2014-DEC-04
FSL version 7.5.651

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

17130 - (APSB14-21) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0547, CVE-2014-0548, CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, CVE-2014-0552, CVE-2014-0553, CVE-2014-0554, CVE-2014-0555, CVE-2014-0556, CVE-2014-0557, CVE-2014-0559

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code or bypass security controls.

The update provided by Adobe bulletin APSB14-21 resolves these issues. The target system is missing this update.

17135 - (APSB13-11) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-1378, CVE-2013-1379, CVE-2013-1380, CVE-2013-2555

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple buffer overflow and logic error. Successful exploitation by a remote attacker could result in execution of arbitrary code.

The update provided by Adobe bulletin APSB13-11 resolves the issues. The target system is missing this update.

17140 - (APSB13-26) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

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

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in multiple core components. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service condition.

The update provided by Adobe bulletin APSB13-26 resolves the issues. The target system is missing this update.

17141 - (APSB13-28) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-5331, CVE-2013-5332

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in multiple core components. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service condition.

The update provided by Adobe bulletin APSB13-28 resolves the issues. The target system is missing this update.

17142 - (APSB14-02) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0491, CVE-2014-0492

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in multiple core components. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-02 resolves the issues. The target system is missing this update.

17144 - (APSB14-07) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0498, CVE-2014-0499, CVE-2014-0502

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaw lies in an unspecified component. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-07 resolves these issues. The target system is missing this update.

17150 - (APSB14-16) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0531, CVE-2014-0532, CVE-2014-0533, CVE-2014-0534, CVE-2014-0535, CVE-2014-0536

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code or bypass security controls.

The update provided by Adobe bulletin APSB14-16 resolves these issues. The target system is missing this update.

17152 - (APSB14-18) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0538, CVE-2014-0540, CVE-2014-0541, CVE-2014-0542, CVE-2014-0543, CVE-2014-0544, CVE-2014-0545, CVE-2014-5333

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code or bypass security controls.

The update provided by Adobe bulletin APSB14-18 resolves these issues. The target system is missing this update.

17456 - WordPress WP DBManager Plugin Remote Command Injection Vulnerability

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

Risk Level: High

CVE: CVE-2014-8334

Description

A command injection vulnerability is present in some versions of WP-DBManager Plugin for WordPress.

Observation

WordPress is a popular blog web application.

A command injection vulnerability is present in some versions of WP-DBManager Plugin for WordPress. The flaw lies in multiple parameters which are not being properly sanitized by the plugin. Successful exploitation could allow an attacker to execute remote code.

16949 - (SOL15404) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2009-3245

Description

An OpenSSL 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.

An OpenSSL vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the embedded version of OpenSSL. Successful exploitation could allow an attacker to cause an unknown impact.

16957 - (APSB13-01) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-0630

Description

A remote code execution vulnerability is present in some versions of Adobe Flash Player and Adobe AIR.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

A remote code execution vulnerability is present in some versions of Adobe Flash Player and Adobe AIR. The flaw is due to an unspecified vulnerability. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service condition.

The update provided by Adobe bulletin APSB13-01 resolves the issue. The target system is missing this update.

17131 - (APSB13-04) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-0633, CVE-2013-0634

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws are due to unspecified vulnerabilities. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service condition.

The update provided by Adobe bulletin APSB13-04 resolves the issue. The target system is missing this update.

17132 - (APSB13-05) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-0637, CVE-2013-0638, CVE-2013-0639 , CVE-2013-0642, CVE-2013-0644, CVE-2013-0645, CVE-2013-0647, CVE-2013-0649, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, CVE-2013-1373, CVE-2013-1374

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws are due to multiple buffer overflow and memory corruption vulnerabilities. Successful exploitation by a remote attacker could result in execution of arbitrary code.

The update provided by Adobe bulletin APSB13-05 resolves the issue. The target system is missing this update.

17133 - (APSB13-08) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-0504, CVE-2013-0643, CVE-2013-0648

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple buffer overflow and logic error. Successful exploitation by a remote attacker could result in execution of arbitrary code.

The update provided by Adobe bulletin APSB13-08 resolves the issue. The target system is missing this update.

17134 - (APSB13-09) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-0646, CVE-2013-0650, CVE-2013-1371, CVE-2013-1375

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws are due to a heap buffer overflow, memory corruption, among other vulnerabilities. Successful exploitation by a remote attacker could result in execution of arbitrary code.

The update provided by Adobe bulletin APSB13-09 resolves the issue. The target system is missing this update.

17136 - (APSB13-14) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, CVE-2013-3335

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple buffer overflow and logic error. Successful exploitation by a remote attacker could result in execution of arbitrary code.

The update provided by Adobe bulletin APSB13-14 resolves the issues. The target system is missing this update.

17137 - (APSB13-16) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-3343

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple buffer overflows in OpenTTD. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service condition.

The update provided by Adobe bulletin APSB13-16 resolves the issues. The target system is missing this update.

17138 - (APSB13-17) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-3344, CVE-2013-3345, CVE-2013-3347

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service condition.

The update provided by Adobe bulletin APSB13-17 resolves the issues. The target system is missing this update.

17139 - (APSB13-21) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-5324, CVE-2013-3361, CVE-2013-3362, CVE-2013-3363

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in multiple core components. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service condition.

The update provided by Adobe bulletin APSB13-21 resolves the issues. The target system is missing this update.

17143 - (APSB14-04) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0497

Description

A vulnerability is present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

A vulnerability is present in some versions of Adobe Flash Player. The flaw lies in an unspecified component. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-04 resolves this issue. The target system is missing this update.

17145 - (APSB14-08) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-0504, CVE-2014-0503

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to access the clipboard information and bypass the same origin policy.

The update provided by Adobe bulletin APSB14-08 resolves these issues. The target system is missing this update.

17146 - (APSB14-09) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0506, CVE-2014-0507, CVE-2014-0508, CVE-2014-0509

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-09 resolves these issues. The target system is missing this update.

17147 - (APSB14-13) Adobe Flash Player Buffer Overflow Remote Code Execution

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0515

Description

A vulnerability in some versions of Adobe Flash Player could lead to remote code execution.

Observation

A vulnerability in some versions of Adobe Flash Player could lead to remote code execution.

The flaw is due to how a malicious flash video file is handled. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17148 - (APSB14-14) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0510, CVE-2014-0516, CVE-2014-0517, CVE-2014-0518, CVE-2014-0519, CVE-2014-0520

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-14 resolves these issues. The target system is missing this update.

17299 - (HT203112) Apple OS X Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2011-2391, CVE-2013-5150, CVE-2013-6438, CVE-2014-0098, CVE-2014-3537, CVE-2014-3566, CVE-2014-4351, CVE-2014-4364, CVE-2014-4371, CVE-2014-4373, CVE-2014-4375, CVE-2014-4380, CVE-2014-4388, CVE-2014-4391, CVE-2014-4404,

CVE-2014-4405, CVE-2014-4407, CVE-2014-4408, CVE-2014-4417, CVE-2014-4418, CVE-2014-4419, CVE-2014-4420, CVE-2014-4421, CVE-2014-4422, CVE-2014-4425, CVE-2014-4426, CVE-2014-4427, CVE-2014-4428, CVE-2014-4430, CVE-2014-4431, CVE-2014-4432, CVE-2014-4433, CVE-2014-4434, CVE-2014-4435, CVE-2014-4436, CVE-2014-4437, CVE-2014-4438, CVE-2014-4439, CVE-2014-4440, CVE-2014-4441, CVE-2014-4442, CVE-2014-4443, CVE-2014-4444, CVE-2014-6271, CVE-2014-7169

Description

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

Observation

Apple Mac OS X is a popular operating system.

Multiple vulnerabilities are present in some versions of Apple Mac OS X. The flaws are present in multiple bundled components. Successful exploitation could allow an attacker to execute arbitrary code with root privileges, disclose information, bypass security measure and cause a denial of service condition.

17451 - WordPress EWWW Image Optimizer Plugin Error Parameter Cross Site Scripting Vulnerability

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

Risk Level: High

CVE: CVE-2014-6243

Description

A Cross-site scripting vulnerability is present in some versions of EWWW Image Optimizer Plugin for WordPress.

Observation

WordPress is a popular blog web application.

A Cross-site scripting vulnerability is present in some versions of EWWW Image Optimizer Plugin for WordPress. The flaws lie in ewww-image-optimizer.php. Successful exploitation could allow an attacker to execute arbitrary web code.

17462 - Google Chrome Multiple Vulnerabilities Prior To 39.0.2171.65

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

Risk Level: High

CVE: CVE-2014-0574, CVE-2014-7899, CVE-2014-7900, CVE-2014-7901, CVE-2014-7902, CVE-2014-7903, CVE-2014-7904, CVE-2014-7905, CVE-2014-7906, CVE-2014-7907, CVE-2014-7908, CVE-2014-7909, CVE-2014-7910

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in the multiple components. Successful exploitation could allow an attacker to disclose potentially sensitive information, conduct spoofing attacks, bypass certain security restrictions and compromise a user's system.

17463 - Google Chrome Multiple Vulnerabilities Prior To 39.0.2171.65

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0574, CVE-2014-7899, CVE-2014-7900, CVE-2014-7901, CVE-2014-7902, CVE-2014-7903, CVE-2014-7904, CVE-

2014-7905, CVE-2014-7906, CVE-2014-7907, CVE-2014-7908, CVE-2014-7909, CVE-2014-7910

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in the multiple components. Successful exploitation could allow an attacker to disclose potentially sensitive information, conduct spoofing attacks, bypass certain security restrictions and compromise a user's system.

140624 - Red Hat Enterprise Linux RHSA-2014-1919 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

Description

The scan detected that the host is missing the following update:
RHSA-2014-1919

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1919.html

RHEL5D
x86_64
firefox-31.3.0-4.el5_11
firefox-debuginfo-31.3.0-4.el5_11

i386
firefox-31.3.0-4.el5_11
firefox-debuginfo-31.3.0-4.el5_11

RHEL5S
x86_64
firefox-31.3.0-4.el5_11
firefox-debuginfo-31.3.0-4.el5_11

i386
firefox-31.3.0-4.el5_11
firefox-debuginfo-31.3.0-4.el5_11

RHEL7S
x86_64
firefox-31.3.0-3.el7_0
firefox-debuginfo-31.3.0-3.el7_0

RHEL6S
x86_64
firefox-debuginfo-31.3.0-3.el6_6
firefox-31.3.0-3.el6_6

i386

firefox-debuginfo-31.3.0-3.el6_6
firefox-31.3.0-3.el6_6

RHEL7D
x86_64
firefox-31.3.0-3.el7_0
firefox-debuginfo-31.3.0-3.el7_0

RHEL6D
x86_64
firefox-debuginfo-31.3.0-3.el6_6
firefox-31.3.0-3.el6_6

i386
firefox-debuginfo-31.3.0-3.el6_6
firefox-31.3.0-3.el6_6

RHEL6WS
x86_64
firefox-debuginfo-31.3.0-3.el6_6
firefox-31.3.0-3.el6_6

i386
firefox-debuginfo-31.3.0-3.el6_6
firefox-31.3.0-3.el6_6

RHEL7WS
x86_64
firefox-31.3.0-3.el7_0
firefox-debuginfo-31.3.0-3.el7_0

170427 - Amazon Linux AMI ALAS-2014-454 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6407, CVE-2014-6408

Description

The scan detected that the host is missing the following update:
ALAS-2014-454

Observation

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

https://alas.aws.amazon.com/ALAS-2014-454.html

Amazon Linux AMI
x86_64
docker-pkg-devel-1.3.2-1.0.amzn1
docker-devel-1.3.2-1.0.amzn1
docker-1.3.2-1.0.amzn1

188553 - Fedora Linux 19 FEDORA-2014-15405 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15405

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145099.html

Fedora Core 19

wget-1.16-3.fc19

17447 - (HT6591) Apple OS X Yosemite Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2014-4453, CVE-2014-4458, CVE-2014-4459, CVE-2014-4460

Description

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

Observation

Apple OS X is an operating system used in Apple's computer.

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

17476 - WordPress Multiple Vulnerabilities III

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

Risk Level: High

CVE: CVE-2014-9031, CVE-2014-9032, CVE-2014-9033, CVE-2014-9034, CVE-2014-9035, CVE-2014-9036, CVE-2014-9037, CVE-2014-9038, CVE-2014-9039

Description

Multiple vulnerabilities are present in some versions of WordPress.

Observation

WordPress is a popular blogging tool.

Multiple vulnerabilities are present in some versions of WordPress. The flaws lie in multiple components of WordPress. Successful exploitation could allow an attacker to inject arbitrary web script or HTML, cause a denial of service or disclose information.

17151 - (APSB14-17) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0537, CVE-2014-0539, CVE-2014-4671

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code or bypass security controls.

The update provided by Adobe bulletin APSB14-17 resolves these issues. The target system is missing this update.

17458 - (SOL15723) F5 BIG-IP OpenSSL Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-3567

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in OpenSSL component. Successful exploitation could allow an attacker to cause denial of service.

17473 - (SOL15867) F5 BIG-IP Multiple Perl Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2012-5195, CVE-2012-5526, CVE-2012-6329, CVE-2013-1667

Description

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

Observation

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

Multiple vulnerabilities are present in some versions of F5 BIG-IP systems. The flaw lies in the Perl binary. Successful exploitation could allow an attacker to obtain sensitive information, manipulate certain data, execute remote execute code or cause a denial of service condition.

43150 - HP-UX 11.X PHCO_43875 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7879

Description

The scan detected that the host is missing the following update:
PHCO_43875

Observation

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

https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHCO_43875

">patch description

HP-UX 11.31 (NA)

OS-Core.CORE2-SHLIBS,fr=B.11.31,fa=HP-UX_B.11.31_PA,v=HP
OS-Core.CORE2-SHLIBS,fr=B.11.31,fa=HP-UX_B.11.31_IA,v=HP
OS-Core.CORE2-64SLIB,fr=B.11.31,fa=HP-UX_B.11.31_IA,v=HP
OS-Core.CORE2-64SLIB,fr=B.11.31,fa=HP-UX_B.11.31_PA,v=HP
OS-Core.CORE-64SLIB,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP
OS-Core.CORE-SHLIBS,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP
OS-Core.CORE-ENG-A-MAN,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP
OS-Core.ADMN-ENG-A-MAN,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP

43151 - HP-UX 11.X PHCO_43873 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7879

Description

The scan detected that the host is missing the following update:
PHCO_43873

Observation

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

https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHCO_43873

">patch description

HP-UX 11.11 (800)
HP-UX 11.11 (700)

OS-Core.CORE-ENG-A-MAN,fr=B.11.11,fa=HP-UX_B.11.11_32/64,v=HP
OS-Core.ADMN-ENG-A-MAN,fr=B.11.11,fa=HP-UX_B.11.11_32/64,v=HP
OS-Core.CORE-SHLIBS,fr=B.11.11,fa=HP-UX_B.11.11_32/64,v=HP

43153 - HP-UX 11.X PHCO_43874 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7879

Description

The scan detected that the host is missing the following update:
PHCO_43874

Observation

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

https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHCO_43874

">patch description

HP-UX 11.23 (800)
HP-UX 11.23 (700)

OS-Core.CORE2-SHLIBS,fr=B.11.23,fa=HP-UX_B.11.23_IA,v=HP
OS-Core.CORE-ENG-A-MAN,fr=B.11.23,fa=HP-UX_B.11.23_IA/PA,v=HP
OS-Core.CORE2-64SLIB,fr=B.11.23,fa=HP-UX_B.11.23_PA,v=HP
OS-Core.ADMN-ENG-A-MAN,fr=B.11.23,fa=HP-UX_B.11.23_IA/PA,v=HP
OS-Core.CORE2-64SLIB,fr=B.11.23,fa=HP-UX_B.11.23_IA,v=HP
OS-Core.CORE2-SHLIBS,fr=B.11.23,fa=HP-UX_B.11.23_PA,v=HP

93427 - Mandriva Linux MBS1 MDVSA-2014-229 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6051, CVE-2014-6052, CVE-2014-6053, CVE-2014-6054, CVE-2014-6055

Description

The scan detected that the host is missing the following update:
MDVSA-2014-229

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-2014%3A229/

Mandriva Linux mbs1
x86_64
lib64vncserver-devel-0.9.9-1
lib64minilzo0-2.08-1.1
lib64lzo2_2-2.08-1.1
lib64lzo-devel-2.08-1.1
lib64vncserver0-0.9.9-1
linuxvnc-0.9.9-1

93430 - Mandriva Linux MBS1 MDVSA-2014-230 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3601, CVE-2014-3610, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-3647, CVE-2014-3673, CVE-2014-3687, CVE-2014-3690, CVE-2014-7825, CVE-2014-7826, CVE-2014-7970, CVE-2014-8369

Description

The scan detected that the host is missing the following update:
MDVSA-2014-230

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-2014%3A230/

Mandriva Linux mbs1
x86_64
kernel-firmware-3.4.104-2.1
kernel-server-3.4.104-2.1
cpupower-3.4.104-2.1
kernel-headers-3.4.104-2.1
lib64cpupower0-3.4.104-2.1
kernel-source-3.4.104-2
perf-3.4.104-2.1
kernel-server-devel-3.4.104-2.1
lib64cpupower-devel-3.4.104-2.1

130000 - Debian Linux 7.0 DSA-3082-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

Description

The scan detected that the host is missing the following update:
DSA-3082-1

Observation

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

http://www.debian.org/security/2014/dsa-3082

Debian 7.0
all
flac_1.2.1-6+deb7u1

130002 - Debian Linux 7.0 DSA-3081-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6051, CVE-2014-6052, CVE-2014-6053, CVE-2014-6054, CVE-2014-6055

Description

The scan detected that the host is missing the following update:
DSA-3081-1

Observation

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

http://www.debian.org/security/2014/dsa-3081

Debian 7.0
all
libvncserver0_0.9.9+dfsg-1+deb7u1
libvncserver0-dbg_0.9.9+dfsg-1+deb7u1
libvncserver-dev_0.9.9+dfsg-1+deb7u1
libvncserver-config_0.9.9+dfsg-1+deb7u1
linuxvnc_0.9.9+dfsg-1+deb7u1

130006 - Debian Linux 7.0 DSA-3079-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3158

Description

The scan detected that the host is missing the following update:
DSA-3079-1

Observation

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

http://www.debian.org/security/2014/dsa-3079

Debian 7.0
all
ppp_2.4.5-5.1+deb7u1

140626 - Red Hat Enterprise Linux RHSA-2014-1915 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8439

Description

The scan detected that the host is missing the following update:
RHSA-2014-1915

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1915.html

RHEL5D
x86_64
flash-plugin-11.2.202.424-1.el5

i386
flash-plugin-11.2.202.424-1.el5

RHEL5S
x86_64
flash-plugin-11.2.202.424-1.el5

i386
flash-plugin-11.2.202.424-1.el5

RHEL6D
x86_64
flash-plugin-11.2.202.424-1.el6

RHEL6S

x86_64
flash-plugin-11.2.202.424-1.el6

i386
flash-plugin-11.2.202.424-1.el6

RHEL6WS
x86_64
flash-plugin-11.2.202.424-1.el6

i386
flash-plugin-11.2.202.424-1.el6

140630 - Red Hat Enterprise Linux RHSA-2014-1924 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

Description

The scan detected that the host is missing the following update:
RHSA-2014-1924

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1924.html

RHEL5D
x86_64
thunderbird-31.3.0-1.el5_11
thunderbird-debuginfo-31.3.0-1.el5_11

i386
thunderbird-31.3.0-1.el5_11
thunderbird-debuginfo-31.3.0-1.el5_11

RHEL6D
x86_64
thunderbird-debuginfo-31.3.0-1.el6_6
thunderbird-31.3.0-1.el6_6

i386
thunderbird-debuginfo-31.3.0-1.el6_6
thunderbird-31.3.0-1.el6_6

RHEL6S
x86_64
thunderbird-debuginfo-31.3.0-1.el6_6
thunderbird-31.3.0-1.el6_6

i386
thunderbird-debuginfo-31.3.0-1.el6_6
thunderbird-31.3.0-1.el6_6

RHEL6WS
x86_64

thunderbird-debuginfo-31.3.0-1.el6_6
thunderbird-31.3.0-1.el6_6

i386
thunderbird-debuginfo-31.3.0-1.el6_6
thunderbird-31.3.0-1.el6_6

184627 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2426-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

Description

The scan detected that the host is missing the following update:
USN-2426-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-November/002743.html

Ubuntu 14.10

libflac8_1.3.0-2ubuntu0.14.10.1

Ubuntu 14.04

libflac8_1.3.0-2ubuntu0.14.04.1

Ubuntu 12.04

libflac8_1.2.1-6ubuntu0.1

Ubuntu 10.04

libflac8_1.2.1-2ubuntu0.1

184631 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2429-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3158

Description

The scan detected that the host is missing the following update:
USN-2429-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002745.html

Ubuntu 14.10

ppp_2.4.5-5.1ubuntu3.1

Ubuntu 14.04

ppp_2.4.5-5.1ubuntu2.1

Ubuntu 12.04

ppp_2.4.5-5ubuntu1.1

Ubuntu 10.04

ppp_2.4.5~git20081126t100229-0ubuntu3.1

188552 - Fedora Linux 19 FEDORA-2014-15503 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0150, CVE-2014-8594, CVE-2014-8595, CVE-2014-9030

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15503

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145039.html

Fedora Core 19

xen-4.2.5-5.fc19

188562 - Fedora Linux 20 FEDORA-2014-15521 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0150, CVE-2014-8594, CVE-2014-8595, CVE-2014-9030

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15521

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145040.html

Fedora Core 20

xen-4.3.3-5.fc20

17339 - Linksys SMART WiFi Firmware Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-2014-8243, CVE-2014-8244

Description

Multiple vulnerabilities are present in some versions of Linksys EA series routers.

Observation

Linksys EA series routers are smart WiFi router.

Multiple vulnerabilities are present in some versions of Linksys EA series router. The flaws lie in web interface. Successful exploitation could allow an attacker to obtain or modify sensitive information.

17443 - Novell Storage Manager OpenSSL Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

Description

Multiple vulnerabilities are present in some versions of Novell Storage Manager.

Observation

Novell Storage Manager is automated storage management.

Multiple vulnerabilities are present in some versions of Novell Storage Manager. The flaws lie in OpenSSL. Successful exploitation could allow attackers to disclose potentially sensitive information, cause a denial of service and compromise a vulnerable system.

17471 - (SOL15548) F5 BIG-IP Rsync sender.c Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2007-4091

Description

A remote code execution vulnerability is present in some versions of F5's BIG-IP.

Observation

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

A remote code execution vulnerability is present in some versions of F5's BIG-IP. The flaw lies in rsync. Successful exploitation could allow an attacker to execute remote code.

130001 - Debian Linux 7.0 DSA-3077-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558

Description

The scan detected that the host is missing the following update:
DSA-3077-1

Observation

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

http://www.debian.org/security/2014/dsa-3077

Debian 7.0
all
openjdk-6-dbg_6b33-1.13.5-2~deb7u1
openjdk-6-doc_6b33-1.13.5-2~deb7u1
openjdk-6-jre-headless_6b33-1.13.5-2~deb7u1
openjdk-6-jdk_6b33-1.13.5-2~deb7u1
openjdk-6-jre_6b33-1.13.5-2~deb7u1
icedtea-6-jre-cacao_6b33-1.13.5-2~deb7u1
openjdk-6-demo_6b33-1.13.5-2~deb7u1
openjdk-6-source_6b33-1.13.5-2~deb7u1
openjdk-6-jre-zero_6b33-1.13.5-2~deb7u1
icedtea-6-jre-jamvm_6b33-1.13.5-2~deb7u1
openjdk-6-jre-lib_6b33-1.13.5-2~deb7u1

130005 - Debian Linux 7.0 DSA-3080-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558

Description

The scan detected that the host is missing the following update:
DSA-3080-1

Observation

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

http://www.debian.org/security/2014/dsa-3080

Debian 7.0
all
openjdk-7-dbg_7u71-2.5.3-2~deb7u1
openjdk-7-jdk_7u71-2.5.3-2~deb7u1
icedtea-7-jre-cacao_7u71-2.5.3-2~deb7u1
icedtea-7-jre-jamvm_7u71-2.5.3-2~deb7u1
openjdk-7-source_7u71-2.5.3-2~deb7u1
openjdk-7-jre-headless_7u71-2.5.3-2~deb7u1
openjdk-7-jre_7u71-2.5.3-2~deb7u1
openjdk-7-demo_7u71-2.5.3-2~deb7u1
openjdk-7-jre-zero_7u71-2.5.3-2~deb7u1
openjdk-7-doc_7u71-2.5.3-2~deb7u1
openjdk-7-jre-lib_7u71-2.5.3-2~deb7u1

170429 - Amazon Linux AMI ALAS-2014-452 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1981, CVE-2013-1982, CVE-2013-1983, CVE-2013-1984, CVE-2013-1985, CVE-2013-1986, CVE-2013-1987, CVE-2013-1988, CVE-2013-1989, CVE-2013-1990, CVE-2013-1991, CVE-2013-1995, CVE-2013-1997, CVE-2013-1998, CVE-2013-1999, CVE-2013-2000, CVE-2013-2001, CVE-2013-2002, CVE-2013-2003, CVE-2013-2004, CVE-2013-2005, CVE-2013-2062, CVE-2013-2064, CVE-2013-2066

Description

The scan detected that the host is missing the following update:
ALAS-2014-452

Observation

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

https://alas.aws.amazon.com/ALAS-2014-452.html

Amazon Linux AMI
x86_64
libXfixes-devel-5.0.1-2.1.8.amzn1
libX11-debuginfo-1.6.0-2.2.12.amzn1
libXxf86dga-devel-1.1.4-2.1.8.amzn1
libXvMC-debuginfo-1.0.8-2.1.8.amzn1
libX11-1.6.0-2.2.12.amzn1
libXi-devel-1.7.2-2.2.9.amzn1
libXxf86dga-1.1.4-2.1.8.amzn1
libXrandr-devel-1.4.1-2.1.8.amzn1
libXrender-debuginfo-0.9.8-2.1.9.amzn1
libXvMC-1.0.8-2.1.8.amzn1
libdmx-debuginfo-1.1.3-3.7.amzn1
libXfixes-debuginfo-5.0.1-2.1.8.amzn1
libXi-debuginfo-1.7.2-2.2.9.amzn1
libX11-devel-1.6.0-2.2.12.amzn1
libXt-1.1.4-6.1.9.amzn1
libdmx-1.1.3-3.7.amzn1
libXi-1.7.2-2.2.9.amzn1
libXres-1.0.7-2.1.8.amzn1
libXxf86vm-debuginfo-1.1.3-2.1.9.amzn1
libXxf86vm-1.1.3-2.1.9.amzn1
libXvMC-devel-1.0.8-2.1.8.amzn1
libXcursor-1.1.14-2.1.9.amzn1
libXres-devel-1.0.7-2.1.8.amzn1
libXcursor-debuginfo-1.1.14-2.1.9.amzn1
libXt-debuginfo-1.1.4-6.1.9.amzn1
libXv-devel-1.0.9-2.1.8.amzn1
libXres-debuginfo-1.0.7-2.1.8.amzn1
libXv-debuginfo-1.0.9-2.1.8.amzn1
libXcursor-devel-1.1.14-2.1.9.amzn1
libXxf86vm-devel-1.1.3-2.1.9.amzn1
libXt-devel-1.1.4-6.1.9.amzn1
libXrandr-debuginfo-1.4.1-2.1.8.amzn1
libXrender-devel-0.9.8-2.1.9.amzn1
libXfixes-5.0.1-2.1.8.amzn1
libX11-common-1.6.0-2.2.12.amzn1
libXxf86dga-debuginfo-1.1.4-2.1.8.amzn1
libXrandr-1.4.1-2.1.8.amzn1
libXv-1.0.9-2.1.8.amzn1
libXrender-0.9.8-2.1.9.amzn1

libdmx-devel-1.1.3-3.7.amzn1

i686
libXfixes-devel-5.0.1-2.1.8.amzn1
libX11-debuginfo-1.6.0-2.2.12.amzn1
libXxf86dga-devel-1.1.4-2.1.8.amzn1
libXvMC-debuginfo-1.0.8-2.1.8.amzn1
libX11-1.6.0-2.2.12.amzn1
libXi-devel-1.7.2-2.2.9.amzn1
libXrandr-devel-1.4.1-2.1.8.amzn1
libXrender-debuginfo-0.9.8-2.1.9.amzn1
libXvMC-1.0.8-2.1.8.amzn1
libdmx-debuginfo-1.1.3-3.7.amzn1
libXfixes-debuginfo-5.0.1-2.1.8.amzn1
libXi-debuginfo-1.7.2-2.2.9.amzn1
libX11-devel-1.6.0-2.2.12.amzn1
libXt-1.1.4-6.1.9.amzn1
libdmx-1.1.3-3.7.amzn1
libXi-1.7.2-2.2.9.amzn1
libXres-1.0.7-2.1.8.amzn1
libXxf86vm-debuginfo-1.1.3-2.1.9.amzn1
libXxf86vm-1.1.3-2.1.9.amzn1
libXvMC-devel-1.0.8-2.1.8.amzn1
libXcursor-1.1.14-2.1.9.amzn1
libXres-devel-1.0.7-2.1.8.amzn1
libXcursor-debuginfo-1.1.14-2.1.9.amzn1
libXxf86dga-1.1.4-2.1.8.amzn1
libXv-devel-1.0.9-2.1.8.amzn1
libXres-debuginfo-1.0.7-2.1.8.amzn1
libXv-debuginfo-1.0.9-2.1.8.amzn1
libXcursor-devel-1.1.14-2.1.9.amzn1
libXxf86vm-devel-1.1.3-2.1.9.amzn1
libXt-devel-1.1.4-6.1.9.amzn1
libXrandr-debuginfo-1.4.1-2.1.8.amzn1
libXrender-devel-0.9.8-2.1.9.amzn1
libXfixes-5.0.1-2.1.8.amzn1
libX11-common-1.6.0-2.2.12.amzn1
libXxf86dga-debuginfo-1.1.4-2.1.8.amzn1
libXrandr-1.4.1-2.1.8.amzn1
libXv-1.0.9-2.1.8.amzn1
libXrender-0.9.8-2.1.9.amzn1
libXt-debuginfo-1.1.4-6.1.9.amzn1
libdmx-devel-1.1.3-3.7.amzn1

noarch
xorg-x11-proto-devel-7.7-9.10.amzn1

177996 - Gentoo Linux GLSA-201411-11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-0128, CVE-2014-7141, CVE-2014-7142

Description

The scan detected that the host is missing the following update:
GLSA-201411-11

Observation

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

http://security.gentoo.org/glsa/glsa-201411-11.xml

Affected packages:
net-proxy/squid < 3.3.13-r1

188545 - Fedora Linux 19 FEDORA-2014-15535 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8958, CVE-2014-8959, CVE-2014-8960, CVE-2014-8961

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15535

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145023.html

Fedora Core 19

phpMyAdmin-4.2.12-1.fc19

188550 - Fedora Linux 19 FEDORA-2014-15307 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-0480, CVE-2014-0481, CVE-2014-0482, CVE-2014-0483

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15307

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145025.html

Fedora Core 19

python-django14-1.4.16-1.fc19

188551 - Fedora Linux 20 FEDORA-2014-15507 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9031, CVE-2014-9032, CVE-2014-9033, CVE-2014-9034, CVE-2014-9035, CVE-2014-9036, CVE-2014-9037, CVE-2014-9038, CVE-2014-9039

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15507

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145127.html

Fedora Core 20

wordpress-4.0.1-1.fc20

188554 - Fedora Linux 20 FEDORA-2014-15538 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8958, CVE-2014-8959, CVE-2014-8960, CVE-2014-8961

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15538

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145013.html

Fedora Core 20

phpMyAdmin-4.2.12-1.fc20

188555 - Fedora Linux 20 FEDORA-2014-14791 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-5615, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6478, CVE-2014-6484, CVE-2014-6495, CVE-2014-6505, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14791

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145119.html

Fedora Core 20

mariadb-galera-5.5.40-2.fc20

188556 - Fedora Linux 19 FEDORA-2014-15515 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-6662, CVE-2014-9015

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15515

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145129.html

Fedora Core 19

drupal6-6.34-1.fc19

188557 - Fedora Linux 20 FEDORA-2014-15519 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-6662, CVE-2014-9015

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15519

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145143.html

Fedora Core 20

drupal6-6.34-1.fc20

188558 - Fedora Linux 20 FEDORA-2014-15266 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-0480, CVE-2014-0481, CVE-2014-0482, CVE-2014-0483

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15266

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145033.html

Fedora Core 20

python-django14-1.4.16-1.fc20

188560 - Fedora Linux 19 FEDORA-2014-15526 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9031, CVE-2014-9032, CVE-2014-9033, CVE-2014-9034, CVE-2014-9035, CVE-2014-9036, CVE-2014-9037, CVE-2014-9038, CVE-2014-9039

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15526

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145140.html

Fedora Core 19

wordpress-4.0.1-1.fc19

188565 - Fedora Linux 20 FEDORA-2014-15541 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8767, CVE-2014-8768, CVE-2014-8769

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15541

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/144951.html

Fedora Core 20

tcpdump-4.5.1-2.fc20

16945 - (SOL15428) F5 BIG-IP Apache Tomcat Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-0096

Description

A security bypass 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 security bypass vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the embedded version of Tomcat which fails to restrict XSLT stylesheets. Successful exploitation could allow an attacker to bypass security restrictions to read arbitrary files.

16946 - (SOL15430) F5 BIG-IP OpenSSH Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-2532

Description

A security bypass 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 security bypass vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the embedded version of OpenSSH which fails to support wildcards in the AcceptEnv parameter. Successful exploitation could allow an attacker to bypass security restrictions.

16947 - (SOL15432) F5 BIG-IP Apache Tomcat Integer Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-0099

Description

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

Observation

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

An integer overflow vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the embedded version of Tomcat. Successful exploitation could allow an attacker to execute remote code through the HTTP smuggling method.

16950 - (SOL15299) F5 BIG-IP Linux Kernel Human Interface Device Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-2888

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Linux kernel Human Interface

Device subsystem. Successful exploitation could allow an attacker to cause a denial of service condition.

16951 - (SOL15277) F5 BIG-IP ICMP Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-1999-0524

Description

An information disclosure 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.

An information disclosure vulnerability is present in some versions of F5 BIG-IP systems. The flaw occurs when ICMP type 13 and 14 are sent to the affected device. Successful exploitation could allow an attacker to obtain the network netmask and timestamp information.

16952 - (SOL15273) F5 BIG-IP Apache HTTPOnly Cookies Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2012-0053

Description

A security bypass 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 security bypass vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the embedded version of Apache web server which fails to restrict the headers information when responding to HTTP bad requests. Successful exploitation could allow an attacker to access the values of HTTPOnly cookies.

17045 - (SOL15426) F5 BIG-IP Apache Tomcat Integer Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-0075

Description

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

Observation

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

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

17328 - (HPSBMU03126) HP Operations Manager Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-2647

Description

A cross-site scripting vulnerability exists in some versions HP Operations Manager.

Observation

HP Operations Manager is Hewlett-Packard System monitoring.

A cross-site scripting vulnerability exists in some versions HP Operations Manager. This issue is due to improper sanitization of user-provided input data in the HP Operations Agent. An attacker can exploit this vulnerability to execute arbitrary script code in the browser of a user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch further attacks.

17329 - (HPSBMU03126) HP Operations Manager Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-2647

Description

A cross-site scripting vulnerability exists in some versions HP Operations Manager.

Observation

HP Operations Manager is Hewlett-Packard System monitoring.

A cross-site scripting vulnerability exists in some versions HP Operations Manager. This issue is due to improper sanitization of user-provided input data in the HP Operations Agent. An attacker can exploit this vulnerability to execute arbitrary script code in the browser of a user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch further attacks.

17442 - (SOL15481) F5 BIG-IP BIND Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2012-1033

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in BIND. Successful exploitation could result in continued resolvability of previously revoked domain names.

17444 - (SOL15722) F5 BIG-IP OpenSSL DTLS SRTP Memory Leak Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3513

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in OpenSSL component. Successful exploitation could allow an attacker to cause denial of service.

17452 - (SOL15797) F5 BIG-IP Kernel KVM Subsystem Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2012-4461

Description

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

Observation

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

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

17455 - Cisco IOS DLSw Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-7992

Description

An information disclosure vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

An information disclosure vulnerability is present in some versions of Cisco IOS. The flaw lies in the DLSw feature of Cisco IOS. Successful exploitation could allow a remote attacker to extract information from previously processed packets.

17457 - (SOL15792) F5 BIG-IP Path MTU Discovery Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2004-1060

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in multiple TCP/IP and ICMP implementations. Successful exploitation could allow an attacker to cause a denial of service condition.

17461 - (SOL15852) F5 BIG-IP Linux Kernel Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3122

Description

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

Observation

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

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

17464 - HP Database And Middleware Automation Unspecified Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-6212

Description

An information disclosure vulnerability is present in some versions of HP Database and Middleware Automation.

Observation

HP Database and Middleware Automation is a database management system.

An information disclosure vulnerability is present in some versions of HP Database and Middleware Automation. The flaw is due to an unspecified vector. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

85832 - CentOS 7 CESA-2014-1912 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
CESA-2014-1912

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-December/020792.html

CentOS 7
x86_64
ruby-libs-2.0.0.353-22.el7_0
rubygem-bigdecimal-1.2.0-22.el7_0
ruby-2.0.0.353-22.el7_0
ruby-devel-2.0.0.353-22.el7_0
ruby-tcltk-2.0.0.353-22.el7_0

rubygem-psych-2.0.0-22.el7_0
rubygem-json-1.7.7-22.el7_0
rubygem-io-console-0.4.2-22.el7_0

i686
ruby-libs-2.0.0.353-22.el7_0

noarch
rubygems-devel-2.0.14-22.el7_0
rubygem-minitest-4.3.2-22.el7_0
rubygem-rdoc-4.0.0-22.el7_0
ruby-doc-2.0.0.353-22.el7_0
ruby-irb-2.0.0.353-22.el7_0
rubygems-2.0.14-22.el7_0
rubygem-rake-0.9.6-22.el7_0

85833 - CentOS 6 CESA-2014-1911 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
CESA-2014-1911

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-December/020791.html

CentOS 6
x86_64
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-ri-1.8.7.374-3.el6_6
ruby-tcltk-1.8.7.374-3.el6_6
ruby-docs-1.8.7.374-3.el6_6
ruby-static-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6

i686
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-ri-1.8.7.374-3.el6_6
ruby-tcltk-1.8.7.374-3.el6_6
ruby-docs-1.8.7.374-3.el6_6
ruby-static-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6

91674 - Oracle Enterprise Linux ELSA-2014-1912 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
ELSA-2014-1912

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004674.html

OEL7
x86_64
ruby-libs-2.0.0.353-22.el7_0
rubygems-devel-2.0.14-22.el7_0
rubygem-bigdecimal-1.2.0-22.el7_0
ruby-irb-2.0.0.353-22.el7_0
rubygems-2.0.14-22.el7_0
ruby-2.0.0.353-22.el7_0
rubygem-minitest-4.3.2-22.el7_0
ruby-devel-2.0.0.353-22.el7_0
ruby-doc-2.0.0.353-22.el7_0
rubygem-psych-2.0.0-22.el7_0
rubygem-rdoc-4.0.0-22.el7_0
rubygem-rake-0.9.6-22.el7_0
ruby-tcltk-2.0.0.353-22.el7_0
rubygem-json-1.7.7-22.el7_0
rubygem-io-console-0.4.2-22.el7_0

91675 - Oracle Enterprise Linux ELSA-2014-1911 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
ELSA-2014-1911

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004673.html

OEL6
x86_64
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-ri-1.8.7.374-3.el6_6
ruby-tcltk-1.8.7.374-3.el6_6
ruby-docs-1.8.7.374-3.el6_6

ruby-static-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6

i386
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-ri-1.8.7.374-3.el6_6
ruby-tcltk-1.8.7.374-3.el6_6
ruby-docs-1.8.7.374-3.el6_6
ruby-static-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6

93428 - Mandriva Linux MBS1 MDVSA-2014-234 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9087

Description

The scan detected that the host is missing the following update:
MDVSA-2014-234

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-2014%3A234/

Mandriva Linux mbs1
x86_64
lib64ksba8-1.3.2-1
lib64ksba-devel-1.3.2-1

93429 - Mandriva Linux MBS1 MDVSA-2014-236 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3710

Description

The scan detected that the host is missing the following update:
MDVSA-2014-236

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-2014%3A236/

Mandriva Linux mbs1
x86_64
lib64magic-devel-5.12-1.6
lib64magic1-5.12-1.6
file-5.12-1.6

lib64magic-static-devel-5.12-1.6
python-magic-5.12-1.6

130004 - Debian Linux 7.0 DSA-3076-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714

Description

The scan detected that the host is missing the following update:
DSA-3076-1

Observation

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

http://www.debian.org/security/2014/dsa-3076

Debian 7.0
all
wireshark_1.8.2-5wheezy13

130007 - Debian Linux 7.0 DSA-3083-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9116

Description

The scan detected that the host is missing the following update:
DSA-3083-1

Observation

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

http://www.debian.org/security/2014/dsa-3083

Debian 7.0
all
mutt_1.5.21-6.2+deb7u3

130008 - Debian Linux 7.0 DSA-3078-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9087

Description

The scan detected that the host is missing the following update:
DSA-3078-1

Observation

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

http://www.debian.org/security/2014/dsa-3078

Debian 7.0
all
libksba8_1.2.0-2+deb7u1
libksba-dev_1.2.0-2+deb7u1

140625 - Red Hat Enterprise Linux RHSA-2014-1912 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
RHSA-2014-1912

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1912.html

RHEL7WS
x86_64
rubygem-bigdecimal-1.2.0-22.el7_0
ruby-2.0.0.353-22.el7_0
ruby-debuginfo-2.0.0.353-22.el7_0
rubygem-io-console-0.4.2-22.el7_0
ruby-libs-2.0.0.353-22.el7_0
rubygem-json-1.7.7-22.el7_0
rubygem-psych-2.0.0-22.el7_0

noarch
rubygem-rdoc-4.0.0-22.el7_0
rubygems-2.0.14-22.el7_0
ruby-irb-2.0.0.353-22.el7_0

RHEL7D
x86_64
rubygem-bigdecimal-1.2.0-22.el7_0
ruby-2.0.0.353-22.el7_0
ruby-debuginfo-2.0.0.353-22.el7_0
rubygem-io-console-0.4.2-22.el7_0
ruby-libs-2.0.0.353-22.el7_0
rubygem-json-1.7.7-22.el7_0
rubygem-psych-2.0.0-22.el7_0

noarch
rubygem-rdoc-4.0.0-22.el7_0
rubygems-2.0.14-22.el7_0
ruby-irb-2.0.0.353-22.el7_0

RHEL7S
x86_64

rubygem-bigdecimal-1.2.0-22.el7_0
ruby-2.0.0.353-22.el7_0
ruby-debuginfo-2.0.0.353-22.el7_0
rubygem-io-console-0.4.2-22.el7_0
ruby-libs-2.0.0.353-22.el7_0
rubygem-json-1.7.7-22.el7_0
rubygem-psych-2.0.0-22.el7_0

noarch
rubygem-rdoc-4.0.0-22.el7_0
rubygems-2.0.14-22.el7_0
ruby-irb-2.0.0.353-22.el7_0

140628 - Red Hat Enterprise Linux RHSA-2014-1911 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
RHSA-2014-1911

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1911.html

RHEL6D
x86_64
ruby-debuginfo-1.8.7.374-3.el6_6
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6

i386
ruby-debuginfo-1.8.7.374-3.el6_6
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6

RHEL6S
x86_64
ruby-debuginfo-1.8.7.374-3.el6_6
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6

i386
ruby-debuginfo-1.8.7.374-3.el6_6
ruby-1.8.7.374-3.el6_6

ruby-irb-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6

RHEL6WS
x86_64
ruby-debuginfo-1.8.7.374-3.el6_6
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6

i386
ruby-debuginfo-1.8.7.374-3.el6_6
ruby-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6

140629 - Red Hat Enterprise Linux RHSA-2014-1913 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
RHSA-2014-1913

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1913.html

RHEL7WS
x86_64
ruby193-rubygem-io-console-0.3-50.el7
ruby193-rubygem-rdoc-3.9.5-50.el7
ruby193-ruby-1.9.3.484-50.el7
ruby193-ruby-debuginfo-1.9.3.484-50.el7
ruby193-ruby-doc-1.9.3.484-50.el7
ruby193-ruby-libs-1.9.3.484-50.el7
ruby193-rubygem-bigdecimal-1.1.0-50.el7
ruby193-ruby-devel-1.9.3.484-50.el7
ruby193-ruby-tcltk-1.9.3.484-50.el7
ruby193-rubygem-json-1.5.5-50.el7

noarch
ruby193-ruby-irb-1.9.3.484-50.el7
ruby193-rubygems-devel-1.8.23-50.el7
ruby193-rubygem-rake-0.9.2.2-50.el7
ruby193-rubygem-minitest-2.5.1-50.el7
ruby193-rubygems-1.8.23-50.el7

RHEL7S
x86_64
ruby193-rubygem-io-console-0.3-50.el7
ruby193-rubygem-rdoc-3.9.5-50.el7
ruby193-ruby-1.9.3.484-50.el7
ruby193-ruby-debuginfo-1.9.3.484-50.el7
ruby193-ruby-doc-1.9.3.484-50.el7
ruby193-ruby-libs-1.9.3.484-50.el7
ruby193-rubygem-bigdecimal-1.1.0-50.el7
ruby193-ruby-devel-1.9.3.484-50.el7
ruby193-ruby-tcltk-1.9.3.484-50.el7
ruby193-rubygem-json-1.5.5-50.el7

noarch
ruby193-ruby-irb-1.9.3.484-50.el7
ruby193-rubygems-devel-1.8.23-50.el7
ruby193-rubygem-rake-0.9.2.2-50.el7
ruby193-rubygem-minitest-2.5.1-50.el7
ruby193-rubygems-1.8.23-50.el7

RHEL6S
x86_64
ruby193-rubygem-io-console-0.3-50.el6
ruby193-rubygem-rdoc-3.9.5-50.el6
ruby193-ruby-1.9.3.484-50.el6
ruby193-rubygem-json-1.5.5-50.el6
ruby193-ruby-libs-1.9.3.484-50.el6
ruby193-ruby-doc-1.9.3.484-50.el6
ruby193-ruby-devel-1.9.3.484-50.el6
ruby193-rubygem-bigdecimal-1.1.0-50.el6
ruby193-ruby-debuginfo-1.9.3.484-50.el6
ruby193-ruby-tcltk-1.9.3.484-50.el6

noarch
ruby193-rubygems-1.8.23-50.el6
ruby193-rubygem-rake-0.9.2.2-50.el6
ruby193-rubygems-devel-1.8.23-50.el6
ruby193-rubygem-minitest-2.5.1-50.el6
ruby193-ruby-irb-1.9.3.484-50.el6

RHEL6WS
x86_64
ruby193-rubygem-io-console-0.3-50.el6
ruby193-rubygem-rdoc-3.9.5-50.el6
ruby193-ruby-1.9.3.484-50.el6
ruby193-rubygem-json-1.5.5-50.el6
ruby193-ruby-libs-1.9.3.484-50.el6
ruby193-ruby-doc-1.9.3.484-50.el6
ruby193-ruby-devel-1.9.3.484-50.el6
ruby193-rubygem-bigdecimal-1.1.0-50.el6
ruby193-ruby-debuginfo-1.9.3.484-50.el6
ruby193-ruby-tcltk-1.9.3.484-50.el6

noarch
ruby193-rubygems-1.8.23-50.el6
ruby193-rubygem-rake-0.9.2.2-50.el6
ruby193-rubygems-devel-1.8.23-50.el6
ruby193-rubygem-minitest-2.5.1-50.el6
ruby193-ruby-irb-1.9.3.484-50.el6

140631 - Red Hat Enterprise Linux RHSA-2014-1914 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
RHSA-2014-1914

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1914.html

RHEL7WS
x86_64
ruby200-rubygem-bigdecimal-1.2.0-24.el7
ruby200-rubygem-json-1.7.7-24.el7
ruby200-ruby-debuginfo-2.0.0.353-24.el7
ruby200-ruby-2.0.0.353-24.el7
ruby200-ruby-libs-2.0.0.353-24.el7
ruby200-rubygem-io-console-0.4.2-24.el7
ruby200-ruby-tcltk-2.0.0.353-24.el7
ruby200-rubygem-psych-2.0.0-24.el7
ruby200-ruby-devel-2.0.0.353-24.el7
ruby200-rubygems-2.0.14-24.el7

noarch
ruby200-rubygems-devel-2.0.14-24.el7
ruby200-rubygem-rake-0.9.6-24.el7
ruby200-rubygem-minitest-4.3.2-24.el7
ruby200-rubygem-rdoc-4.0.0-24.el7
ruby200-ruby-doc-2.0.0.353-24.el7
ruby200-ruby-irb-2.0.0.353-24.el7

RHEL7S
x86_64
ruby200-rubygem-bigdecimal-1.2.0-24.el7
ruby200-rubygem-json-1.7.7-24.el7
ruby200-ruby-debuginfo-2.0.0.353-24.el7
ruby200-ruby-2.0.0.353-24.el7
ruby200-ruby-libs-2.0.0.353-24.el7
ruby200-rubygem-io-console-0.4.2-24.el7
ruby200-ruby-tcltk-2.0.0.353-24.el7
ruby200-rubygem-psych-2.0.0-24.el7
ruby200-ruby-devel-2.0.0.353-24.el7
ruby200-rubygems-2.0.14-24.el7

noarch
ruby200-rubygems-devel-2.0.14-24.el7
ruby200-rubygem-rake-0.9.6-24.el7
ruby200-rubygem-minitest-4.3.2-24.el7
ruby200-rubygem-rdoc-4.0.0-24.el7
ruby200-ruby-doc-2.0.0.353-24.el7
ruby200-ruby-irb-2.0.0.353-24.el7

RHEL6S

x86_64
ruby200-rubygem-bigdecimal-1.2.0-24.el6
ruby200-ruby-debuginfo-2.0.0.353-24.el6
ruby200-ruby-2.0.0.353-24.el6
ruby200-ruby-libs-2.0.0.353-24.el6
ruby200-rubygem-json-1.7.7-24.el6
ruby200-ruby-tcltk-2.0.0.353-24.el6
ruby200-rubygem-io-console-0.4.2-24.el6
ruby200-rubygem-psych-2.0.0-24.el6
ruby200-rubygems-2.0.14-24.el6
ruby200-ruby-devel-2.0.0.353-24.el6

noarch
ruby200-ruby-irb-2.0.0.353-24.el6
ruby200-rubygem-rake-0.9.6-24.el6
ruby200-rubygems-devel-2.0.14-24.el6
ruby200-rubygem-rdoc-4.0.0-24.el6
ruby200-rubygem-minitest-4.3.2-24.el6
ruby200-ruby-doc-2.0.0.353-24.el6

RHEL6WS
x86_64
ruby200-rubygem-bigdecimal-1.2.0-24.el6
ruby200-ruby-debuginfo-2.0.0.353-24.el6
ruby200-ruby-2.0.0.353-24.el6
ruby200-ruby-libs-2.0.0.353-24.el6
ruby200-rubygem-json-1.7.7-24.el6
ruby200-ruby-tcltk-2.0.0.353-24.el6
ruby200-rubygem-io-console-0.4.2-24.el6
ruby200-rubygem-psych-2.0.0-24.el6
ruby200-rubygems-2.0.14-24.el6
ruby200-ruby-devel-2.0.0.353-24.el6

noarch
ruby200-ruby-irb-2.0.0.353-24.el6
ruby200-rubygem-rake-0.9.6-24.el6
ruby200-rubygems-devel-2.0.14-24.el6
ruby200-rubygem-rdoc-4.0.0-24.el6
ruby200-rubygem-minitest-4.3.2-24.el6
ruby200-ruby-doc-2.0.0.353-24.el6

142530 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1503-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1503-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00104.html

SuSE Linux 13.1

i586
wireshark-1.10.11-28.1
wireshark-debugsource-1.10.11-28.1
wireshark-debuginfo-1.10.11-28.1
wireshark-devel-1.10.11-28.1

SuSE Linux 12.3
i586
wireshark-devel-1.10.11-1.48.1
wireshark-debugsource-1.10.11-1.48.1
wireshark-1.10.11-1.48.1
wireshark-debuginfo-1.10.11-1.48.1

SuSE Linux 13.2
i586
wireshark-debuginfo-1.12.2-4.1
wireshark-devel-1.12.2-4.1
wireshark-ui-qt-1.12.2-4.1
wireshark-debugsource-1.12.2-4.1
wireshark-ui-gtk-debuginfo-1.12.2-4.1
wireshark-ui-qt-debuginfo-1.12.2-4.1
wireshark-ui-gtk-1.12.2-4.1
wireshark-1.12.2-4.1

142531 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1502-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7819

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1502-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00103.html

SuSE Linux 13.1
i586
rubygem-sprockets-2_1-doc-2.1.3-6.4.1
rubygem-sprockets-2_1-2.1.3-6.4.1

SuSE Linux 12.3
i586
rubygem-sprockets-2_1-doc-2.1.3-4.4.1
rubygem-sprockets-2_1-2.1.3-4.4.1

SuSE Linux 13.2
i586
rubygem-sprockets-2_1-doc-2.1.3-8.4.1
rubygem-sprockets-2_1-2.1.3-8.4.1

142532 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1515-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7818, CVE-2014-7829

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1515-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00112.html

SuSE Linux 13.1
i586
rubygem-actionpack-3_2-3.2.13-2.28.1
rubygem-actionpack-3_2-doc-3.2.13-2.28.1

SuSE Linux 12.3
i586
rubygem-actionpack-3_2-3.2.12-1.32.1
rubygem-actionpack-3_2-doc-3.2.12-1.32.1

SuSE Linux 13.2
i586
rubygem-actionpack-3_2-3.2.17-3.4.1
rubygem-actionpack-3_2-doc-3.2.17-3.4.1

142533 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1516-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3710

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1516-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00113.html

SuSE Linux 13.1
x86_64
libmagic1-debuginfo-32bit-5.15-4.24.1
libmagic1-32bit-5.15-4.24.1

i586
file-debugsource-5.15-4.24.1
file-5.15-4.24.1
python-magic-5.15-4.24.1
file-debuginfo-5.15-4.24.1
file-devel-5.15-4.24.1
libmagic1-5.15-4.24.1

file-magic-5.15-4.24.1
libmagic1-debuginfo-5.15-4.24.1

SuSE Linux 12.3
x86_64
libmagic1-debuginfo-32bit-5.11-12.27.1
libmagic1-32bit-5.11-12.27.1

i586
libmagic1-5.11-12.27.1
file-devel-5.11-12.27.1
file-debuginfo-5.11-12.27.1
libmagic-data-5.11-12.27.1
file-debugsource-5.11-12.27.1
file-5.11-12.27.1
libmagic1-debuginfo-5.11-12.27.1
python-magic-5.11-12.27.1

SuSE Linux 13.2
x86_64
libmagic1-32bit-5.19-3.4.1
libmagic1-debuginfo-32bit-5.19-3.4.1

i586
file-debugsource-5.19-3.4.1
libmagic1-debuginfo-5.19-3.4.1
file-debuginfo-5.19-3.4.1
libmagic1-5.19-3.4.1
file-devel-5.19-3.4.1
file-5.19-3.4.1
python-magic-5.19-3.4.1
file-magic-5.19-3.4.1

142534 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1513-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7819

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1513-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00110.html

SuSE Linux 13.1
i586
rubygem-sprockets-doc-2.10.0-2.4.1
rubygem-sprockets-2.10.0-2.4.1

SuSE Linux 12.3
i586
rubygem-sprockets-doc-2.8.2-2.4.1
rubygem-sprockets-2.8.2-2.4.1

142535 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1504-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7819

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1504-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00105.html

SuSE Linux 13.1
i586
rubygem-sprockets-2_2-doc-2.2.2-5.4.1
rubygem-sprockets-2_2-2.2.2-5.4.1

SuSE Linux 12.3
i586
rubygem-sprockets-2_2-2.2.2-2.4.1
rubygem-sprockets-2_2-doc-2.2.2-2.4.1

SuSE Linux 13.2
i586
rubygem-sprockets-2_2-doc-2.2.2-8.4.1
rubygem-sprockets-2_2-2.2.2-8.4.1

142536 - SuSE Linux 13.2 openSUSE-SU-2014:1514-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7819

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1514-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00111.html

SuSE Linux 13.2
i586
rubygem-sprockets-2.12.1-2.4.1
rubygem-tilt-1_4-testsuite-1.4.1-2.1
rubygem-tilt-1_4-1.4.1-2.1
rubygem-sprockets-doc-2.12.1-2.4.1
rubygem-tilt-1_4-doc-1.4.1-2.1

170428 - Amazon Linux AMI ALAS-2014-453 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3710

Description

The scan detected that the host is missing the following update:
ALAS-2014-453

Observation

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

https://alas.aws.amazon.com/ALAS-2014-453.html

Amazon Linux AMI
x86_64
file-debuginfo-5.19-7.24.amzn1
file-libs-5.19-7.24.amzn1
file-5.19-7.24.amzn1
file-static-5.19-7.24.amzn1
file-devel-5.19-7.24.amzn1

i686
file-debuginfo-5.19-7.24.amzn1
file-libs-5.19-7.24.amzn1
file-5.19-7.24.amzn1
file-static-5.19-7.24.amzn1
file-devel-5.19-7.24.amzn1

noarch
python-magic-5.19-7.24.amzn1

170430 - Amazon Linux AMI ALAS-2014-451 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3710

Description

The scan detected that the host is missing the following update:
ALAS-2014-451

Observation

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

https://alas.aws.amazon.com/ALAS-2014-451.html

Amazon Linux AMI
x86_64
php55-soap-5.5.19-2.93.amzn1
php55-mbstring-5.5.19-2.93.amzn1
php55-gd-5.5.19-2.93.amzn1
php55-ldap-5.5.19-2.93.amzn1

php55-intl-5.5.19-2.93.amzn1
php55-dba-5.5.19-2.93.amzn1
php55-recode-5.5.19-2.93.amzn1
php55-embedded-5.5.19-2.93.amzn1
php55-enchant-5.5.19-2.93.amzn1
php55-xml-5.5.19-2.93.amzn1
php55-opcache-5.5.19-2.93.amzn1
php55-tidy-5.5.19-2.93.amzn1
php55-pdo-5.5.19-2.93.amzn1
php55-xmlrpc-5.5.19-2.93.amzn1
php55-5.5.19-2.93.amzn1
php55-mssql-5.5.19-2.93.amzn1
php55-mcrypt-5.5.19-2.93.amzn1
php55-cli-5.5.19-2.93.amzn1
php55-pspell-5.5.19-2.93.amzn1
php55-fpm-5.5.19-2.93.amzn1
php55-process-5.5.19-2.93.amzn1
php55-imap-5.5.19-2.93.amzn1
php55-odbc-5.5.19-2.93.amzn1
php55-bcmath-5.5.19-2.93.amzn1
php55-common-5.5.19-2.93.amzn1
php55-debuginfo-5.5.19-2.93.amzn1
php55-devel-5.5.19-2.93.amzn1
php55-pgsql-5.5.19-2.93.amzn1
php55-mysqlnd-5.5.19-2.93.amzn1
php55-snmp-5.5.19-2.93.amzn1
php55-gmp-5.5.19-2.93.amzn1

i686
php55-soap-5.5.19-2.93.amzn1
php55-mbstring-5.5.19-2.93.amzn1
php55-gd-5.5.19-2.93.amzn1
php55-ldap-5.5.19-2.93.amzn1
php55-tidy-5.5.19-2.93.amzn1
php55-common-5.5.19-2.93.amzn1
php55-opcache-5.5.19-2.93.amzn1
php55-dba-5.5.19-2.93.amzn1
php55-recode-5.5.19-2.93.amzn1
php55-intl-5.5.19-2.93.amzn1
php55-xml-5.5.19-2.93.amzn1
php55-embedded-5.5.19-2.93.amzn1
php55-gmp-5.5.19-2.93.amzn1
php55-xmlrpc-5.5.19-2.93.amzn1
php55-5.5.19-2.93.amzn1
php55-mssql-5.5.19-2.93.amzn1
php55-mcrypt-5.5.19-2.93.amzn1
php55-cli-5.5.19-2.93.amzn1
php55-pspell-5.5.19-2.93.amzn1
php55-fpm-5.5.19-2.93.amzn1
php55-process-5.5.19-2.93.amzn1
php55-pgsql-5.5.19-2.93.amzn1
php55-odbc-5.5.19-2.93.amzn1
php55-bcmath-5.5.19-2.93.amzn1
php55-imap-5.5.19-2.93.amzn1
php55-pdo-5.5.19-2.93.amzn1
php55-debuginfo-5.5.19-2.93.amzn1
php55-devel-5.5.19-2.93.amzn1
php55-mysqlnd-5.5.19-2.93.amzn1
php55-snmp-5.5.19-2.93.amzn1
php55-enchant-5.5.19-2.93.amzn1

170431 - Amazon Linux AMI ALAS-2014-450 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3710

Description

The scan detected that the host is missing the following update:
ALAS-2014-450

Observation

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

https://alas.aws.amazon.com/ALAS-2014-450.html

Amazon Linux AMI
x86_64
php54-gd-5.4.35-1.63.amzn1
php54-intl-5.4.35-1.63.amzn1
php54-fpm-5.4.35-1.63.amzn1
php54-odbc-5.4.35-1.63.amzn1
php54-imap-5.4.35-1.63.amzn1
php54-devel-5.4.35-1.63.amzn1
php54-common-5.4.35-1.63.amzn1
php54-dba-5.4.35-1.63.amzn1
php54-debuginfo-5.4.35-1.63.amzn1
php54-enchant-5.4.35-1.63.amzn1
php54-pdo-5.4.35-1.63.amzn1
php54-pspell-5.4.35-1.63.amzn1
php54-embedded-5.4.35-1.63.amzn1
php54-recode-5.4.35-1.63.amzn1
php54-pgsql-5.4.35-1.63.amzn1
php54-tidy-5.4.35-1.63.amzn1
php54-mysql-5.4.35-1.63.amzn1
php54-snmp-5.4.35-1.63.amzn1
php54-xml-5.4.35-1.63.amzn1
php54-mssql-5.4.35-1.63.amzn1
php54-mbstring-5.4.35-1.63.amzn1
php54-bcmath-5.4.35-1.63.amzn1
php54-ldap-5.4.35-1.63.amzn1
php54-mysqlnd-5.4.35-1.63.amzn1
php54-soap-5.4.35-1.63.amzn1
php54-mcrypt-5.4.35-1.63.amzn1
php54-xmlrpc-5.4.35-1.63.amzn1
php54-5.4.35-1.63.amzn1
php54-process-5.4.35-1.63.amzn1
php54-cli-5.4.35-1.63.amzn1

i686
php54-pgsql-5.4.35-1.63.amzn1
php54-gd-5.4.35-1.63.amzn1
php54-snmp-5.4.35-1.63.amzn1
php54-fpm-5.4.35-1.63.amzn1
php54-mysql-5.4.35-1.63.amzn1
php54-cli-5.4.35-1.63.amzn1
php54-devel-5.4.35-1.63.amzn1
php54-common-5.4.35-1.63.amzn1

php54-dba-5.4.35-1.63.amzn1
php54-enchant-5.4.35-1.63.amzn1
php54-pdo-5.4.35-1.63.amzn1
php54-debuginfo-5.4.35-1.63.amzn1
php54-embedded-5.4.35-1.63.amzn1
php54-recode-5.4.35-1.63.amzn1
php54-imap-5.4.35-1.63.amzn1
php54-tidy-5.4.35-1.63.amzn1
php54-soap-5.4.35-1.63.amzn1
php54-xml-5.4.35-1.63.amzn1
php54-mssql-5.4.35-1.63.amzn1
php54-mbstring-5.4.35-1.63.amzn1
php54-intl-5.4.35-1.63.amzn1
php54-bcmath-5.4.35-1.63.amzn1
php54-mysqlnd-5.4.35-1.63.amzn1
php54-ldap-5.4.35-1.63.amzn1
php54-odbc-5.4.35-1.63.amzn1
php54-pspell-5.4.35-1.63.amzn1
php54-xmlrpc-5.4.35-1.63.amzn1
php54-5.4.35-1.63.amzn1
php54-process-5.4.35-1.63.amzn1
php54-mcrypt-5.4.35-1.63.amzn1

174598 - Scientific Linux Security ERRATA Moderate: ruby on SL7.x x86_64 (1412-79)

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ruby on SL7.x x86_64 (1412-79)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=79

SL7
x86_64
ruby-libs-2.0.0.353-22.el7_0
rubygem-bigdecimal-1.2.0-22.el7_0
ruby-2.0.0.353-22.el7_0
ruby-devel-2.0.0.353-22.el7_0
ruby-debuginfo-2.0.0.353-22.el7_0
ruby-tcltk-2.0.0.353-22.el7_0
rubygem-psych-2.0.0-22.el7_0
rubygem-json-1.7.7-22.el7_0
rubygem-io-console-0.4.2-22.el7_0

noarch
rubygems-devel-2.0.14-22.el7_0
rubygem-minitest-4.3.2-22.el7_0
rubygem-rdoc-4.0.0-22.el7_0
rubygems-2.0.14-22.el7_0
ruby-irb-2.0.0.353-22.el7_0
rubygem-rake-0.9.6-22.el7_0

ruby-doc-2.0.0.353-22.el7_0

174599 - Scientific Linux Security ERRATA Moderate: ruby on SL6.x i386/x86_64 (1412-194)

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

Risk Level: Medium

CVE: CVE-2014-8080, CVE-2014-8090

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ruby on SL6.x i386/x86_64 (1412-194)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=194

SL6
x86_64
ruby-1.8.7.374-3.el6_6
ruby-debuginfo-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-ri-1.8.7.374-3.el6_6
ruby-tcltk-1.8.7.374-3.el6_6
ruby-docs-1.8.7.374-3.el6_6
ruby-static-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6

i386
ruby-1.8.7.374-3.el6_6
ruby-debuginfo-1.8.7.374-3.el6_6
ruby-irb-1.8.7.374-3.el6_6
ruby-libs-1.8.7.374-3.el6_6
ruby-devel-1.8.7.374-3.el6_6
ruby-ri-1.8.7.374-3.el6_6
ruby-tcltk-1.8.7.374-3.el6_6
ruby-docs-1.8.7.374-3.el6_6
ruby-static-1.8.7.374-3.el6_6
ruby-rdoc-1.8.7.374-3.el6_6

184628 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2423-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6497, CVE-2014-9050

Description

The scan detected that the host is missing the following update:
USN-2423-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-November/002741.html

Ubuntu 14.10

clamav_0.98.5+dfsg-0ubuntu0.14.10.1

Ubuntu 14.04

clamav_0.98.5+addedllvm-0ubuntu0.14.04.1

Ubuntu 12.04

clamav_0.98.5+addedllvm-0ubuntu0.12.04.1

184630 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2427-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9087

Description

The scan detected that the host is missing the following update:
USN-2427-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-November/002744.html

Ubuntu 14.10

libksba8_1.3.0-3ubuntu0.14.10.1

Ubuntu 14.04

libksba8_1.3.0-3ubuntu0.14.04.1

Ubuntu 12.04

libksba8_1.2.0-2ubuntu0.1

188544 - Fedora Linux 19 FEDORA-2014-15463 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6497, CVE-2014-9050

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15463

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-November/144979.html

Fedora Core 19

clamav-0.98.5-1.fc19

188561 - Fedora Linux 19 FEDORA-2014-15522 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9016

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15522

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145138.html

Fedora Core 19

drupal7-7.34-1.fc19

188563 - Fedora Linux 20 FEDORA-2014-15528 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9016

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15528

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145126.html

Fedora Core 20

drupal7-7.34-1.fc20

17478 - IBM WebSphere Portal Unspecified Cross-Site Scripting Vulnerability II

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

Risk Level: Medium

CVE: CVE-2014-6093

Description

A vulnerability is present in some versions of IBM WebSphere Portal.

Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw is due to improper validation of user-supplied input. Successful exploitation could allow a remote attacker to inject arbitrary web script or HTML code.

93431 - Mandriva Linux MBS1 MDVSA-2014-232 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7817

Description

The scan detected that the host is missing the following update:
MDVSA-2014-232

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-2014%3A232/

Mandriva Linux mbs1
x86_64
glibc-i18ndata-2.14.1-12.10
nscd-2.14.1-12.10
glibc-doc-pdf-2.14.1-12.10
glibc-devel-2.14.1-12.10
glibc-profile-2.14.1-12.10
glibc-2.14.1-12.10
glibc-static-devel-2.14.1-12.10
glibc-utils-2.14.1-12.10
glibc-doc-2.14.1-12.10

140627 - Red Hat Enterprise Linux RHSA-2014-1948 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

The scan detected that the host is missing the following update:
RHSA-2014-1948

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1948.html

RHEL5D
x86_64
nss-tools-3.16.2.3-1.el5_11

nss-debuginfo-3.16.2.3-1.el5_11
nss-3.16.2.3-1.el5_11

i386
nss-tools-3.16.2.3-1.el5_11
nss-debuginfo-3.16.2.3-1.el5_11
nss-3.16.2.3-1.el5_11

RHEL5S
x86_64
nss-pkcs11-devel-3.16.2.3-1.el5_11
nss-tools-3.16.2.3-1.el5_11
nss-debuginfo-3.16.2.3-1.el5_11
nss-3.16.2.3-1.el5_11
nss-devel-3.16.2.3-1.el5_11

i386
nss-pkcs11-devel-3.16.2.3-1.el5_11
nss-tools-3.16.2.3-1.el5_11
nss-debuginfo-3.16.2.3-1.el5_11
nss-3.16.2.3-1.el5_11
nss-devel-3.16.2.3-1.el5_11

RHEL7S
x86_64
nss-sysinit-3.16.2.3-2.el7_0
nss-softokn-freebl-3.16.2.3-1.el7_0
nss-softokn-debuginfo-3.16.2.3-1.el7_0
nss-softokn-freebl-devel-3.16.2.3-1.el7_0
nss-softokn-devel-3.16.2.3-1.el7_0
nss-3.16.2.3-2.el7_0
nss-util-devel-3.16.2.3-1.el7_0
nss-debuginfo-3.16.2.3-2.el7_0
nss-softokn-3.16.2.3-1.el7_0
nss-util-3.16.2.3-1.el7_0
nss-devel-3.16.2.3-2.el7_0
nss-util-debuginfo-3.16.2.3-1.el7_0
nss-tools-3.16.2.3-2.el7_0

RHEL6S
x86_64
nss-util-devel-3.16.2.3-2.el6_6
nss-3.16.2.3-3.el6_6
nss-sysinit-3.16.2.3-3.el6_6
nss-tools-3.16.2.3-3.el6_6
nss-util-3.16.2.3-2.el6_6
nss-debuginfo-3.16.2.3-3.el6_6
nss-devel-3.16.2.3-3.el6_6
nss-util-debuginfo-3.16.2.3-2.el6_6

i386
nss-util-devel-3.16.2.3-2.el6_6
nss-3.16.2.3-3.el6_6
nss-sysinit-3.16.2.3-3.el6_6
nss-tools-3.16.2.3-3.el6_6
nss-util-3.16.2.3-2.el6_6
nss-debuginfo-3.16.2.3-3.el6_6
nss-devel-3.16.2.3-3.el6_6
nss-util-debuginfo-3.16.2.3-2.el6_6

RHEL7D
x86_64
nss-sysinit-3.16.2.3-2.el7_0
nss-softokn-freebl-3.16.2.3-1.el7_0
nss-softokn-debuginfo-3.16.2.3-1.el7_0
nss-3.16.2.3-2.el7_0
nss-debuginfo-3.16.2.3-2.el7_0
nss-softokn-3.16.2.3-1.el7_0
nss-util-3.16.2.3-1.el7_0
nss-util-debuginfo-3.16.2.3-1.el7_0
nss-tools-3.16.2.3-2.el7_0

RHEL6D
x86_64
nss-util-debuginfo-3.16.2.3-2.el6_6
nss-tools-3.16.2.3-3.el6_6
nss-sysinit-3.16.2.3-3.el6_6
nss-3.16.2.3-3.el6_6
nss-util-3.16.2.3-2.el6_6
nss-debuginfo-3.16.2.3-3.el6_6

i386
nss-util-debuginfo-3.16.2.3-2.el6_6
nss-tools-3.16.2.3-3.el6_6
nss-sysinit-3.16.2.3-3.el6_6
nss-3.16.2.3-3.el6_6
nss-util-3.16.2.3-2.el6_6
nss-debuginfo-3.16.2.3-3.el6_6

RHEL6WS
x86_64
nss-util-devel-3.16.2.3-2.el6_6
nss-3.16.2.3-3.el6_6
nss-sysinit-3.16.2.3-3.el6_6
nss-tools-3.16.2.3-3.el6_6
nss-util-3.16.2.3-2.el6_6
nss-debuginfo-3.16.2.3-3.el6_6
nss-devel-3.16.2.3-3.el6_6
nss-util-debuginfo-3.16.2.3-2.el6_6

i386
nss-util-devel-3.16.2.3-2.el6_6
nss-3.16.2.3-3.el6_6
nss-sysinit-3.16.2.3-3.el6_6
nss-tools-3.16.2.3-3.el6_6
nss-util-3.16.2.3-2.el6_6
nss-debuginfo-3.16.2.3-3.el6_6
nss-devel-3.16.2.3-3.el6_6
nss-util-debuginfo-3.16.2.3-2.el6_6

RHEL7WS
x86_64
nss-sysinit-3.16.2.3-2.el7_0
nss-softokn-freebl-3.16.2.3-1.el7_0
nss-softokn-debuginfo-3.16.2.3-1.el7_0
nss-softokn-freebl-devel-3.16.2.3-1.el7_0
nss-softokn-devel-3.16.2.3-1.el7_0
nss-3.16.2.3-2.el7_0
nss-util-devel-3.16.2.3-1.el7_0
nss-debuginfo-3.16.2.3-2.el7_0

nss-softokn-3.16.2.3-1.el7_0
nss-util-3.16.2.3-1.el7_0
nss-devel-3.16.2.3-2.el7_0
nss-util-debuginfo-3.16.2.3-1.el7_0
nss-tools-3.16.2.3-2.el7_0

188547 - Fedora Linux 20 FEDORA-2014-15706 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3707

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15706

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145016.html

Fedora Core 20

curl-7.32.0-16.fc20

55237 - Top Weekly Malware Env - Trojan-smrss (smrss.exe)

Category: Windows Host Assessment -> Top Weekly Malware
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is infected by the malware:
Env - Trojan-smrss (smrss.exe)

Observation

This malware shows the following behavior:

The files and directories below were created:
%temp%\\smrss.exe

For more information on this malware, visit http://vil.nai.com/vil/default.aspx

130003 - Debian Linux 7.0 DSA-3084-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8104

Description

The scan detected that the host is missing the following update:
DSA-3084-1

Observation

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

http://www.debian.org/security/2014/dsa-3084

Debian 7.0
all
openvpn_2.2.1-8+deb7u3

181295 - FreeBSD OpenVPN Denial Of Service Security Vulnerability (23ab5c3e-79c3-11e4-8b1e-d050992ecde8)

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

Risk Level: Low

CVE: CVE-2014-8104

Description

The scan detected that the host is missing the following update:
OpenVPN -- denial of service security vulnerability (23ab5c3e-79c3-11e4-8b1e-d050992ecde8)

Observation

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

http://www.vuxml.org/freebsd/23ab5c3e-79c3-11e4-8b1e-d050992ecde8.html

Affected packages:
openvpn < 2.0.11
2.1.0 <= openvpn < 2.2.3
2.3.0 <= openvpn < 2.3.6

184625 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2430-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8104

Description

The scan detected that the host is missing the following update:
USN-2430-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002746.html

Ubuntu 14.10

openvpn_2.3.2-9ubuntu1.1

Ubuntu 14.04

openvpn_2.3.2-7ubuntu3.1

Ubuntu 12.04

openvpn_2.2.1-8ubuntu1.4

184626 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2424-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

Description

The scan detected that the host is missing the following update:
USN-2424-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002747.html

Ubuntu 14.10

firefox_34.0+build2-0ubuntu0.14.10.2

Ubuntu 14.04

firefox_34.0+build2-0ubuntu0.14.04.1

Ubuntu 12.04

firefox_34.0+build2-0ubuntu0.12.04.1

188546 - Fedora Linux 19 FEDORA-2014-15477 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1934

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15477

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145070.html

Fedora Core 19

python-eyed3-0.7.4-4.fc19

188548 - Fedora Linux 20 FEDORA-2014-15393 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8990

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15393

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145114.html

Fedora Core 20

lsyncd-2.1.4-4.fc20.1

188549 - Fedora Linux 20 FEDORA-2014-15394 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1693

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15394

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145017.html

Fedora Core 20

erlang-R16B-03.9.fc20

188559 - Fedora Linux 19 FEDORA-2014-15373 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8990

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15373

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145131.html

Fedora Core 19

lsyncd-2.1.4-4.fc19.1

188564 - Fedora Linux 20 FEDORA-2014-15464 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1934

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15464

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145071.html

Fedora Core 20

python-eyed3-0.7.4-4.fc20

184629 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2425-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-7824

Description

The scan detected that the host is missing the following update:
USN-2425-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-November/002742.html

Ubuntu 14.10

libdbus-1-3_1.8.8-1ubuntu2.1
dbus_1.8.8-1ubuntu2.1

Ubuntu 14.04

libdbus-1-3_1.6.18-0ubuntu4.3
dbus_1.6.18-0ubuntu4.3

Ubuntu 12.04

dbus_1.4.18-1ubuntu1.7
libdbus-1-3_1.4.18-1ubuntu1.7

43152 - HP-UX 11.X PHNE_44180 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
PHNE_44180

Observation

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

https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHNE_44180

">patch description

HP-UX 11.23 (800)
HP-UX 11.23 (700)

InternetSrvcs.INETSVCS2-BOOT,fr=B.11.23,fa=HP-UX_B.11.23_PA,v=HP
InternetSrvcs.INETSVCS-INETD,fr=B.11.23,fa=HP-UX_B.11.23_IA/PA,v=HP
InternetSrvcs.INET-ENG-A-MAN,fr=B.11.23,fa=HP-UX_B.11.23_IA/PA,v=HP
InternetSrvcs.INETSVCS2-BOOT,fr=B.11.23,fa=HP-UX_B.11.23_IA,v=HP

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.

16274 - Oracle MySQL Enterprise Monitor Service Manager Remote Code Execution

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

Risk Level: High

CVE: CVE-2013-4316

Update Details

Risk is updated

16694 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXI Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1804

Update Details

Risk is updated

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

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

Risk Level: High

CVE: CVE-2013-4495

Update Details

Risk is updated

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

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

Risk Level: High

CVE: CVE-2013-4495

Update Details

Risk is updated

95681 - SuSE SLES 11, 11 SP3 java-1_6_0-ibm-7920 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-0401, CVE-2013-1491, CVE-2013-1537, CVE-2013-1540, CVE-2013-1557, CVE-2013-1563, CVE-2013-1569, CVE-2013-2383, CVE-2013-2384, CVE-2013-2394, CVE-2013-2417, CVE-2013-2418, CVE-2013-2419, CVE-2013-2420, CVE-2013-2422, CVE-2013-2424, CVE-2013-2429, CVE-2013-2430, CVE-2013-2432, CVE-2013-2433, CVE-2013-2435, CVE-2013-2440

Update Details

Risk is updated

181193 - FreeBSD mozilla Multiple Vulnerabilities (985d4d6c-cfbd-11e3-a003-b4b52fce4ce8)

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

Risk Level: High

CVE: CVE-2014-1492, CVE-2014-1518, CVE-2014-1519, CVE-2014-1520, CVE-2014-1522, CVE-2014-1523, CVE-2014-1524, CVE-2014-1525, CVE-2014-1526, CVE-2014-1527, CVE-2014-1528, CVE-2014-1529, CVE-2014-1530, CVE-2014-1531, CVE-2014-1532

Update Details

Risk is updated

16214 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution I (2916605)

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

Risk Level: High

CVE: CVE-2014-0258

Update Details

Risk is updated

16215 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution II (2916605)

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

Risk Level: High

CVE: CVE-2014-0259

Update Details

Risk is updated

16216 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution III (2916605)

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

Risk Level: High

CVE: CVE-2014-0260

Update Details

Risk is updated

16289 - (MS14-010) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0267

Update Details

Risk is updated

16291 - (MS14-010) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0269

Update Details

Risk is updated

16292 - (MS14-010) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0270

Update Details

Risk is updated

16293 - (MS14-010) Microsoft Internet Explorer VBScript Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0271

Update Details

Risk is updated

16294 - (MS14-010) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0272

Update Details

Risk is updated

16295 - (MS14-010) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0273

Update Details

Risk is updated

16296 - (MS14-010) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0274

Update Details

Risk is updated

16297 - (MS14-010) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0275

Update Details

Risk is updated

16298 - (MS14-010) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0276

Update Details

Risk is updated

16299 - (MS14-010) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0277

Update Details

Risk is updated

16300 - (MS14-010) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0278

Update Details

Risk is updated

16301 - (MS14-010) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0279

Update Details

Risk is updated

16302 - (MS14-010) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0280

Update Details

Risk is updated

16304 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0283

Update Details

Risk is updated

16305 - (MS14-010) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0284

Update Details

Risk is updated

16306 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0285

Update Details

Risk is updated

16307 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0286

Update Details

Risk is updated

16308 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0287

Update Details

Risk is updated

16309 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0288

Update Details

Risk is updated

16310 - (MS14-010) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0289

Update Details

Risk is updated

16311 - (MS14-010) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0290

Update Details

Risk is updated

16484 - (MS14-018) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-0235

Update Details

Risk is updated

16485 - (MS14-018) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-1751

Update Details

Risk is updated

16486 - (MS14-018) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-1752

Update Details

Risk is updated

16487 - (MS14-018) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-1753

Update Details

Risk is updated

16488 - (MS14-018) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-1755

Update Details

Risk is updated

16489 - (MS14-018) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-1760

Update Details

Risk is updated

16493 - (MS14-017) Microsoft Word File Parsing Stack Overflow Remote Code Execution (2949660)

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

Risk Level: High

CVE: CVE-2014-1758

Update Details

Risk is updated

16494 - (MS14-017) Microsoft Word File Format Converter Remote Code Execution (2949660)

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

Risk Level: High

CVE: CVE-2014-1757

Update Details

Risk is updated

16524 - (VMSA-2014-0003) VMware vSphere Client Insecure Download Vulnerability

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

Risk Level: High

CVE: CVE-2014-1209

Update Details

Risk is updated

16609 - (MS14-029) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2962482)

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

Risk Level: High

CVE: CVE-2014-0310

Update Details

Risk is updated

16610 - (MS14-029) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2962482)

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

Risk Level: High

CVE: CVE-2014-1815

Update Details

Risk is updated

16690 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1799

Update Details

Risk is updated

16691 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1800

Update Details

Risk is updated

16692 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXIX Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1802

Update Details

Risk is updated

16693 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXX Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1803

Update Details

Risk is updated

16695 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1805

Update Details

Risk is updated

16696 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXIII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-2753

Update Details

Risk is updated

16760 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1795

Update Details

Risk is updated

16762 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1796

Update Details

Risk is updated

16763 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVI Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1797

Update Details

Risk is updated

16844 - (MS14-038) Microsoft Windows Journal Remote Code Execution (2975689)

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

Risk Level: High

CVE: CVE-2014-1824

Update Details

Risk is updated

17064 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXVI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4111

Update Details

Risk is updated

17065 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4110

Update Details

Risk is updated

17066 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXIV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4109

Update Details

Risk is updated

17067 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXIII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4108

Update Details

Risk is updated

17068 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4107

Update Details

Risk is updated

17069 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4106

Update Details

Risk is updated

17070 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXX Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4105

Update Details

Risk is updated

17071 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIX Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4104

Update Details

Risk is updated

17072 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4103

Update Details

Risk is updated

17073 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4102

Update Details

Risk is updated

17074 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4101

Update Details

Risk is updated

17075 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4100

Update Details

Risk is updated

17076 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4099

Update Details

Risk is updated

17077 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4098

Update Details

Risk is updated

17078 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4097

Update Details

Risk is updated

17079 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4096

Update Details

Risk is updated

17080 - (MS14-052) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4095

Update Details

Risk is updated

17081 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4094

Update Details

Risk is updated

17082 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4093

Update Details

Risk is updated

17083 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4092

Update Details

Risk is updated

17084 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4091

Update Details

Risk is updated

17085 - (MS14-052) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4090

Update Details

Risk is updated

17086 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4089

Update Details

Risk is updated

17087 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4088

Update Details

Risk is updated

17088 - (MS14-052) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4087

Update Details

Risk is updated

17089 - (MS14-052) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4086

Update Details

Risk is updated

17090 - (MS14-052) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4085

Update Details

Risk is updated

17091 - (MS14-052) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4084

Update Details

Risk is updated

17092 - (MS14-052) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4083

Update Details

Risk is updated

17093 - (MS14-052) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4082

Update Details

Risk is updated

17094 - (MS14-052) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4081

Update Details

Risk is updated

17095 - (MS14-052) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4080

Update Details

Risk is updated

17096 - (MS14-052) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4079

Update Details

Risk is updated

17097 - (MS14-052) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4065

Update Details

Risk is updated

17098 - (MS14-052) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4059

Update Details

Risk is updated

17099 - (MS14-052) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-2799

Update Details

Risk is updated

17149 - (MS13-060) Microsoft Windows Unicode Scripts Font Parsing Remote Code Execution (2850869)

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

Risk Level: High

CVE: CVE-2013-3181

Update Details

Risk is updated

17369 - (MS14-067) Microsoft Windows MSXML Core Services Remote Code Execution (2993958)

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

Risk Level: High

CVE: CVE-2014-4118

Update Details

Risk is updated

10615 - Microsoft Data Access Objects Library 3.6 DLL Hijacking Vulnerability (2269637)

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

Risk Level: High

CVE: CVE-2010-4182

Update Details

Observation is updated

181120 - FreeBSD samba Multiple Vulnerabilities (613e45d1-6154-11e3-9b62-000c292e4fd8)

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

Risk Level: High

CVE: CVE-2012-6150, CVE-2013-4408

Update Details

Risk is updated

11430 - Microsoft Malware Protection Engine Privilege Elevation (2491888)

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

Risk Level: High

CVE: CVE-2011-0037

Update Details

FASLScript is updated

15959 - VMware Workstation/Player Shared Library Privilege Escalation

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-5972

Update Details

Risk is updated

16219 - Juniper Junos SRX Flow Daemon IP Packets Denial of Service Vulnerability (CVE-2014-0617)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0617

Update Details

Risk is updated

16230 - Juniper Junos BGP UPDATE Routing Daemon Denial of Service Vulnerability (CVE-2014-0616)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0616

Update Details

Risk is updated

16480 - Schneider Electric OPC Factory Server OPC Automation Server Object ActiveX Control Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2014-0789

Update Details

Risk is updated

16618 - IBM AIX Perl Locale::Maketext Command Execution Vulnerability

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

Risk Level: High

CVE: CVE-2012-6329

Update Details

Risk is updated

16893 - (JSA10635) Juniper Junos NAT Protocol Translation Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3817

Update Details

Risk is updated

16894 - (JSA10637) Juniper Junos RPD PIM Packet Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3819

Update Details

Risk is updated

17186 - Google Chrome Vulnerability Prior To 37.0.2062.124

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

Risk Level: High

CVE: CVE-2014-1568

Update Details

Risk is updated

17187 - Google Chrome Vulnerability Prior To 37.0.2062.124

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1568

Update Details

Risk is updated

17270 - Cisco ASA SQL*NET Inspection Engine Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3382

Update Details

Risk is updated

17271 - Cisco ASA VPN Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2014-3383

Update Details
Risk is updated

17272 - Cisco ASA IKEv2 Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2014-3384

Update Details
Risk is updated

17274 - Cisco ASA HPM ASDM Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2014-3385

Update Details
Risk is updated

17275 - Cisco ASA GTP Inspection Engine Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2014-3386

Update Details
Risk is updated

17276 - Cisco ASA SunRPC Inspection Engine Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High
CVE: CVE-2014-3387

Update Details
Risk is updated

17285 - (JSA10650) Juniper Junos SRX flowd ALG Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High

CVE: CVE-2014-3825

Update Details

Risk is updated

17301 - Cisco ASA DNS Inspection Engine Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-3388

Update Details

Risk is updated

85778 - CentOS 6 CESA-2014-1167 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0205, CVE-2014-3535, CVE-2014-3917, CVE-2014-4667

Update Details

Risk is updated

88627 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2014-220-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3509, CVE-2014-3510, CVE-2014-3511, CVE-2014-3512, CVE-2014-5139

Update Details

Risk is updated

91593 - Oracle Enterprise Linux ELSA-2014-1167 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0205, CVE-2014-3535, CVE-2014-3917, CVE-2014-4667, CVE-2014-4699, CVE-2014-4943

Update Details

Risk is updated

140547 - Red Hat Enterprise Linux RHSA-2014-1167 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0205, CVE-2014-3535, CVE-2014-3917, CVE-2014-4667

Update Details

Risk is updated

142360 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:0977-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4341, CVE-2014-4342, CVE-2014-4343, CVE-2014-4344

Update Details

Risk is updated

142519 - SuSE SLES 10 SP4 firefox31-201411-8991 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1575, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1583, CVE-2014-1585, CVE-2014-1586

Update Details

FASLScript is updated

188408 - Fedora Linux 20 FEDORA-2014-13558 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-3690, CVE-2014-8086

Update Details

Risk is updated

16745 - (MS14-035) Microsoft Internet Explorer Privilege Escalation II (2969262)

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

Risk Level: Medium

CVE: CVE-2014-1778

Update Details

Risk is updated

16759 - (MS14-035) Microsoft Internet Explorer TLS Server Certificate Renegotiation Information Disclosure (2969262)

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

Risk Level: Medium

CVE: CVE-2014-1771

Update Details

Risk is updated

16845 - (MS14-037) Microsoft Internet Explorer Extended Validation Certificate Security Bypass (2975687)

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

Risk Level: Medium

CVE: CVE-2014-2783

Update Details

Risk is updated

16960 - (MS14-043) Microsoft Windows Media Center CSyncBasePlayer Use After Free Remote Code Execution (2978742)

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

Risk Level: Medium

CVE: CVE-2014-4060

Update Details

Risk is updated

17154 - Apache Tomcat Malicious JSP Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2013-4444

Update Details

Risk is updated

17302 - Cisco ASA Software VNMC Command Input Validation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3390

Update Details

Risk is updated

17303 - Cisco ASA Software Untrusted Search Path Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3391

Update Details

Risk is updated

87906 - Fedora Linux 19 FEDORA-2013-12663 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4073

Update Details

Risk is updated

87917 - Fedora Linux 18 FEDORA-2013-12123 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-4073

Update Details
Risk is updated

87922 - Fedora Linux 17 FEDORA-2013-12062 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-4073

Update Details
Risk is updated

91388 - Oracle Enterprise Linux ELSA-2013-1701 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-1775, CVE-2013-2776, CVE-2013-2777

Update Details
Risk is updated

91595 - Oracle Enterprise Linux ELSA-2014-3073 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-0205, CVE-2014-3917

Update Details
Risk is updated

93159 - Mandriva Linux MBS1 MDVSA-2013-201 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-4073

Update Details
Risk is updated

93160 - Mandriva Linux MBS1 MDVSA-2013-198 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-0338, CVE-2013-0339, CVE-2013-2877

Update Details

Risk is updated

93371 - Mandriva Linux MBS1 MDVSA-2014-158 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3509, CVE-2014-3510

Update Details

Risk is updated

95699 - SuSE SLES 10 SP4, SLED 10 SP4 xorg-x11-8623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1981, CVE-2013-1982, CVE-2013-1983, CVE-2013-1984, CVE-2013-1985, CVE-2013-1987, CVE-2013-1988, CVE-2013-1989, CVE-2013-1990, CVE-2013-1991, CVE-2013-1992, CVE-2013-1995, CVE-2013-1996, CVE-2013-1997, CVE-2013-1998, CVE-2013-1999, CVE-2013-2000, CVE-2013-2001, CVE-2013-2002, CVE-2013-2003, CVE-2013-2004, CVE-2013-2005, CVE-2013-2062, CVE-2013-2063, CVE-2013-2066

Update Details

Risk is updated

184091 - Ubuntu Linux 10.04, 12.04, 12.10, 13.04 USN-1904-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0339, CVE-2013-2877

Update Details

Risk is updated

184095 - Ubuntu Linux 10.04, 12.04, 12.10, 13.04 USN-1904-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0339, CVE-2013-2877

Update Details

Risk is updated

2707 - BEA WebLogic File Existence Vulnerability

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

Risk Level: Medium

CVE: CVE-2003-0621, CVE-2003-0622, CVE-2003-0623

Update Details

Risk is updated

3246 - (MS00-063) IIS 4.0 Invalid URL Vulnerability

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

Risk Level: Medium

CVE: CVE-2000-0858

Update Details

Risk is updated

16888 - (SOL15348) F5 BIG-IP OpenSSL DTLS Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2009-1387

Update Details

Risk is updated

17281 - SSLv3 Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3566

Update Details

Recommendation is updated

58658 - Debian Linux 6.0, 7.0 DSA-2734-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4930, CVE-2013-4932, CVE-2013-4933, CVE-2013-4934, CVE-2013-4935

Update Details

Risk is updated

58957 - Debian Linux 7.0 DSA-3038-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-0179, CVE-2014-3633

Update Details

Risk is updated

87910 - Fedora Linux 18 FEDORA-2013-12541 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4114

Update Details

Risk is updated

87918 - Fedora Linux 19 FEDORA-2013-12526 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4114

Update Details

Risk is updated

87944 - Fedora Linux 19 FEDORA-2013-10467 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2014, CVE-2013-2157

Update Details

Risk is updated

88535 - Slackware Linux 13.1, 13.37, 14.0 SSA:2013-218-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4124

Update Details

Risk is updated

93157 - Mandriva Linux MES5 MDVSA-2013-197 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1861, CVE-2013-3802, CVE-2013-3804

Update Details

Risk is updated

93165 - Mandriva Linux MBS1, MES5 MDVSA-2013-207 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4124

Update Details

Risk is updated

95677 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 gnutls-7918 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2013-2116

Update Details
Risk is updated

95689 - SuSE SLES 10 SP4, SLED 10 SP4 krb5-8631 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2002-2443

Update Details
Risk is updated

95695 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 krb5-7962 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2002-2443

Update Details
Risk is updated

95696 - SuSE SLES 11, 11 SP2, SLED 11, 11 SP2 krb5-7968 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2002-2443

Update Details
Risk is updated

181056 - FreeBSD PHP5 Integer Overflow In Calendar Module (5def3175-f3f9-4476-ba40-b46627cc638c)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-4635

Update Details
Risk is updated

184092 - Ubuntu Linux 12.10, 13.04 USN-1906-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-4668

Update Details
Risk is updated

184099 - Ubuntu Linux 10.04, 12.04, 12.10, 13.04 USN-1909-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1861, CVE-2013-2162, CVE-2013-3783, CVE-2013-3793, CVE-2013-3802, CVE-2013-3804, CVE-2013-3809, CVE-2013-3812

Update Details

Risk is updated

17032 - BlackBerry Enterprise Server Credentials Logging Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-1469

Update Details

Risk is updated

87895 - Fedora Linux 18 FEDORA-2013-11646 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2209

Update Details

Risk is updated

87900 - Fedora Linux 19 FEDORA-2013-11682 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2209

Update Details

Risk is updated

87931 - Fedora Linux 19 FEDORA-2013-12901 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2232

Update Details

Risk is updated

87932 - Fedora Linux 18 FEDORA-2013-12950 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2242, CVE-2013-2243, CVE-2013-2244, CVE-2013-2245, CVE-2013-2246

Update Details

Risk is updated

87949 - Fedora Linux 19 FEDORA-2013-12964 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2242, CVE-2013-2243, CVE-2013-2244, CVE-2013-2245, CVE-2013-2246

Update Details

Risk is updated

87955 - Fedora Linux 17 FEDORA-2013-13252 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2242, CVE-2013-2243, CVE-2013-2244, CVE-2013-2245, CVE-2013-2246

Update Details

Risk is updated

87958 - Fedora Linux 18 FEDORA-2013-13234 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4136

Update Details

Risk is updated

87969 - Fedora Linux 19 FEDORA-2013-13297 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4136

Update Details

Risk is updated

87971 - Fedora Linux 17 FEDORA-2013-13231 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4136

Update Details

Risk is updated

87982 - Fedora Linux 19 FEDORA-2013-13696 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-4131

Update Details
Risk is updated

93155 - Mandriva Linux MBS1, MES5 MDVSA-2013-193 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-1896

Update Details
Risk is updated

93166 - Mandriva Linux MBS1 MDVSA-2013-209 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-4131

Update Details
Risk is updated

95727 - SuSE SLES 10 SP4 strongswan-8546 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-2944

Update Details
Risk is updated

95741 - SuSE SLES 11, 11 SP2, SLED 11, 11 SP2 strongswan-7638 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-2944

Update Details
Risk is updated

95743 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 strongswan-8021 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-2944

Update Details

Risk is updated

181061 - FreeBSD subversion Remotely Triggerable "Assertion Failed" DoS Vulnerability Or Read Overflow. (2ae24334-f2e6-11e2-8346-001e8c75

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

Risk Level: Medium

CVE: CVE-2013-4131

Update Details

Risk is updated

181064 - FreeBSD wordpress Multiple Vulnerabilities (049332d2-f6e1-11e2-82f3-000c29ee3065)

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

Risk Level: Medium

CVE: CVE-2013-2199, CVE-2013-2200, CVE-2013-2201, CVE-2013-2202, CVE-2013-2203, CVE-2013-2204, CVE-2013-2205

Update Details

Risk is updated

181066 - FreeBSD typo3 Multiple Vulnerabilities In TYPO3 Core (e6839625-fdfa-11e2-9430-20cf30e32f6d)

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

Risk Level: Medium

CVE: CVE-2011-3642, CVE-2013-1464

Update Details

Risk is updated

184084 - Ubuntu Linux 12.04 USN-1901-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-0037

Update Details

Risk is updated

DELETED CHECKS

43113 - HP-UX 11.X PHNE_43602 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

ADDITIONAL NOTES

- **43113** - was 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.