pycrypto < 2.6.1

py31-pycrypto < 2.6.1

py32-pycrypto < 2.6.1

py33-pycrypto < 2.6.1

181096 - FreeBSD node.js DoS Vulnerability (206f9826-a06d-4927-9a85-771c37010b32)

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

Risk Level: Low

Description

The scan detected that the host is missing the following update: node.js -- DoS Vulnerability (206f9826-a06d-4927-9a85-771c37010b32)

Observation

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

<http://www.vuxml.org/freebsd/206f9826-a06d-4927-9a85-771c37010b32.html>

Affected packages:

node < 0.10.21

node-devel < 0.11.7

181098 - FreeBSD dropbear Exposure Of Sensitive Information, DoS (8c9b48d1-3715-11e3-a624-00262d8b701d)

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

Risk Level: Low

CVE: CVE-2013-4421, CVE-2013-4434

Description

The scan detected that the host is missing the following update: dropbear -- exposure of sensitive information, DoS (8c9b48d1-3715-11e3-a624-00262d8b701d)

Observation

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

<http://www.vuxml.org/freebsd/8c9b48d1-3715-11e3-a624-00262d8b701d.html>

Affected packages:

2012.55 <= dropbear < 2013.59

184178 - Ubuntu Linux 12.04 USN-1993-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2237

Description

The scan detected that the host is missing the following update: USN-1993-1

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-October/002281.html>

Ubuntu 12.04

linux-image-3.2.0-1439-omap4_3.2.0-1439.58

184181 - Ubuntu Linux 12.10 USN-1996-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2147

Description

The scan detected that the host is missing the following update: USN-1996-1

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-October/002284.html>

Ubuntu 12.10

linux-image-3.5.0-42-generic_3.5.0-42.65

linux-image-3.5.0-42-omap_3.5.0-42.65

linux-image-3.5.0-42-highbank_3.5.0-42.65

linux-image-3.5.0-42-powerpc-smp_3.5.0-42.65

linux-image-3.5.0-42-powerpc64-smp_3.5.0-42.65

184183 - Ubuntu Linux 12.10 USN-1997-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2147

Description

The scan detected that the host is missing the following update: USN-1997-1

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-October/002285.html>

Ubuntu 12.10

linux-image-3.5.0-234-omap4_3.5.0-234.50

184184 - Ubuntu Linux 12.04 USN-1994-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2147

Description

The scan detected that the host is missing the following update: USN-1994-1

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-October/002283.html>

Ubuntu 12.04

linux-image-3.5.0-42-generic_3.5.0-42.65~precise1

184185 - Ubuntu Linux 13.04 USN-1999-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2147

Description

The scan detected that the host is missing the following update: USN-1999-1

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-October/002287.html>

Ubuntu 13.04

linux-image-3.5.0-234-omap4_3.5.0-234.50

184187 - Ubuntu Linux 12.04 USN-1992-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2237

Description

The scan detected that the host is missing the following update: USN-1992-1

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-October/002280.html>

Ubuntu 12.04

linux-image-3.2.0-55-omap_3.2.0-55.85
linux-image-3.2.0-55-powerpc-smp_3.2.0-55.85
linux-image-3.2.0-55-powerpc64-smp_3.2.0-55.85
linux-image-3.2.0-55-highbank_3.2.0-55.85
linux-image-3.2.0-55-generic_3.2.0-55.85
linux-image-3.2.0-55-generic-pae_3.2.0-55.85
linux-image-3.2.0-55-virtual_3.2.0-55.85

187228 - Fedora Linux 18 FEDORA-2013-17904 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-2013-17904

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119256.html>

Fedora Core 18

fedmsg-0.7.1-2.fc18

187229 - Fedora Linux 18 FEDORA-2013-18401 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-2013-18401

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119400.html>

Fedora Core 18

fping-3.5-3.fc18

187233 - Fedora Linux 19 FEDORA-2013-17925 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-2013-17925

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119241.html>

Fedora Core 19

fedmsg-0.7.1-2.fc19

187234 - Fedora Linux 18 FEDORA-2013-18606 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4421

Description

The scan detected that the host is missing the following update: FEDORA-2013-18606

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119300.html>

Fedora Core 18

dropbear-2013.59-1.fc18

187238 - Fedora Linux 19 FEDORA-2013-19338 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-2013-19338

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119331.html>

Fedora Core 19

java-1.7.0-openjdk-1.7.0.60-2.4.3.0.fc19

187239 - Fedora Linux 19 FEDORA-2013-18593 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4421

Description

The scan detected that the host is missing the following update: FEDORA-2013-18593

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119323.html>

Fedora Core 19

dropbear-2013.59-1.fc19

187240 - Fedora Linux 18 FEDORA-2013-19285 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-2013-19285

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-October/119271.html>

Fedora Core 18

java-1.7.0-openjdk-1.7.0.60-2.4.3.0.fc18

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.

11641 - CA Message Queuing Server Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2007-0060

Update Details

Recommendation is updated.

15783 - Cisco ASA Software Multiple Vulnerabilities (cisco-sa-20131009-asa)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-3415, CVE-2013-5507, CVE-2013-5508, CVE-2013-5509, CVE-2013-5510, CVE-2013-5511, CVE-2013-5512, CVE-2013-5513, CVE-2013-5515, CVE-2013-5542

Update Details

CVE is updated.

91363 - Oracle Enterprise Linux ELSA-2013-1426 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4396

Update Details

FASLScript is updated.

10796 - NTP Mode 7 Request Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2009-3563

Update Details

Recommendation is updated.

14440 - Apache Tomcat Security Bypass and Denial of Service Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2012-2733, CVE-2012-3439

DISA IAVA: 2012-B-0110

Update Details

Observation is updated.

70086 - oracle.fasl3.inc

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

Risk Level: Informational

Update Details

FASLScript is updated.

DELETED CHECKS

15748 - IBM DB2 Fast Communications Manager Denial of Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2013-4032

ADDITIONAL NOTES

15748 - was recategorized and replaced by FID 15799

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.

MCAFEETECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com/>

Multi-National Phone Support available here:

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

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

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

Copyright 2012 McAfee, Inc.

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