2014-NOV-20
FSL version 7.5.649

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

140612 - Red Hat Enterprise Linux RHSA-2014-1852 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0573, CVE-2014-0574, CVE-2014-0576, CVE-2014-0577, CVE-2014-0581, CVE-2014-0582, CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, CVE-2014-0588, CVE-2014-0589, CVE-2014-0590, CVE-2014-8437, CVE-2014-8438, CVE-2014-8440, CVE-2014-8441

Description

The scan detected that the host is missing the following update:
RHSA-2014-1852

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1852.html

RHEL5D
x86_64
flash-plugin-11.2.202.418-1.el5

i386
flash-plugin-11.2.202.418-1.el5

RHEL5S
x86_64
flash-plugin-11.2.202.418-1.el5

i386
flash-plugin-11.2.202.418-1.el5

RHEL6D
x86_64
flash-plugin-11.2.202.418-1.el6

RHEL6S
x86_64
flash-plugin-11.2.202.418-1.el6

i386
flash-plugin-11.2.202.418-1.el6

RHEL6WS
x86_64
flash-plugin-11.2.202.418-1.el6

i386
flash-plugin-11.2.202.418-1.el6

142504 - SuSE SLED 11 SP3 flash-player-9958 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0573, CVE-2014-0574, CVE-2014-0576, CVE-2014-0577, CVE-2014-0581, CVE-2014-0582, CVE-2014-0583, CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, CVE-2014-0588, CVE-2014-0589, CVE-2014-0590, CVE-2014-8437, CVE-2014-8438, CVE-2014-8440, CVE-2014-8441, CVE-2014-8442

Description

The scan detected that the host is missing the following update:
flash-player-9958

Observation

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

https://download.suse.com/Download?buildid=RJxSkx10gvE~
https://download.suse.com/Download?buildid=NtRCO6gWGsw~

SuSE SLED 11 SP3
x86_64
flash-player-11.2.202.418-0.3.1
flash-player-kde4-11.2.202.418-0.3.1
flash-player-gnome-11.2.202.418-0.3.1

i586
flash-player-11.2.202.418-0.3.1
flash-player-kde4-11.2.202.418-0.3.1
flash-player-gnome-11.2.202.418-0.3.1

142511 - SuSE SLED 11 SP3 java-1_7_0-openjdk-9906 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4288, CVE-2014-6456, CVE-2014-6457, CVE-2014-6458, CVE-2014-6466, CVE-2014-6468, CVE-2014-6476, CVE-2014-6485, CVE-2014-6492, CVE-2014-6493, CVE-2014-6502, CVE-2014-6503, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6513, CVE-2014-6515, CVE-2014-6517, CVE-2014-6519, CVE-2014-6527, CVE-2014-6531, CVE-2014-6532, CVE-2014-6558, CVE-2014-6562

Description

The scan detected that the host is missing the following update:
java-1_7_0-openjdk-9906

Observation

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

https://download.suse.com/Download?buildid=nxSzWgaj9gk~
https://download.suse.com/Download?buildid=tjs8m3ZO-Nw~

SuSE SLED 11 SP3
x86_64

java-1_7_0-openjdk-demo-1.7.0.71-0.7.1
java-1_7_0-openjdk-devel-1.7.0.71-0.7.1
java-1_7_0-openjdk-1.7.0.71-0.7.1

i586
java-1_7_0-openjdk-demo-1.7.0.71-0.7.1
java-1_7_0-openjdk-devel-1.7.0.71-0.7.1
java-1_7_0-openjdk-1.7.0.71-0.7.1

181287 - FreeBSD chromium Multiple Vulnerabilities (d395e44f-6f4f-11e4-a444-00262d5ed8ee)

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

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

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (d395e44f-6f4f-11e4-a444-00262d5ed8ee)

Observation

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

http://www.vuxml.org/freebsd/d395e44f-6f4f-11e4-a444-00262d5ed8ee.html

Affected packages:
chromium < 39.0.2171.65
chromium-pulse < 39.0.2171.65

17253 - (JSA10652) Juniper Junos Malformed RSVP Packet Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6378

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in RSVP packet management. Successful exploitation could allow an attacker to cause a denial of service condition.

17294 - Mozilla Firefox Multiple Vulnerabilities Prior To 33

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1575, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1580, CVE-2014-1581, CVE-2014-1582, CVE-2014-1583, CVE-2014-1584, CVE-2014-1585, CVE-2014-1586

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

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

17295 - Mozilla Firefox Multiple Vulnerabilities Prior To 33

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1575, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1580, CVE-2014-1581, CVE-2014-1582, CVE-2014-1583, CVE-2014-1584, CVE-2014-1585, CVE-2014-1586

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

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

17296 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 31.2

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1583, CVE-2014-1585, CVE-2014-1586

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is an open source web browser.

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

17297 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 31.2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1583, CVE-2014-1585, CVE-2014-1586

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is an open source web browser.

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

17332 - (HT6493) Apple QuickTime Multiple Vulnerabilities Prior To 7.7.6

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

Risk Level: High

CVE: CVE-2014-1391, CVE-2014-4350, CVE-2014-4351, CVE-2014-4979

Description

Multiple vulnerabilities are present in some versions of Apple QuickTime Player.

Observation

Apple QuickTime is a popular media player.

Multiple vulnerabilities are present in some versions of Apple QuickTime Player. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code on the affected system.

17431 - Rockwell Automation CCW ActiveX Component Remote Code Execution

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

Risk Level: High

CVE: CVE-2014-5424

Description

A vulnerability in some versions of Rockwell Automation Connected Components Workbench could lead to remote code execution.

Observation

A vulnerability in some versions of Rockwell Automation Connected Components Workbench could lead to remote code execution.

The flaw lies in multiple ActiveX components. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

17432 - (HPSBMU03127) HP Operations Manager Remote Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-2649

Description

A remote code execution vulnerability is present in some versions of HP Operations Manager.

Observation

HP Operations Manager is a package management software.

A remote code execution vulnerability is present in some versions of HP Operations Manager. The flaw is due to an unspecified defect. Successful exploitation could allow attackers to execute arbitrary code.

17435 - Symantec Endpoint Protection Manager XML External Entity Injection Information Disclosure

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

Risk Level: High

CVE: CVE-2014-3437

Description

A vulnerability in some versions of Symantec Endpoint Protection Manager could lead to an information disclosure.

Observation

A vulnerability in some versions of Symantec Endpoint Protection Manager could lead to an information disclosure.

The flaw occurs as the management console does not properly validate incoming XML data. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

142501 - SuSE SLES 10 SP4 wget-8985 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
wget-8985

Observation

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

https://download.suse.com/Download?buildid=zcOnTnlZbJE~
https://download.suse.com/Download?buildid=z8hDcC2XkkM~
https://download.suse.com/Download?buildid=uVeQWnULBRc~

SuSE SLES 10 SP4
x86_64
wget-1.10.2-15.14.5

i586
wget-1.10.2-15.14.5

142514 - SuSE SLES 11 SP2 wget-9939 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
wget-9939

Observation

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

https://download.suse.com/Download?buildid=t6hzPtCcoqo~

https://download.suse.com/Download?buildid=FyraF5oXT_Y~
https://download.suse.com/Download?buildid=liIO7uM4Tqk~

SuSE SLES 11 SP2
x86_64
wget-1.11.4-1.19.1

i586
wget-1.11.4-1.19.1

177990 - Gentoo Linux GLSA-201411-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
GLSA-201411-05

Observation

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

http://security.gentoo.org/glsa/glsa-201411-05.xml

Affected packages:
net-misc/wget < 1.16

17266 - (JSA10655) Juniper Junos Crafted Fragmented Packets Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6380

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw occurs due to improper fragmented packets handling. Successful exploitation could allow an attacker to cause FPCs resetting or going offline.

85824 - CentOS 7 CESA-2014-1861 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-5615, CVE-2014-2494, CVE-2014-4207, CVE-2014-4243, CVE-2014-4258, CVE-2014-4260, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559

Description

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

CESA-2014-1861

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020761.html

CentOS 7
x86_64
mariadb-bench-5.5.40-1.el7_0
mariadb-embedded-devel-5.5.40-1.el7_0
mariadb-embedded-5.5.40-1.el7_0
mariadb-5.5.40-1.el7_0
mariadb-libs-5.5.40-1.el7_0
mariadb-devel-5.5.40-1.el7_0
mariadb-test-5.5.40-1.el7_0
mariadb-server-5.5.40-1.el7_0

i686
mariadb-embedded-devel-5.5.40-1.el7_0
mariadb-devel-5.5.40-1.el7_0
mariadb-libs-5.5.40-1.el7_0
mariadb-embedded-5.5.40-1.el7_0

85826 - CentOS 5 CESA-2014-1859 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-5615, CVE-2014-2494, CVE-2014-4207, CVE-2014-4243, CVE-2014-4258, CVE-2014-4260, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
CESA-2014-1859

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020762.html

CentOS 5
x86_64
mysql55-mysql-server-5.5.40-2.el5
mysql55-mysql-test-5.5.40-2.el5
mysql55-mysql-libs-5.5.40-2.el5
mysql55-mysql-devel-5.5.40-2.el5
mysql55-mysql-5.5.40-2.el5
mysql55-mysql-bench-5.5.40-2.el5

i386
mysql55-mysql-server-5.5.40-2.el5
mysql55-mysql-test-5.5.40-2.el5
mysql55-mysql-libs-5.5.40-2.el5
mysql55-mysql-devel-5.5.40-2.el5

mysql55-mysql-5.5.40-2.el5
mysql55-mysql-bench-5.5.40-2.el5

140608 - Red Hat Enterprise Linux RHSA-2014-1861 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2494, CVE-2014-4207, CVE-2014-4243, CVE-2014-4258, CVE-2014-4260, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
RHSA-2014-1861

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1861.html

RHEL7WS
x86_64
mariadb-test-5.5.40-1.el7_0
mariadb-devel-5.5.40-1.el7_0
mariadb-debuginfo-5.5.40-1.el7_0
mariadb-server-5.5.40-1.el7_0
mariadb-bench-5.5.40-1.el7_0
mariadb-libs-5.5.40-1.el7_0
mariadb-5.5.40-1.el7_0

RHEL7D
x86_64
mariadb-server-5.5.40-1.el7_0
mariadb-debuginfo-5.5.40-1.el7_0
mariadb-libs-5.5.40-1.el7_0
mariadb-5.5.40-1.el7_0

RHEL7S
x86_64
mariadb-test-5.5.40-1.el7_0
mariadb-devel-5.5.40-1.el7_0
mariadb-debuginfo-5.5.40-1.el7_0
mariadb-server-5.5.40-1.el7_0
mariadb-bench-5.5.40-1.el7_0
mariadb-libs-5.5.40-1.el7_0
mariadb-5.5.40-1.el7_0

140611 - Red Hat Enterprise Linux RHSA-2014-1862 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2494, CVE-2014-4207, CVE-2014-4243, CVE-2014-4258, CVE-2014-4260, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
RHSA-2014-1862

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1862.html

RHEL7WS
x86_64
mariadb55-mariadb-bench-5.5.40-10.el7
mariadb55-mariadb-server-5.5.40-10.el7
mariadb55-mariadb-debuginfo-5.5.40-10.el7
mariadb55-mariadb-5.5.40-10.el7
mariadb55-mariadb-devel-5.5.40-10.el7
mariadb55-mariadb-test-5.5.40-10.el7
mariadb55-mariadb-libs-5.5.40-10.el7

RHEL7S
x86_64
mariadb55-mariadb-bench-5.5.40-10.el7
mariadb55-mariadb-server-5.5.40-10.el7
mariadb55-mariadb-debuginfo-5.5.40-10.el7
mariadb55-mariadb-5.5.40-10.el7
mariadb55-mariadb-devel-5.5.40-10.el7
mariadb55-mariadb-test-5.5.40-10.el7
mariadb55-mariadb-libs-5.5.40-10.el7

RHEL6S
x86_64
mariadb55-mariadb-test-5.5.40-10.el6
mariadb55-mariadb-server-5.5.40-10.el6
mariadb55-mariadb-bench-5.5.40-10.el6
mariadb55-mariadb-libs-5.5.40-10.el6
mariadb55-mariadb-debuginfo-5.5.40-10.el6
mariadb55-mariadb-5.5.40-10.el6
mariadb55-mariadb-devel-5.5.40-10.el6

RHEL6WS
x86_64
mariadb55-mariadb-test-5.5.40-10.el6
mariadb55-mariadb-server-5.5.40-10.el6
mariadb55-mariadb-bench-5.5.40-10.el6
mariadb55-mariadb-libs-5.5.40-10.el6
mariadb55-mariadb-debuginfo-5.5.40-10.el6
mariadb55-mariadb-5.5.40-10.el6
mariadb55-mariadb-devel-5.5.40-10.el6

140614 - Red Hat Enterprise Linux RHSA-2014-1860 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2494, CVE-2014-4207, CVE-2014-4243, CVE-2014-4258, CVE-2014-4260, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
RHSA-2014-1860

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1860.html

RHEL7WS
x86_64
mysql55-mysql-libs-5.5.40-1.el7
mysql55-mysql-devel-5.5.40-1.el7
mysql55-mysql-server-5.5.40-1.el7
mysql55-mysql-debuginfo-5.5.40-1.el7
mysql55-mysql-test-5.5.40-1.el7
mysql55-mysql-5.5.40-1.el7
mysql55-mysql-bench-5.5.40-1.el7

RHEL7S
x86_64
mysql55-mysql-libs-5.5.40-1.el7
mysql55-mysql-devel-5.5.40-1.el7
mysql55-mysql-server-5.5.40-1.el7
mysql55-mysql-debuginfo-5.5.40-1.el7
mysql55-mysql-test-5.5.40-1.el7
mysql55-mysql-5.5.40-1.el7
mysql55-mysql-bench-5.5.40-1.el7

RHEL6S
x86_64
mysql55-mysql-server-5.5.40-1.el6
mysql55-mysql-devel-5.5.40-1.el6
mysql55-mysql-test-5.5.40-1.el6
mysql55-mysql-bench-5.5.40-1.el6
mysql55-mysql-debuginfo-5.5.40-1.el6
mysql55-mysql-libs-5.5.40-1.el6
mysql55-mysql-5.5.40-1.el6

RHEL6WS
x86_64
mysql55-mysql-server-5.5.40-1.el6
mysql55-mysql-devel-5.5.40-1.el6
mysql55-mysql-test-5.5.40-1.el6
mysql55-mysql-bench-5.5.40-1.el6
mysql55-mysql-debuginfo-5.5.40-1.el6
mysql55-mysql-libs-5.5.40-1.el6
mysql55-mysql-5.5.40-1.el6

140615 - Red Hat Enterprise Linux RHSA-2014-1859 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2494, CVE-2014-4207, CVE-2014-4243, CVE-2014-4258, CVE-2014-4260, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
RHSA-2014-1859

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1859.html

RHEL5D
x86_64
mysql55-mysql-debuginfo-5.5.40-2.el5
mysql55-mysql-server-5.5.40-2.el5
mysql55-mysql-test-5.5.40-2.el5
mysql55-mysql-libs-5.5.40-2.el5
mysql55-mysql-5.5.40-2.el5
mysql55-mysql-bench-5.5.40-2.el5

i386
mysql55-mysql-debuginfo-5.5.40-2.el5
mysql55-mysql-server-5.5.40-2.el5
mysql55-mysql-test-5.5.40-2.el5
mysql55-mysql-libs-5.5.40-2.el5
mysql55-mysql-5.5.40-2.el5
mysql55-mysql-bench-5.5.40-2.el5

RHEL5S
x86_64
mysql55-mysql-debuginfo-5.5.40-2.el5
mysql55-mysql-server-5.5.40-2.el5
mysql55-mysql-test-5.5.40-2.el5
mysql55-mysql-libs-5.5.40-2.el5
mysql55-mysql-devel-5.5.40-2.el5
mysql55-mysql-5.5.40-2.el5
mysql55-mysql-bench-5.5.40-2.el5

i386
mysql55-mysql-debuginfo-5.5.40-2.el5
mysql55-mysql-server-5.5.40-2.el5
mysql55-mysql-test-5.5.40-2.el5
mysql55-mysql-libs-5.5.40-2.el5
mysql55-mysql-devel-5.5.40-2.el5
mysql55-mysql-5.5.40-2.el5
mysql55-mysql-bench-5.5.40-2.el5

170424 - Amazon Linux AMI ALAS-2014-443 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1418, CVE-2013-6800, CVE-2014-4341, CVE-2014-4342, CVE-2014-4343, CVE-2014-4344, CVE-2014-4345

Description

The scan detected that the host is missing the following update:
ALAS-2014-443

Observation

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

For more information see:

https://alas.aws.amazon.com/ALAS-2014-443.html

Amazon Linux AMI
x86_64
krb5-debuginfo-1.10.3-33.28.amzn1
krb5-pkinit-openssl-1.10.3-33.28.amzn1
krb5-workstation-1.10.3-33.28.amzn1
krb5-libs-1.10.3-33.28.amzn1
krb5-server-ldap-1.10.3-33.28.amzn1
krb5-devel-1.10.3-33.28.amzn1
krb5-server-1.10.3-33.28.amzn1

i686
krb5-debuginfo-1.10.3-33.28.amzn1
krb5-workstation-1.10.3-33.28.amzn1
krb5-devel-1.10.3-33.28.amzn1
krb5-libs-1.10.3-33.28.amzn1
krb5-pkinit-openssl-1.10.3-33.28.amzn1
krb5-server-ldap-1.10.3-33.28.amzn1
krb5-server-1.10.3-33.28.amzn1

174593 - Scientific Linux Security ERRATA Important: mysql55-mysql on SL5.x i386/x86_64 (1411-3069)

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

Risk Level: High

CVE: CVE-2014-2494, CVE-2014-4207, CVE-2014-4243, CVE-2014-4258, CVE-2014-4260, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: mysql55-mysql on SL5.x i386/x86_64 (1411-3069)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=3069

SL5
x86_64
mysql55-mysql-debuginfo-5.5.40-2.el5
mysql55-mysql-devel-5.5.40-2.el5
mysql55-mysql-server-5.5.40-2.el5
mysql55-mysql-test-5.5.40-2.el5
mysql55-mysql-libs-5.5.40-2.el5
mysql55-mysql-5.5.40-2.el5
mysql55-mysql-bench-5.5.40-2.el5

i386
mysql55-mysql-debuginfo-5.5.40-2.el5
mysql55-mysql-devel-5.5.40-2.el5
mysql55-mysql-server-5.5.40-2.el5
mysql55-mysql-test-5.5.40-2.el5
mysql55-mysql-libs-5.5.40-2.el5
mysql55-mysql-5.5.40-2.el5

mysql55-mysql-bench-5.5.40-2.el5

174595 - Scientific Linux Security ERRATA Important: mariadb on SL7.x x86_64 (1411-3203)

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

Risk Level: High

CVE: CVE-2014-2494, CVE-2014-4207, CVE-2014-4243, CVE-2014-4258, CVE-2014-4260, CVE-2014-4274, CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: mariadb on SL7.x x86_64 (1411-3203)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=3203

SL7
x86_64
mariadb-bench-5.5.40-1.el7_0
mariadb-embedded-devel-5.5.40-1.el7_0
mariadb-embedded-5.5.40-1.el7_0
mariadb-5.5.40-1.el7_0
mariadb-debuginfo-5.5.40-1.el7_0
mariadb-libs-5.5.40-1.el7_0
mariadb-devel-5.5.40-1.el7_0
mariadb-test-5.5.40-1.el7_0
mariadb-server-5.5.40-1.el7_0

17289 - Oracle WebLogic Server Critical Patch Update October 2014

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

Risk Level: High

CVE: CVE-2014-0114, CVE-2014-6534

Description

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

Observation

Oracle WebLogic Server is a Java application server.

Multiple vulnerabilities are present in some versions of Oracle WebLogic Server. The flaws lie in WLS-Console. Successful exploitation could allow an attacker to execute arbitrary code.

85828 - CentOS 6, 7 CESA-2014-1870 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0209, CVE-2014-0210, CVE-2014-0211

Description

The scan detected that the host is missing the following update:
CESA-2014-1870

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020769.html
http://lists.centos.org/pipermail/centos-announce/2014-November/020768.html

CentOS 7
x86_64
libXfont-1.4.7-2.el7_0
libXfont-devel-1.4.7-2.el7_0

i686
libXfont-1.4.7-2.el7_0
libXfont-devel-1.4.7-2.el7_0

CentOS 6
x86_64
libXfont-1.4.5-4.el6_6
libXfont-devel-1.4.5-4.el6_6

i686
libXfont-1.4.5-4.el6_6
libXfont-devel-1.4.5-4.el6_6

91661 - Oracle Enterprise Linux ELSA-2014-3088 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687

Description

The scan detected that the host is missing the following update:
ELSA-2014-3088

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/004637.html
http://oss.oracle.com/pipermail/el-errata/2014-November/004636.html

OEL6
x86_64
kernel-uek-devel-2.6.39-400.215.13.el6uek
kernel-uek-2.6.39-400.215.13.el6uek
kernel-uek-debug-2.6.39-400.215.13.el6uek
kernel-uek-firmware-2.6.39-400.215.13.el6uek
kernel-uek-doc-2.6.39-400.215.13.el6uek
kernel-uek-debug-devel-2.6.39-400.215.13.el6uek

i386
kernel-uek-debug-devel-2.6.39-400.215.13.el6uek

kernel-uek-2.6.39-400.215.13.el6uek
kernel-uek-debug-2.6.39-400.215.13.el6uek
kernel-uek-firmware-2.6.39-400.215.13.el6uek
kernel-uek-devel-2.6.39-400.215.13.el6uek
kernel-uek-doc-2.6.39-400.215.13.el6uek

OEL5
x86_64
kernel-uek-firmware-2.6.39-400.215.13.el5uek
kernel-uek-2.6.39-400.215.13.el5uek
kernel-uek-doc-2.6.39-400.215.13.el5uek
kernel-uek-debug-devel-2.6.39-400.215.13.el5uek
kernel-uek-debug-2.6.39-400.215.13.el5uek
kernel-uek-devel-2.6.39-400.215.13.el5uek

i386
kernel-uek-debug-devel-2.6.39-400.215.13.el5uek
kernel-uek-firmware-2.6.39-400.215.13.el5uek
kernel-uek-2.6.39-400.215.13.el5uek
kernel-uek-debug-2.6.39-400.215.13.el5uek
kernel-uek-devel-2.6.39-400.215.13.el5uek
kernel-uek-doc-2.6.39-400.215.13.el5uek

91663 - Oracle Enterprise Linux ELSA-2014-3089 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687

Description

The scan detected that the host is missing the following update:
ELSA-2014-3089

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/004644.html
http://oss.oracle.com/pipermail/el-errata/2014-November/004645.html

OEL6
x86_64
kernel-uek-firmware-2.6.32-400.36.11.el6uek
kernel-uek-doc-2.6.32-400.36.11.el6uek
mlnx_en-2.6.32-400.36.11.el6uek-1.5.7-0.1
kernel-uek-2.6.32-400.36.11.el6uek
kernel-uek-debug-devel-2.6.32-400.36.11.el6uek
kernel-uek-headers-2.6.32-400.36.11.el6uek
ofa-2.6.32-400.36.11.el6uekdebug-1.5.1-4.0.58
kernel-uek-debug-2.6.32-400.36.11.el6uek
kernel-uek-devel-2.6.32-400.36.11.el6uek
ofa-2.6.32-400.36.11.el6uek-1.5.1-4.0.58
mlnx_en-2.6.32-400.36.11.el6uekdebug-1.5.7-0.1

i386
kernel-uek-firmware-2.6.32-400.36.11.el6uek
kernel-uek-doc-2.6.32-400.36.11.el6uek
mlnx_en-2.6.32-400.36.11.el6uek-1.5.7-0.1

kernel-uek-2.6.32-400.36.11.el6uek
kernel-uek-debug-devel-2.6.32-400.36.11.el6uek
kernel-uek-headers-2.6.32-400.36.11.el6uek
ofa-2.6.32-400.36.11.el6uekdebug-1.5.1-4.0.58
kernel-uek-debug-2.6.32-400.36.11.el6uek
kernel-uek-devel-2.6.32-400.36.11.el6uek
ofa-2.6.32-400.36.11.el6uek-1.5.1-4.0.58
mlnx_en-2.6.32-400.36.11.el6uekdebug-1.5.7-0.1

OEL5
x86_64
mlnx_en-2.6.32-400.36.11.el5uek-1.5.7-2
kernel-uek-doc-2.6.32-400.36.11.el5uek
ofa-2.6.32-400.36.11.el5uek-1.5.1-4.0.58
kernel-uek-firmware-2.6.32-400.36.11.el5uek
kernel-uek-devel-2.6.32-400.36.11.el5uek
kernel-uek-headers-2.6.32-400.36.11.el5uek
mlnx_en-2.6.32-400.36.11.el5uekdebug-1.5.7-2
kernel-uek-debug-2.6.32-400.36.11.el5uek
kernel-uek-2.6.32-400.36.11.el5uek
ofa-2.6.32-400.36.11.el5uekdebug-1.5.1-4.0.58
kernel-uek-debug-devel-2.6.32-400.36.11.el5uek

i386
mlnx_en-2.6.32-400.36.11.el5uek-1.5.7-2
kernel-uek-doc-2.6.32-400.36.11.el5uek
ofa-2.6.32-400.36.11.el5uek-1.5.1-4.0.58
kernel-uek-firmware-2.6.32-400.36.11.el5uek
kernel-uek-devel-2.6.32-400.36.11.el5uek
kernel-uek-headers-2.6.32-400.36.11.el5uek
mlnx_en-2.6.32-400.36.11.el5uekdebug-1.5.7-2
kernel-uek-debug-2.6.32-400.36.11.el5uek
kernel-uek-2.6.32-400.36.11.el5uek
ofa-2.6.32-400.36.11.el5uekdebug-1.5.1-4.0.58
kernel-uek-debug-devel-2.6.32-400.36.11.el5uek

91664 - Oracle Enterprise Linux ELSA-2014-3087 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687

Description

The scan detected that the host is missing the following update:
ELSA-2014-3087

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/004634.html
http://oss.oracle.com/pipermail/el-errata/2014-November/004635.html

OEL6
x86_64
kernel-uek-firmware-3.8.13-44.1.5.el6uek
kernel-uek-doc-3.8.13-44.1.5.el6uek
kernel-uek-debug-devel-3.8.13-44.1.5.el6uek

kernel-uek-devel-3.8.13-44.1.5.el6uek
dtrace-modules-3.8.13-44.1.5.el6uek-0.4.3-4.el6
kernel-uek-3.8.13-44.1.5.el6uek
kernel-uek-debug-3.8.13-44.1.5.el6uek

OEL7

140613 - Red Hat Enterprise Linux RHSA-2014-1870 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0209, CVE-2014-0210, CVE-2014-0211

Description

The scan detected that the host is missing the following update:
RHSA-2014-1870

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1870.html

RHEL7WS
x86_64
libXfont-1.4.7-2.el7_0
libXfont-debuginfo-1.4.7-2.el7_0

RHEL7D
x86_64
libXfont-1.4.7-2.el7_0
libXfont-debuginfo-1.4.7-2.el7_0

RHEL6D
x86_64
libXfont-1.4.5-4.el6_6
libXfont-debuginfo-1.4.5-4.el6_6

i386
libXfont-1.4.5-4.el6_6
libXfont-debuginfo-1.4.5-4.el6_6

RHEL6S
x86_64
libXfont-1.4.5-4.el6_6
libXfont-debuginfo-1.4.5-4.el6_6

i386
libXfont-1.4.5-4.el6_6
libXfont-debuginfo-1.4.5-4.el6_6

RHEL7S
x86_64
libXfont-1.4.7-2.el7_0
libXfont-debuginfo-1.4.7-2.el7_0

RHEL6WS
x86_64

libXfont-1.4.5-4.el6_6
libXfont-debuginfo-1.4.5-4.el6_6

i386
libXfont-1.4.5-4.el6_6
libXfont-debuginfo-1.4.5-4.el6_6

142500 - SuSE Linux 13.2 openSUSE-SU-2014:1443-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3693

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1443-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00070.html

SuSE Linux 13.2
i586
libreoffice-base-4.3.3.2-4.1
libreoffice-kde4-debuginfo-4.3.3.2-4.1
libreoffice-l10n-da-4.3.3.2-4.1
libreoffice-l10n-es-4.3.3.2-4.1
libreoffice-pyuno-4.3.3.2-4.1
libreoffice-l10n-ga-4.3.3.2-4.1
libreoffice-mailmerge-4.3.3.2-4.1
libreoffice-l10n-sl-4.3.3.2-4.1
libreoffice-l10n-eu-4.3.3.2-4.1
libreoffice-l10n-zu-4.3.3.2-4.1
libreoffice-l10n-fa-4.3.3.2-4.1
libreoffice-l10n-bg-4.3.3.2-4.1
libreoffice-l10n-pt-BR-4.3.3.2-4.1
libreoffice-math-4.3.3.2-4.1
libreoffice-l10n-ss-4.3.3.2-4.1
libreoffice-officebean-4.3.3.2-4.1
libreoffice-l10n-st-4.3.3.2-4.1
libreoffice-l10n-ve-4.3.3.2-4.1
libreoffice-l10n-nl-4.3.3.2-4.1
libreoffice-base-debuginfo-4.3.3.2-4.1
libreoffice-l10n-ja-4.3.3.2-4.1
libreoffice-l10n-sr-4.3.3.2-4.1
libreoffice-base-drivers-mysql-4.3.3.2-4.1
libreoffice-l10n-fr-4.3.3.2-4.1
libreoffice-4.3.3.2-4.1
libreoffice-base-drivers-postgresql-4.3.3.2-4.1
libreoffice-l10n-hu-4.3.3.2-4.1
libreoffice-debugsource-4.3.3.2-4.1
libreoffice-l10n-sk-4.3.3.2-4.1
libreoffice-gnome-debuginfo-4.3.3.2-4.1
libreoffice-l10n-fi-4.3.3.2-4.1
libreoffice-l10n-mai-4.3.3.2-4.1
libreoffice-l10n-ts-4.3.3.2-4.1

libreoffice-icon-theme-galaxy-4.3.3.2-4.1
libreoffice-l10n-as-4.3.3.2-4.1
libreoffice-writer-extensions-4.3.3.2-4.1
libreoffice-sdk-doc-4.3.3.2-4.1
libreoffice-draw-debuginfo-4.3.3.2-4.1
libreoffice-l10n-zh-Hant-4.3.3.2-4.1
libreoffice-l10n-nb-4.3.3.2-4.1
libreoffice-l10n-ar-4.3.3.2-4.1
libreoffice-l10n-pl-4.3.3.2-4.1
libreoffice-impress-4.3.3.2-4.1
libreoffice-l10n-dz-4.3.3.2-4.1
libreoffice-l10n-uk-4.3.3.2-4.1
libreoffice-l10n-kn-4.3.3.2-4.1
libreoffice-l10n-af-4.3.3.2-4.1
libreoffice-l10n-hi-4.3.3.2-4.1
libreoffice-l10n-lv-4.3.3.2-4.1
libreoffice-icon-theme-sifr-4.3.3.2-4.1
libreoffice-icon-theme-hicontrast-4.3.3.2-4.1
libreoffice-impress-debuginfo-4.3.3.2-4.1
libreoffice-l10n-th-4.3.3.2-4.1
libreoffice-l10n-lt-4.3.3.2-4.1
libreoffice-sdk-debuginfo-4.3.3.2-4.1
libreoffice-l10n-br-4.3.3.2-4.1
libreoffice-l10n-de-4.3.3.2-4.1
libreoffice-writer-4.3.3.2-4.1
libreoffice-l10n-ru-4.3.3.2-4.1
libreoffice-l10n-mr-4.3.3.2-4.1
libreoffice-icon-theme-oxygen-4.3.3.2-4.1
libreoffice-l10n-xh-4.3.3.2-4.1
libreoffice-l10n-gl-4.3.3.2-4.1
libreoffice-l10n-pt-PT-4.3.3.2-4.1
libreoffice-l10n-si-4.3.3.2-4.1
libreoffice-l10n-nn-4.3.3.2-4.1
libreoffice-calc-extensions-4.3.3.2-4.1
libreoffice-pyuno-debuginfo-4.3.3.2-4.1
libreoffice-l10n-he-4.3.3.2-4.1
libreoffice-l10n-hr-4.3.3.2-4.1
libreoffice-l10n-bn-4.3.3.2-4.1
libreoffice-debuginfo-4.3.3.2-4.1
libreoffice-l10n-kk-4.3.3.2-4.1
libreoffice-l10n-en-4.3.3.2-4.1
libreoffice-l10n-ko-4.3.3.2-4.1
libreoffice-sdk-4.3.3.2-4.1
libreoffice-base-drivers-mysql-debuginfo-4.3.3.2-4.1
libreoffice-l10n-gu-4.3.3.2-4.1
libreoffice-draw-4.3.3.2-4.1
libreoffice-l10n-ta-4.3.3.2-4.1
libreoffice-writer-debuginfo-4.3.3.2-4.1
libreoffice-officebean-debuginfo-4.3.3.2-4.1
libreoffice-l10n-ml-4.3.3.2-4.1
libreoffice-l10n-nr-4.3.3.2-4.1
libreoffice-l10n-cy-4.3.3.2-4.1
libreoffice-kde4-4.3.3.2-4.1
libreoffice-l10n-et-4.3.3.2-4.1
libreoffice-calc-4.3.3.2-4.1
libreoffice-l10n-tr-4.3.3.2-4.1
libreoffice-l10n-nso-4.3.3.2-4.1
libreoffice-l10n-ro-4.3.3.2-4.1
libreoffice-base-drivers-postgresql-debuginfo-4.3.3.2-4.1
libreoffice-filters-optional-4.3.3.2-4.1

libreoffice-l10n-sv-4.3.3.2-4.1
libreoffice-icon-theme-crystal-4.3.3.2-4.1
libreoffice-branding-upstream-4.3.3.2-4.1
libreoffice-l10n-ca-4.3.3.2-4.1
libreoffice-icon-theme-tango-4.3.3.2-4.1
libreoffice-l10n-or-4.3.3.2-4.1
libreoffice-l10n-pa-4.3.3.2-4.1
libreoffice-l10n-it-4.3.3.2-4.1
libreoffice-l10n-cs-4.3.3.2-4.1
libreoffice-l10n-tn-4.3.3.2-4.1
libreoffice-l10n-te-4.3.3.2-4.1
libreoffice-l10n-el-4.3.3.2-4.1
libreoffice-math-debuginfo-4.3.3.2-4.1
libreoffice-calc-debuginfo-4.3.3.2-4.1
libreoffice-l10n-zh-Hans-4.3.3.2-4.1
libreoffice-gnome-4.3.3.2-4.1

142502 - SuSE SLES 11 SP3 apache2-mod_php53-9916 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
apache2-mod_php53-9916

Observation

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

https://download.suse.com/Download?buildid=Exepr193Sdo~
https://download.suse.com/Download?buildid=F2lbDT4Z370~
https://download.suse.com/Download?buildid=jjUeay-Ch9w~
https://download.suse.com/Download?buildid=e1KssCUv5L0~
https://download.suse.com/Download?buildid=j0mwVCnqNzs~
https://download.suse.com/Download?buildid=1hRPNIRsAUw~
https://download.suse.com/Download?buildid=YoF2iqWAnkg~

SuSE SLES 11 SP3
x86_64
php53-snmp-5.3.17-0.31.1
php53-fastcgi-5.3.17-0.31.1
php53-pdo-5.3.17-0.31.1
php53-pcntl-5.3.17-0.31.1
php53-shmop-5.3.17-0.31.1
php53-intl-5.3.17-0.31.1
php53-zip-5.3.17-0.31.1
php53-gettext-5.3.17-0.31.1
php53-openssl-5.3.17-0.31.1
php53-pspell-5.3.17-0.31.1
php53-mcrypt-5.3.17-0.31.1
php53-ctype-5.3.17-0.31.1
php53-5.3.17-0.31.1
php53-fileinfo-5.3.17-0.31.1
php53-pear-5.3.17-0.31.1
php53-dom-5.3.17-0.31.1
php53-gd-5.3.17-0.31.1

php53-iconv-5.3.17-0.31.1
php53-suhosin-5.3.17-0.31.1
php53-exif-5.3.17-0.31.1
php53-tokenizer-5.3.17-0.31.1
php53-sysvsem-5.3.17-0.31.1
php53-sysvmsg-5.3.17-0.31.1
php53-xmlreader-5.3.17-0.31.1
php53-zlib-5.3.17-0.31.1
php53-odbc-5.3.17-0.31.1
php53-dba-5.3.17-0.31.1
php53-pgsql-5.3.17-0.31.1
apache2-mod_php53-5.3.17-0.31.1
php53-wddx-5.3.17-0.31.1
php53-json-5.3.17-0.31.1
php53-bz2-5.3.17-0.31.1
php53-calendar-5.3.17-0.31.1
php53-mysql-5.3.17-0.31.1
php53-curl-5.3.17-0.31.1
php53-xsl-5.3.17-0.31.1
php53-bcmath-5.3.17-0.31.1
php53-soap-5.3.17-0.31.1
php53-mbstring-5.3.17-0.31.1
php53-gmp-5.3.17-0.31.1
php53-ldap-5.3.17-0.31.1
php53-ftp-5.3.17-0.31.1
php53-xmlrpc-5.3.17-0.31.1
php53-xmlwriter-5.3.17-0.31.1
php53-sysvshm-5.3.17-0.31.1

i586
php53-snmp-5.3.17-0.31.1
php53-fastcgi-5.3.17-0.31.1
php53-pdo-5.3.17-0.31.1
php53-pcntl-5.3.17-0.31.1
php53-shmop-5.3.17-0.31.1
php53-intl-5.3.17-0.31.1
php53-zip-5.3.17-0.31.1
php53-gettext-5.3.17-0.31.1
php53-openssl-5.3.17-0.31.1
php53-pspell-5.3.17-0.31.1
php53-mcrypt-5.3.17-0.31.1
php53-ctype-5.3.17-0.31.1
php53-5.3.17-0.31.1
php53-fileinfo-5.3.17-0.31.1
php53-pear-5.3.17-0.31.1
php53-dom-5.3.17-0.31.1
php53-gd-5.3.17-0.31.1
php53-iconv-5.3.17-0.31.1
php53-suhosin-5.3.17-0.31.1
php53-exif-5.3.17-0.31.1
php53-tokenizer-5.3.17-0.31.1
php53-sysvsem-5.3.17-0.31.1
php53-sysvmsg-5.3.17-0.31.1
php53-xmlreader-5.3.17-0.31.1
php53-zlib-5.3.17-0.31.1
php53-odbc-5.3.17-0.31.1
php53-dba-5.3.17-0.31.1
php53-pgsql-5.3.17-0.31.1
apache2-mod_php53-5.3.17-0.31.1
php53-wddx-5.3.17-0.31.1

php53-json-5.3.17-0.31.1
php53-bz2-5.3.17-0.31.1
php53-calendar-5.3.17-0.31.1
php53-mysql-5.3.17-0.31.1
php53-curl-5.3.17-0.31.1
php53-xsl-5.3.17-0.31.1
php53-bcmath-5.3.17-0.31.1
php53-soap-5.3.17-0.31.1
php53-mbstring-5.3.17-0.31.1
php53-gmp-5.3.17-0.31.1
php53-ldap-5.3.17-0.31.1
php53-ftp-5.3.17-0.31.1
php53-xmlrpc-5.3.17-0.31.1
php53-xmlwriter-5.3.17-0.31.1
php53-sysvshm-5.3.17-0.31.1

142508 - SuSE Linux 13.1 openSUSE-SU-2014:1412-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3693

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1412-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00049.html

SuSE Linux 13.1
i586
libreoffice-l10n-ca-4.1.6.2-29.3
libreoffice-help-bg-4.1.6.2-29.1
libreoffice-base-debuginfo-4.1.6.2-29.1
libreoffice-filters-optional-4.1.6.2-29.1
libreoffice-writer-extensions-4.1.6.2-29.1
libreoffice-l10n-prebuilt-4.1.6.2-29.1
libreoffice-draw-4.1.6.2-29.1
libreoffice-l10n-sr-4.1.6.2-29.3
libreoffice-help-gl-4.1.6.2-29.1
libreoffice-help-sv-4.1.6.2-29.1
libreoffice-help-sl-4.1.6.2-29.1
libreoffice-help-ru-4.1.6.2-29.1
libreoffice-l10n-ka-4.1.6.2-29.3
libreoffice-draw-debuginfo-4.1.6.2-29.1
libreoffice-debugsource-4.1.6.2-29.1
libreoffice-l10n-be-BY-4.1.6.2-29.3
libreoffice-l10n-ss-4.1.6.2-29.3
libreoffice-l10n-et-4.1.6.2-29.3
libreoffice-sdk-doc-4.1.6.2-29.1
libreoffice-help-fr-4.1.6.2-29.1
libreoffice-calc-4.1.6.2-29.1
libreoffice-l10n-ts-4.1.6.2-29.3
libreoffice-gnome-4.1.6.2-29.1
libreoffice-l10n-en-GB-4.1.6.2-29.3

libreoffice-l10n-st-4.1.6.2-29.3
libreoffice-l10n-tg-4.1.6.2-29.3
libreoffice-help-sk-4.1.6.2-29.1
libreoffice-help-gu-IN-4.1.6.2-29.1
libreoffice-help-km-4.1.6.2-29.1
libreoffice-kde-4.1.6.2-29.1
libreoffice-help-ast-4.1.6.2-29.1
libreoffice-l10n-hu-4.1.6.2-29.3
libreoffice-help-pt-BR-4.1.6.2-29.1
libreoffice-l10n-nn-4.1.6.2-29.3
libreoffice-icon-theme-oxygen-4.1.6.2-29.1
libreoffice-l10n-ar-4.1.6.2-29.3
libreoffice-l10n-pt-4.1.6.2-29.3
libreoffice-l10n-de-4.1.6.2-29.3
libreoffice-help-pt-4.1.6.2-29.1
libreoffice-l10n-gu-IN-4.1.6.2-29.3
libreoffice-l10n-mk-4.1.6.2-29.3
libreoffice-help-et-4.1.6.2-29.1
libreoffice-l10n-km-4.1.6.2-29.3
libreoffice-l10n-vi-4.1.6.2-29.3
libreoffice-l10n-fr-4.1.6.2-29.3
libreoffice-sdk-4.1.6.2-29.1
libreoffice-l10n-th-4.1.6.2-29.3
libreoffice-help-fi-4.1.6.2-29.1
libreoffice-kde-debuginfo-4.1.6.2-29.1
libreoffice-l10n-en-ZA-4.1.6.2-29.3
libreoffice-l10n-mr-4.1.6.2-29.3
libreoffice-l10n-cs-4.1.6.2-29.3
libreoffice-help-vi-4.1.6.2-29.1
libreoffice-base-drivers-postgresql-4.1.6.2-29.1
libreoffice-l10n-te-4.1.6.2-29.3
libreoffice-help-en-GB-4.1.6.2-29.1
libreoffice-kde4-4.1.6.2-29.1
libreoffice-l10n-uk-4.1.6.2-29.3
libreoffice-base-extensions-4.1.6.2-29.1
libreoffice-l10n-as-4.1.6.2-29.3
libreoffice-l10n-ve-4.1.6.2-29.3
libreoffice-help-ja-4.1.6.2-29.1
libreoffice-help-hu-4.1.6.2-29.1
libreoffice-pyuno-4.1.6.2-29.1
libreoffice-l10n-zh-CN-4.1.6.2-29.3
libreoffice-debuginfo-4.1.6.2-29.1
libreoffice-l10n-pl-4.1.6.2-29.3
libreoffice-l10n-am-4.1.6.2-29.3
libreoffice-l10n-ja-4.1.6.2-29.3
libreoffice-icon-theme-hicontrast-4.1.6.2-29.1
libreoffice-help-ca-4.1.6.2-29.1
libreoffice-l10n-el-4.1.6.2-29.3
libreoffice-l10n-nr-4.1.6.2-29.3
libreoffice-help-mk-4.1.6.2-29.1
libreoffice-impress-extensions-debuginfo-4.1.6.2-29.1
libreoffice-l10n-or-4.1.6.2-29.3
libreoffice-l10n-id-4.1.6.2-29.3
libreoffice-l10n-da-4.1.6.2-29.3
libreoffice-impress-extensions-4.1.6.2-29.1
libreoffice-help-de-4.1.6.2-29.1
libreoffice-kde4-debuginfo-4.1.6.2-29.1
libreoffice-l10n-sl-4.1.6.2-29.3
libreoffice-base-drivers-mysql-debuginfo-4.1.6.2-29.1
libreoffice-base-4.1.6.2-29.1

libreoffice-math-debuginfo-4.1.6.2-29.1
libreoffice-l10n-fi-4.1.6.2-29.3
libreoffice-pyuno-debuginfo-4.1.6.2-29.1
libreoffice-impress-4.1.6.2-29.1
libreoffice-l10n-cy-4.1.6.2-29.3
libreoffice-l10n-ga-4.1.6.2-29.3
libreoffice-l10n-lt-4.1.6.2-29.3
libreoffice-l10n-hr-4.1.6.2-29.3
libreoffice-calc-extensions-4.1.6.2-29.1
libreoffice-help-cs-4.1.6.2-29.1
libreoffice-l10n-sv-4.1.6.2-29.3
libreoffice-l10n-it-4.1.6.2-29.3
libreoffice-help-en-US-4.1.6.2-29.1
libreoffice-help-es-4.1.6.2-29.1
libreoffice-l10n-pt-BR-4.1.6.2-29.3
libreoffice-base-drivers-mysql-4.1.6.2-29.1
libreoffice-l10n-tr-4.1.6.2-29.3
libreoffice-l10n-ko-4.1.6.2-29.3
libreoffice-l10n-gl-4.1.6.2-29.3
libreoffice-help-en-ZA-4.1.6.2-29.1
libreoffice-officebean-4.1.6.2-29.1
libreoffice-l10n-eo-4.1.6.2-29.3
libreoffice-l10n-eu-4.1.6.2-29.3
libreoffice-gnome-debuginfo-4.1.6.2-29.1
libreoffice-calc-debuginfo-4.1.6.2-29.1
libreoffice-l10n-ug-4.1.6.2-29.3
libreoffice-writer-debuginfo-4.1.6.2-29.1
libreoffice-l10n-bg-4.1.6.2-29.3
libreoffice-help-zh-CN-4.1.6.2-29.1
libreoffice-l10n-sh-4.1.6.2-29.3
libreoffice-l10n-kn-4.1.6.2-29.3
libreoffice-draw-extensions-4.1.6.2-29.1
libreoffice-help-hi-IN-4.1.6.2-29.1
libreoffice-help-it-4.1.6.2-29.1
libreoffice-help-zh-TW-4.1.6.2-29.1
libreoffice-sdk-debuginfo-4.1.6.2-29.1
libreoffice-l10n-ml-4.1.6.2-29.3
libreoffice-l10n-is-4.1.6.2-29.3
libreoffice-help-tr-4.1.6.2-29.1
libreoffice-l10n-gd-4.1.6.2-29.3
libreoffice-l10n-es-4.1.6.2-29.3
libreoffice-icon-theme-crystal-4.1.6.2-29.1
libreoffice-icon-theme-galaxy-4.1.6.2-29.1
libreoffice-branding-upstream-4.1.6.2-29.1
libreoffice-mailmerge-4.1.6.2-29.1
libreoffice-l10n-xh-4.1.6.2-29.3
libreoffice-l10n-zu-4.1.6.2-29.3
libreoffice-icon-themes-prebuilt-4.1.6.2-29.1
libreoffice-l10n-ro-4.1.6.2-29.3
libreoffice-l10n-hi-IN-4.1.6.2-29.3
libreoffice-l10n-ru-4.1.6.2-29.3
libreoffice-l10n-af-4.1.6.2-29.3
libreoffice-help-eu-4.1.6.2-29.1
libreoffice-help-ko-4.1.6.2-29.1
libreoffice-l10n-he-4.1.6.2-29.3
libreoffice-l10n-pa-IN-4.1.6.2-29.3
libreoffice-l10n-zh-TW-4.1.6.2-29.3
libreoffice-help-el-4.1.6.2-29.1
libreoffice-math-4.1.6.2-29.1
libreoffice-help-nb-4.1.6.2-29.1

libreoffice-l10n-br-4.1.6.2-29.3
libreoffice-4.1.6.2-29.1
libreoffice-l10n-ta-4.1.6.2-29.3
libreoffice-icon-theme-tango-4.1.6.2-29.1
libreoffice-l10n-nl-4.1.6.2-29.3
libreoffice-help-nl-4.1.6.2-29.1
libreoffice-l10n-nb-4.1.6.2-29.3
libreoffice-help-pl-4.1.6.2-29.1
libreoffice-l10n-sk-4.1.6.2-29.3
libreoffice-help-da-4.1.6.2-29.1
libreoffice-l10n-ast-4.1.6.2-29.3
libreoffice-impress-debuginfo-4.1.6.2-29.1
libreoffice-writer-4.1.6.2-29.1
libreoffice-officebean-debuginfo-4.1.6.2-29.1
libreoffice-l10n-rw-4.1.6.2-29.3
libreoffice-l10n-om-4.1.6.2-29.3
libreoffice-base-drivers-postgresql-debuginfo-4.1.6.2-29.1

142510 - SuSE Linux 13.2 openSUSE-SU-2014:1426-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1426-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00059.html

SuSE Linux 13.2
x86_64
openssl-doc-1.0.1j-2.4.1
libopenssl1_0_0-32bit-1.0.1j-2.4.1
libopenssl1_0_0-debuginfo-32bit-1.0.1j-2.4.1
libopenssl-devel-32bit-1.0.1j-2.4.1
libopenssl1_0_0-hmac-32bit-1.0.1j-2.4.1

i586
libopenssl1_0_0-1.0.1j-2.4.1
openssl-1.0.1j-2.4.1
libopenssl1_0_0-debuginfo-1.0.1j-2.4.1
libopenssl-devel-1.0.1j-2.4.1
libopenssl1_0_0-hmac-1.0.1j-2.4.1
openssl-debugsource-1.0.1j-2.4.1
openssl-debuginfo-1.0.1j-2.4.1

170422 - Amazon Linux AMI ALAS-2014-445 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634

Description

The scan detected that the host is missing the following update:
ALAS-2014-445

Observation

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

https://alas.aws.amazon.com/ALAS-2014-445.html

Amazon Linux AMI
x86_64
rsyslog-debuginfo-5.8.10-9.26.amzn1
rsyslog-snmp-5.8.10-9.26.amzn1
rsyslog-5.8.10-9.26.amzn1
rsyslog-gssapi-5.8.10-9.26.amzn1
rsyslog-gnutls-5.8.10-9.26.amzn1
rsyslog-pgsql-5.8.10-9.26.amzn1
rsyslog-mysql-5.8.10-9.26.amzn1

i686
rsyslog-debuginfo-5.8.10-9.26.amzn1
rsyslog-snmp-5.8.10-9.26.amzn1
rsyslog-gssapi-5.8.10-9.26.amzn1
rsyslog-5.8.10-9.26.amzn1
rsyslog-gnutls-5.8.10-9.26.amzn1
rsyslog-pgsql-5.8.10-9.26.amzn1
rsyslog-mysql-5.8.10-9.26.amzn1

174589 - Scientific Linux Security ERRATA Moderate: libvncserver on SL6.x, SL7.x i386/x86_64 (1411-2805)

Category: SSH Module -> NonIntrusive -> Scientific Linux 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:
Security ERRATA Moderate: libvncserver on SL6.x, SL7.x i386/x86_64 (1411-2805)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=2805

SL7
x86_64
libvncserver-devel-0.9.9-9.el7_0.1
libvncserver-0.9.9-9.el7_0.1
libvncserver-debuginfo-0.9.9-9.el7_0.1

SL6
x86_64
libvncserver-0.9.7-7.el6_6.1
libvncserver-debuginfo-0.9.7-7.el6_6.1
libvncserver-devel-0.9.7-7.el6_6.1

i386
libvncserver-0.9.7-7.el6_6.1
libvncserver-debuginfo-0.9.7-7.el6_6.1
libvncserver-devel-0.9.7-7.el6_6.1

174594 - Scientific Linux Security ERRATA Important: libXfont on SL6.x, SL7.x i386/srpm/x86_64 (1411-3802)

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

Risk Level: High

CVE: CVE-2014-0209, CVE-2014-0210, CVE-2014-0211

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libXfont on SL6.x, SL7.x i386/srpm/x86_64 (1411-3802)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=3802

SL7
x86_64
libXfont-1.4.7-2.el7_0
libXfont-debuginfo-1.4.7-2.el7_0
libXfont-devel-1.4.7-2.el7_0

noarch
libXfont-debuginfo-1.4.7-2.el7_0

SL6
x86_64
libXfont-1.4.5-4.el6_6
libXfont-devel-1.4.5-4.el6_6
libXfont-debuginfo-1.4.5-4.el6_6

i386
libXfont-1.4.5-4.el6_6
libXfont-devel-1.4.5-4.el6_6
libXfont-debuginfo-1.4.5-4.el6_6

noarch
libXfont-debuginfo-1.4.5-4.el6_6

184611 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2409-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3615, CVE-2014-3640, CVE-2014-3689, CVE-2014-5263, CVE-2014-5388, CVE-2014-7815

Description

The scan detected that the host is missing the following update:
USN-2409-1

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/002727.html

Ubuntu 14.10

qemu-system-arm_2.1+dfsg-4ubuntu6.1
qemu-system-aarch64_2.1+dfsg-4ubuntu6.1
qemu-system_2.1+dfsg-4ubuntu6.1
qemu-system-mips_2.1+dfsg-4ubuntu6.1
qemu-system-misc_2.1+dfsg-4ubuntu6.1
qemu-system-x86_2.1+dfsg-4ubuntu6.1
qemu-system-ppc_2.1+dfsg-4ubuntu6.1
qemu-system-sparc_2.1+dfsg-4ubuntu6.1

Ubuntu 14.04

qemu-system-misc_2.0.0+dfsg-2ubuntu1.7
qemu-system_2.0.0+dfsg-2ubuntu1.7
qemu-system-arm_2.0.0+dfsg-2ubuntu1.7
qemu-system-ppc_2.0.0+dfsg-2ubuntu1.7
qemu-system-mips_2.0.0+dfsg-2ubuntu1.7
qemu-system-aarch64_2.0.0+dfsg-2ubuntu1.7
qemu-system-sparc_2.0.0+dfsg-2ubuntu1.7
qemu-system-x86_2.0.0+dfsg-2ubuntu1.7

Ubuntu 12.04

qemu-kvm_1.0+noroms-0ubuntu14.19

Ubuntu 10.04

qemu-kvm_0.12.3+noroms-0ubuntu9.25

188497 - Fedora Linux 20 FEDORA-2014-14113 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8517

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14113

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/143408.html

Fedora Core 20

tnftp-20141031-1.fc20

188498 - Fedora Linux 19 FEDORA-2014-14059 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3675, CVE-2014-3676, CVE-2014-3677

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14059

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/143420.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143421.html

Fedora Core 19

mokutil-0.2.0-1.fc19
shim-signed-0.8-2

188501 - Fedora Linux 20 FEDORA-2014-14058 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3675, CVE-2014-3676, CVE-2014-3677

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14058

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/143465.html
http://lists.fedoraproject.org/pipermail/package-announce/2014-November/143464.html

Fedora Core 20

mokutil-0.2.0-1.fc20
shim-signed-0.8-3

188519 - Fedora Linux 19 FEDORA-2014-14068 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3610, CVE-2014-3611, CVE-2014-3646, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-3690, CVE-2014-8369

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14068

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/144040.html

Fedora Core 19

kernel-3.14.23-100.fc19

17434 - (SOL15780) F5 BIG-IP Multiple OpenSSH Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-2532, CVE-2014-2653

Description

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

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 devices. The flaws lie in the OpenSSH component. Successful exploitation could allow an attacker to obtain sensitive information or bypass security restrictions.

85827 - CentOS 7 CESA-2014-1827 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
CESA-2014-1827

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020753.html

CentOS 7
x86_64
kdenetwork-4.10.5-8.el7_0
kdenetwork-kopete-4.10.5-8.el7_0
kdenetwork-kopete-libs-4.10.5-8.el7_0
kdenetwork-krfb-4.10.5-8.el7_0
kdenetwork-krdc-devel-4.10.5-8.el7_0
kdenetwork-kopete-devel-4.10.5-8.el7_0
kdenetwork-krfb-libs-4.10.5-8.el7_0
kdenetwork-kdnssd-4.10.5-8.el7_0
kdenetwork-fileshare-samba-4.10.5-8.el7_0
kdenetwork-kget-libs-4.10.5-8.el7_0
kdenetwork-krdc-libs-4.10.5-8.el7_0
kdenetwork-krdc-4.10.5-8.el7_0
kdenetwork-kget-4.10.5-8.el7_0

i686

kdenetwork-kget-libs-4.10.5-8.el7_0
kdenetwork-krdc-devel-4.10.5-8.el7_0
kdenetwork-kopete-devel-4.10.5-8.el7_0
kdenetwork-kopete-libs-4.10.5-8.el7_0
kdenetwork-krfb-libs-4.10.5-8.el7_0
kdenetwork-krdc-libs-4.10.5-8.el7_0

noarch
kdenetwork-devel-4.10.5-8.el7_0
kdenetwork-common-4.10.5-8.el7_0

93414 - Mandriva Linux MBS1 MDVSA-2014-214 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3635, CVE-2014-3636, CVE-2014-3637, CVE-2014-3638, CVE-2014-3639, CVE-2014-7824

Description

The scan detected that the host is missing the following update:
MDVSA-2014-214

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%3A214/

Mandriva Linux mbs1
x86_64
dbus-1.4.16-7.5
lib64dbus-1_3-1.4.16-7.5
dbus-doc-1.4.16-7.5
dbus-x11-1.4.16-7.5
lib64dbus-1-devel-1.4.16-7.5

142505 - SuSE Linux 13.2 openSUSE-SU-2014:1397-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3694, CVE-2014-3695, CVE-2014-3696, CVE-2014-3697, CVE-2014-3698

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1397-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00037.html

SuSE Linux 13.2
i586
libpurple-tcl-2.10.10-5.4.1
libpurple-lang-2.10.10-5.4.1
finch-devel-2.10.10-5.4.1

libpurple-debuginfo-2.10.10-5.4.1
libpurple-2.10.10-5.4.1
finch-debuginfo-2.10.10-5.4.1
pidgin-2.10.10-5.4.1
libpurple-branding-upstream-2.10.10-5.4.1
libpurple-tcl-debuginfo-2.10.10-5.4.1
libpurple-meanwhile-2.10.10-5.4.1
finch-2.10.10-5.4.1
pidgin-devel-2.10.10-5.4.1
pidgin-debuginfo-2.10.10-5.4.1
libpurple-meanwhile-debuginfo-2.10.10-5.4.1
libpurple-branding-openSUSE-13.2-2.3.1
libpurple-devel-2.10.10-5.4.1
pidgin-debugsource-2.10.10-5.4.1

174588 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1411-2556)

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1411-2556)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=2556

SL6
x86_64
kernel-debuginfo-2.6.32-504.1.3.el6
python-perf-debuginfo-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-debug-debuginfo-2.6.32-504.1.3.el6
kernel-debuginfo-common-x86_64-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
python-perf-2.6.32-504.1.3.el6
perf-debuginfo-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6

i386
kernel-debuginfo-2.6.32-504.1.3.el6
kernel-debug-devel-2.6.32-504.1.3.el6
kernel-headers-2.6.32-504.1.3.el6
kernel-debug-2.6.32-504.1.3.el6
kernel-debug-debuginfo-2.6.32-504.1.3.el6
python-perf-debuginfo-2.6.32-504.1.3.el6
kernel-2.6.32-504.1.3.el6
python-perf-2.6.32-504.1.3.el6
perf-debuginfo-2.6.32-504.1.3.el6
kernel-devel-2.6.32-504.1.3.el6
perf-2.6.32-504.1.3.el6

kernel-debuginfo-common-i686-2.6.32-504.1.3.el6

noarch
kernel-doc-2.6.32-504.1.3.el6
kernel-firmware-2.6.32-504.1.3.el6
kernel-abi-whitelists-2.6.32-504.1.3.el6

174590 - Scientific Linux Security ERRATA Moderate: kdenetwork on SL7.x x86_64 (1411-2944)

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: kdenetwork on SL7.x x86_64 (1411-2944)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=2944

SL7
x86_64
kdenetwork-kget-libs-4.10.5-8.el7_0
kdenetwork-krfb-libs-4.10.5-8.el7_0
kdenetwork-kopete-libs-4.10.5-8.el7_0
kdenetwork-krfb-4.10.5-8.el7_0
kdenetwork-krdc-devel-4.10.5-8.el7_0
kdenetwork-krdc-libs-4.10.5-8.el7_0
kdenetwork-kopete-4.10.5-8.el7_0
kdenetwork-kopete-devel-4.10.5-8.el7_0
kdenetwork-4.10.5-8.el7_0
kdenetwork-kdnssd-4.10.5-8.el7_0
kdenetwork-fileshare-samba-4.10.5-8.el7_0
kdenetwork-debuginfo-4.10.5-8.el7_0
kdenetwork-krdc-4.10.5-8.el7_0
kdenetwork-kget-4.10.5-8.el7_0

noarch
kdenetwork-devel-4.10.5-8.el7_0
kdenetwork-common-4.10.5-8.el7_0

188505 - Fedora Linux 21 FEDORA-2014-14892 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5648

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14892

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/144230.html

Fedora Core 21

libdigidoc-3.9.1.1191-1.fc21

17267 - (JSA10654) Juniper Junos RADIUS Authentication Server Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-6379

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in the RADIUS authentication and accounting components. Successful exploitation could allow lead to possible unintended authentication success.

17313 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 31.2

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

Risk Level: Medium

CVE: CVE-2014-1574, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1585, CVE-2014-1586

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source Email, newsgroup, news feed, and chat client.

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

17314 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 31.2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-1574, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1585, CVE-2014-1586

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source Email, newsgroup, news feed, and chat client.

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

17327 - IOServer Resource Exhaustion Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-5425

Description

A resource exhaustion vulnerability is present in some versions of IOServer OPC Server.

Observation

IOServer OPC Server allows HMI and SCADA systems to exchange plant floor data with Programmable Logic Controllers.

A resource exhaustion vulnerability is present in some versions of IOServer OPC Server. The flaw is in the DNP3 protocol that causes an out of bound read. Successful exploitation by a remote attacker could result in crashing the OPC server or resource exhaustion on the affected system.

17345 - (HPSBMU03152) HP Operations Orchestration SSL Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

A SSL information disclosure vulnerability is present in some versions of HP Operations Orchestration.

Observation

HP Operations Orchestration is Hewlett-Packard IT Process Automation solution.

A SSL information disclosure vulnerability is present in some versions of HP Operations Orchestration. The flaw lies in a weakness in the CBC encryption algorithm within the SSL 3.0 protocol. Successful exploitation by a remote attacker could allow access to potentially sensitive information.

17349 - IBM WebSphere Portal Multiple Information Disclosure Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-3083, CVE-2014-4761

Description

Multiple vulnerabilities are 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.

Multiple vulnerabilities are present in some versions of IBM WebSphere Portal. The flaws lie in the WebSphere Application Server component. Successful exploitation could allow a remote attacker to disclose sensitive information.

17419 - IBM WebSphere Portal Unspecified Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-4814

Description

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

Observation

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

A denial of service vulnerability is present in some versions of IBM WebSphere. The flaw is due to the failure to properly detect recursion during entity expansion. Successful exploitation by a remote attacker could result in a denial of service condition.

17420 - IBM WebSphere Portal Unspecified Arbitrary Code Execution Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-4808

Description

A vulnerability is present in some versions of IBM WebSphere.

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. The flaw is due to unspecified reason. Successful exploitation could allow a remote attacker to execute arbitrary code on the system or cause a denial of service.

17421 - IBM WebSphere Portal Filename Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-4821

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 different web server error codes based on whether a requested file exists. Successful exploitation could allow a remote attacker to disclose sensitive information.

17422 - IBM WebSphere Portal Cross-site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-6125

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 caused by improper validation of user-supplied input. Successful exploitation could allow a remote attacker to inject arbitrary web script or HTML code.

17423 - IBM WebSphere Portal Unspecified Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-6126

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.

17433 - (SOL15732) F5 BIG-IP Linux Kernel Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-0311

Description

A privilege escalation vulnerability is present in some versions of F5 BIG-IP devices.

Observation

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

A privilege escalation vulnerability is present in some versions of F5 BIG-IP devices. The flaw lies in Linux kernel. Successful exploitation could allow an attacker to obtain sensitive information, cause denial of service or obtain OS privileges.

17436 - Symantec Endpoint Protection Manager Multiple Cross-Site Scripting

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

Risk Level: Medium

CVE: CVE-2014-3438

Description

A vulnerability in some versions of Symantec Endpoint Protection Manager could lead to cross-site scripting.

Observation

A vulnerability in some versions of Symantec Endpoint Protection Manager could lead to cross-site scripting.

The flaw occurs as the management console does not provide sufficient validation/sanitation of incoming input. Successful exploitation could allow a remote attacker to inject arbitrary web script or HTML code.

17437 - Symantec Endpoint Protection Manager Arbitrary File Write Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2014-3439

Description

A vulnerability in some versions of Symantec Endpoint Protection Manager could lead to remote code execution.

Observation

A vulnerability in some versions of Symantec Endpoint Protection Manager could lead to remote code execution.

The flaw is due to improper filtering of user-supplied data to the logging component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17439 - WordPress Comment Status Manipulation Cross Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-7233

Description

A Cross-site request forgery vulnerability is present in some versions of WordPress.

Observation

WordPress is a popular blog web application.

A Cross-site request forgery vulnerability is present in some versions of WordPress. The flaw lies in options-discussion.php. Successful exploitation could allow an attacker to execute remote code.

58997 - Debian Linux 7.0 DSA-3072-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3710

Description

The scan detected that the host is missing the following update:
DSA-3072-1

Observation

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

http://www.debian.org/security/2014/dsa-3072

Debian 7.0
all
file_5.11-2+deb7u6

85825 - CentOS 7 CESA-2014-1846 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8564

Description

The scan detected that the host is missing the following update:
CESA-2014-1846

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020756.html

CentOS 7
x86_64
gnutls-utils-3.1.18-10.el7_0
gnutls-devel-3.1.18-10.el7_0
gnutls-3.1.18-10.el7_0
gnutls-dane-3.1.18-10.el7_0
gnutls-c++-3.1.18-10.el7_0

i686
gnutls-devel-3.1.18-10.el7_0
gnutls-3.1.18-10.el7_0
gnutls-dane-3.1.18-10.el7_0
gnutls-c++-3.1.18-10.el7_0

91662 - Oracle Enterprise Linux ELSA-2014-1846 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8564

Description

The scan detected that the host is missing the following update:
ELSA-2014-1846

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/004631.html

OEL7
x86_64
gnutls-utils-3.1.18-10.el7_0
gnutls-devel-3.1.18-10.el7_0
gnutls-3.1.18-10.el7_0
gnutls-dane-3.1.18-10.el7_0
gnutls-c++-3.1.18-10.el7_0

140609 - Red Hat Enterprise Linux RHSA-2014-1873 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3633, CVE-2014-3657, CVE-2014-7823

Description

The scan detected that the host is missing the following update:
RHSA-2014-1873

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1873.html

RHEL6D
x86_64
libvirt-client-0.10.2-46.el6_6.2
libvirt-debuginfo-0.10.2-46.el6_6.2
libvirt-0.10.2-46.el6_6.2
libvirt-python-0.10.2-46.el6_6.2

i386
libvirt-client-0.10.2-46.el6_6.2
libvirt-debuginfo-0.10.2-46.el6_6.2
libvirt-0.10.2-46.el6_6.2
libvirt-python-0.10.2-46.el6_6.2

RHEL6S
x86_64
libvirt-devel-0.10.2-46.el6_6.2
libvirt-client-0.10.2-46.el6_6.2
libvirt-debuginfo-0.10.2-46.el6_6.2
libvirt-0.10.2-46.el6_6.2
libvirt-python-0.10.2-46.el6_6.2

i386
libvirt-devel-0.10.2-46.el6_6.2
libvirt-client-0.10.2-46.el6_6.2
libvirt-debuginfo-0.10.2-46.el6_6.2
libvirt-0.10.2-46.el6_6.2
libvirt-python-0.10.2-46.el6_6.2

RHEL6WS
x86_64
libvirt-devel-0.10.2-46.el6_6.2
libvirt-client-0.10.2-46.el6_6.2
libvirt-debuginfo-0.10.2-46.el6_6.2
libvirt-0.10.2-46.el6_6.2
libvirt-python-0.10.2-46.el6_6.2

i386
libvirt-devel-0.10.2-46.el6_6.2
libvirt-client-0.10.2-46.el6_6.2
libvirt-debuginfo-0.10.2-46.el6_6.2
libvirt-0.10.2-46.el6_6.2
libvirt-python-0.10.2-46.el6_6.2

140610 - Red Hat Enterprise Linux RHSA-2014-1846 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8564

Description

The scan detected that the host is missing the following update:
RHSA-2014-1846

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1846.html

RHEL7WS
x86_64
gnutls-utils-3.1.18-10.el7_0
gnutls-devel-3.1.18-10.el7_0
gnutls-debuginfo-3.1.18-10.el7_0
gnutls-3.1.18-10.el7_0
gnutls-dane-3.1.18-10.el7_0
gnutls-c++-3.1.18-10.el7_0

RHEL7D
x86_64
gnutls-utils-3.1.18-10.el7_0
gnutls-debuginfo-3.1.18-10.el7_0
gnutls-3.1.18-10.el7_0
gnutls-dane-3.1.18-10.el7_0

RHEL7S
x86_64
gnutls-utils-3.1.18-10.el7_0
gnutls-devel-3.1.18-10.el7_0
gnutls-debuginfo-3.1.18-10.el7_0
gnutls-3.1.18-10.el7_0
gnutls-dane-3.1.18-10.el7_0
gnutls-c++-3.1.18-10.el7_0

142503 - SuSE Linux 13.2 openSUSE-SU-2014:1411-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-5277, CVE-2014-7189

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1411-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00048.html

SuSE Linux 13.2

x86_64
docker-debuginfo-1.3.1-5.2
docker-zsh-completion-1.3.1-5.2
docker-debugsource-1.3.1-5.2
docker-1.3.1-5.2
docker-bash-completion-1.3.1-5.2

i586
go-1.3.3-5.1
go-vim-1.3.3-5.1
go-emacs-1.3.3-5.1
go-doc-1.3.3-5.1
go-debugsource-1.3.3-5.1
go-debuginfo-1.3.3-5.1

142509 - SuSE SLES 11 SP3, SLED 11 SP3 libxml2-9914 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
libxml2-9914

Observation

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

https://download.suse.com/Download?buildid=55--zgjWUls~
https://download.suse.com/Download?buildid=vHWWIKaVq54~
https://download.suse.com/Download?buildid=McgKzeMSUQ8~
https://download.suse.com/Download?buildid=EXOHpO8hl0w~
https://download.suse.com/Download?buildid=XC-Nk6k1fUs~
https://download.suse.com/Download?buildid=SAbRXiOMuz0~
https://download.suse.com/Download?buildid=SQI9kGOnSgA~
https://download.suse.com/Download?buildid=goZ2K-ZZz0I~
https://download.suse.com/Download?buildid=jpCFvTI5cVs~

SuSE SLED 11 SP3
x86_64
libxml2-python-2.7.6-0.31.1
libxml2-32bit-2.7.6-0.31.1
libxml2-2.7.6-0.31.1

i586
libxml2-python-2.7.6-0.31.1
libxml2-2.7.6-0.31.1

SuSE SLES 11 SP3
x86_64
libxml2-python-2.7.6-0.31.1
libxml2-32bit-2.7.6-0.31.1
libxml2-2.7.6-0.31.1
libxml2-doc-2.7.6-0.31.1

i586
libxml2-python-2.7.6-0.31.1

libxml2-2.7.6-0.31.1
libxml2-doc-2.7.6-0.31.1

142515 - SuSE Linux 13.2 openSUSE-SU-2014:1406-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1406-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00046.html

SuSE Linux 13.2
i586
konversation-debuginfo-1.5.1-3.4.1
konversation-debugsource-1.5.1-3.4.1
konversation-lang-1.5.1-3.4.1
konversation-1.5.1-3.4.1

170420 - Amazon Linux AMI ALAS-2014-447 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8090

Description

The scan detected that the host is missing the following update:
ALAS-2014-447

Observation

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

https://alas.aws.amazon.com/ALAS-2014-447.html

Amazon Linux AMI
x86_64
ruby19-libs-1.9.3.551-32.64.amzn1
rubygem19-bigdecimal-1.1.0-32.64.amzn1
rubygem19-io-console-0.3-32.64.amzn1
ruby19-devel-1.9.3.551-32.64.amzn1
rubygem19-json-1.5.5-32.64.amzn1
ruby19-debuginfo-1.9.3.551-32.64.amzn1
ruby19-doc-1.9.3.551-32.64.amzn1
ruby19-1.9.3.551-32.64.amzn1

i686
ruby19-libs-1.9.3.551-32.64.amzn1
rubygem19-bigdecimal-1.1.0-32.64.amzn1

rubygem19-io-console-0.3-32.64.amzn1
ruby19-devel-1.9.3.551-32.64.amzn1
rubygem19-json-1.5.5-32.64.amzn1
ruby19-debuginfo-1.9.3.551-32.64.amzn1
ruby19-doc-1.9.3.551-32.64.amzn1
ruby19-1.9.3.551-32.64.amzn1

noarch
rubygem19-minitest-2.5.1-32.64.amzn1
rubygems19-devel-1.8.23.2-32.64.amzn1
rubygem19-rdoc-3.9.5-32.64.amzn1
ruby19-irb-1.9.3.551-32.64.amzn1
rubygems19-1.8.23.2-32.64.amzn1
rubygem19-rake-0.9.2.2-32.64.amzn1

170421 - Amazon Linux AMI ALAS-2014-446 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-6421, CVE-2014-6422, CVE-2014-6423, CVE-2014-6424, CVE-2014-6425, CVE-2014-6426, CVE-2014-6427, CVE-2014-6428, CVE-2014-6429, CVE-2014-6430, CVE-2014-6431, CVE-2014-6432

Description

The scan detected that the host is missing the following update:
ALAS-2014-446

Observation

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

https://alas.aws.amazon.com/ALAS-2014-446.html

Amazon Linux AMI
x86_64
wireshark-devel-1.8.10-8.14.amzn1
wireshark-1.8.10-8.14.amzn1
wireshark-debuginfo-1.8.10-8.14.amzn1

i686
wireshark-devel-1.8.10-8.14.amzn1
wireshark-1.8.10-8.14.amzn1
wireshark-debuginfo-1.8.10-8.14.amzn1

170423 - Amazon Linux AMI ALAS-2014-444 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
ALAS-2014-444

Observation

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

https://alas.aws.amazon.com/ALAS-2014-444.html

Amazon Linux AMI
x86_64
libxml2-static-2.9.1-3.1.32.amzn1
libxml2-python-2.9.1-3.1.32.amzn1
libxml2-devel-2.9.1-3.1.32.amzn1
libxml2-2.9.1-3.1.32.amzn1
libxml2-debuginfo-2.9.1-3.1.32.amzn1

i686
libxml2-debuginfo-2.9.1-3.1.32.amzn1
libxml2-python-2.9.1-3.1.32.amzn1
libxml2-devel-2.9.1-3.1.32.amzn1
libxml2-2.9.1-3.1.32.amzn1
libxml2-static-2.9.1-3.1.32.amzn1

170425 - Amazon Linux AMI ALAS-2014-449 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8090

Description

The scan detected that the host is missing the following update:
ALAS-2014-449

Observation

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

https://alas.aws.amazon.com/ALAS-2014-449.html

Amazon Linux AMI
x86_64
rubygem21-bigdecimal-1.2.4-1.15.amzn1
rubygem21-psych-2.0.5-1.15.amzn1
ruby21-devel-2.1.5-1.15.amzn1
rubygem21-io-console-0.4.2-1.15.amzn1
ruby21-libs-2.1.5-1.15.amzn1
ruby21-2.1.5-1.15.amzn1
ruby21-debuginfo-2.1.5-1.15.amzn1

i686
rubygem21-bigdecimal-1.2.4-1.15.amzn1
rubygem21-psych-2.0.5-1.15.amzn1
ruby21-devel-2.1.5-1.15.amzn1
rubygem21-io-console-0.4.2-1.15.amzn1
ruby21-libs-2.1.5-1.15.amzn1
ruby21-2.1.5-1.15.amzn1
ruby21-debuginfo-2.1.5-1.15.amzn1

noarch
ruby21-irb-2.1.5-1.15.amzn1
ruby21-doc-2.1.5-1.15.amzn1
rubygems21-2.2.2-1.15.amzn1
rubygems21-devel-2.2.2-1.15.amzn1

170426 - Amazon Linux AMI ALAS-2014-448 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8090

Description

The scan detected that the host is missing the following update:
ALAS-2014-448

Observation

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

https://alas.aws.amazon.com/ALAS-2014-448.html

Amazon Linux AMI
x86_64
rubygem20-bigdecimal-1.2.0-1.20.amzn1
ruby20-debuginfo-2.0.0.598-1.20.amzn1
rubygem20-io-console-0.4.2-1.20.amzn1
ruby20-devel-2.0.0.598-1.20.amzn1
rubygem20-psych-2.0.0-1.20.amzn1
ruby20-2.0.0.598-1.20.amzn1
ruby20-libs-2.0.0.598-1.20.amzn1

i686
rubygem20-bigdecimal-1.2.0-1.20.amzn1
ruby20-debuginfo-2.0.0.598-1.20.amzn1
rubygem20-io-console-0.4.2-1.20.amzn1
ruby20-devel-2.0.0.598-1.20.amzn1
rubygem20-psych-2.0.0-1.20.amzn1
ruby20-2.0.0.598-1.20.amzn1
ruby20-libs-2.0.0.598-1.20.amzn1

noarch
ruby20-irb-2.0.0.598-1.20.amzn1
ruby20-doc-2.0.0.598-1.20.amzn1
rubygems20-2.0.14-1.20.amzn1
rubygems20-devel-2.0.14-1.20.amzn1

174591 - Scientific Linux Security ERRATA Moderate: libvirt on SL6.x i386/x86_64 (1411-3675)

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

Risk Level: Medium

CVE: CVE-2014-3633, CVE-2014-3657, CVE-2014-7823

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libvirt on SL6.x i386/x86_64 (1411-3675)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=3675

SL6
x86_64
libvirt-devel-0.10.2-46.el6_6.2
libvirt-client-0.10.2-46.el6_6.2
libvirt-debuginfo-0.10.2-46.el6_6.2
libvirt-0.10.2-46.el6_6.2
libvirt-python-0.10.2-46.el6_6.2
libvirt-lock-sanlock-0.10.2-46.el6_6.2

i386
libvirt-devel-0.10.2-46.el6_6.2
libvirt-client-0.10.2-46.el6_6.2
libvirt-debuginfo-0.10.2-46.el6_6.2
libvirt-0.10.2-46.el6_6.2
libvirt-python-0.10.2-46.el6_6.2

174592 - Scientific Linux Security ERRATA Moderate: gnutls on SL7.x x86_64 (1411-2684)

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

Risk Level: Medium

CVE: CVE-2014-8564

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: gnutls on SL7.x x86_64 (1411-2684)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=2684

SL7
x86_64
gnutls-utils-3.1.18-10.el7_0
gnutls-devel-3.1.18-10.el7_0
gnutls-debuginfo-3.1.18-10.el7_0
gnutls-3.1.18-10.el7_0
gnutls-dane-3.1.18-10.el7_0
gnutls-c++-3.1.18-10.el7_0

188504 - Fedora Linux 19 FEDORA-2014-13702 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13702

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/143968.html

Fedora Core 19

konversation-1.5.1-1.fc19

188508 - Fedora Linux 21 FEDORA-2014-13837 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13837

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/143409.html

Fedora Core 21

konversation-1.5.1-1.fc21

188511 - Fedora Linux 20 FEDORA-2014-13791 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13791

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/143788.html

Fedora Core 20

konversation-1.5.1-1.fc20

188514 - Fedora Linux 21 FEDORA-2014-14734 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8564

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14734

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/143994.html

Fedora Core 21

gnutls-3.3.10-1.fc21

188520 - Fedora Linux 20 FEDORA-2014-14760 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8564

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14760

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/143630.html

Fedora Core 20

gnutls-3.1.28-1.fc20

93413 - Mandriva Linux MBS1 MDVSA-2014-213 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3707

Description

The scan detected that the host is missing the following update:
MDVSA-2014-213

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%3A213/

Mandriva Linux mbs1
x86_64
lib64curl-devel-7.24.0-3.7
lib64curl4-7.24.0-3.7
curl-7.24.0-3.7
curl-examples-7.24.0-3.7

142507 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1395-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1395-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00035.html

SuSE Linux 13.1
i586
libserf-devel-1.3.8-20.1
libserf-1-1-1.3.8-20.1
libserf-debugsource-1.3.8-20.1
libserf-1-1-debuginfo-1.3.8-20.1

SuSE Linux 12.3
i586
libserf-1-0-1.1.1-2.8.1
libserf-devel-1.1.1-2.8.1
libserf-debugsource-1.1.1-2.8.1
libserf-1-0-debuginfo-1.1.1-2.8.1

SuSE Linux 13.2
i586
libserf-devel-1.3.8-2.4.1
libserf-1-1-1.3.8-2.4.1
libserf-debugsource-1.3.8-2.4.1
libserf-1-1-debuginfo-1.3.8-2.4.1

188515 - Fedora Linux 20 FEDORA-2014-13777 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2005-2090, CVE-2011-3389, CVE-2012-4929, CVE-2014-3566

Description

The scan detected that the host is missing the following update:
FEDORA-2014-13777

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/143507.html

Fedora Core 20

Pound-2.6-8.fc20

188516 - Fedora Linux 21 FEDORA-2014-15159 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7825, CVE-2014-7826, CVE-2014-7841, CVE-2014-7842, CVE-2014-7843

Description

The scan detected that the host is missing the following update:
FEDORA-2014-15159

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/144193.html

Fedora Core 21

kernel-3.17.3-300.fc21

33279 - Oracle Solaris 144180-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
144180-02

Observation

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

https://getupdates.oracle.com/readme/144180-02

SunOS 5.10: nfslogd patch

SOLARIS_10

SUNWnfssu:11.10.0,REV=2005.01.21.15.53

33280 - Oracle Solaris 144181-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
144181-02

Observation

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

https://getupdates.oracle.com/readme/144181-02

SunOS 5.10(x86): nfslogd patch

SOLARIS_10_x86

SUNWnfssu:11.10.0,REV=2005.01.21.16.34

33281 - Oracle Solaris 151561-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
151561-01

Observation

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

https://getupdates.oracle.com/readme/151561-01

SunOS 5.10: libshare_nfs.so.1 patch

SOLARIS_10

SUNWnfssu:11.10.0,REV=2005.01.21.15.53

33282 - Oracle Solaris 151562-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
151562-01

Observation

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

https://getupdates.oracle.com/readme/151562-01

SunOS 5.10(x86): libshare_nfs.so.1 patch

SOLARIS_10_x86

SUNWnfssu:11.10.0,REV=2005.01.21.16.34

88648 - Slackware Linux 14.1 SSA:2014-320-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2014-320-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.314855

Slackware 14.1
x86_64
mozilla-thunderbird-31.2.0-x86_64-1

142506 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1396-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8354, CVE-2014-8355, CVE-2014-8562

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1396-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00036.html

SuSE Linux 13.1
x86_64
libMagickCore-6_Q16-1-32bit-6.8.6.9-2.24.1
libMagick++-devel-32bit-6.8.6.9-2.24.1
libMagickWand-6_Q16-1-32bit-6.8.6.9-2.24.1
libMagick++-6_Q16-2-32bit-6.8.6.9-2.24.1
ImageMagick-doc-6.8.6.9-2.24.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.6.9-2.24.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.6.9-2.24.1
ImageMagick-devel-32bit-6.8.6.9-2.24.1
libMagick++-6_Q16-2-debuginfo-32bit-6.8.6.9-2.24.1

i586
ImageMagick-extra-debuginfo-6.8.6.9-2.24.1
ImageMagick-devel-6.8.6.9-2.24.1
libMagickCore-6_Q16-1-6.8.6.9-2.24.1
libMagickCore-6_Q16-1-debuginfo-6.8.6.9-2.24.1
libMagick++-devel-6.8.6.9-2.24.1
ImageMagick-extra-6.8.6.9-2.24.1
libMagickWand-6_Q16-1-6.8.6.9-2.24.1

ImageMagick-6.8.6.9-2.24.1
ImageMagick-debugsource-6.8.6.9-2.24.1
perl-PerlMagick-debuginfo-6.8.6.9-2.24.1
perl-PerlMagick-6.8.6.9-2.24.1
ImageMagick-debuginfo-6.8.6.9-2.24.1
libMagick++-6_Q16-2-6.8.6.9-2.24.1
libMagickWand-6_Q16-1-debuginfo-6.8.6.9-2.24.1
libMagick++-6_Q16-2-debuginfo-6.8.6.9-2.24.1

SuSE Linux 12.3
x86_64
libMagickCore5-32bit-6.7.8.8-4.17.1
ImageMagick-doc-6.7.8.8-4.17.1
libMagickWand5-32bit-6.7.8.8-4.17.1
libMagickCore5-debuginfo-32bit-6.7.8.8-4.17.1
ImageMagick-devel-32bit-6.7.8.8-4.17.1
libMagickWand5-debuginfo-32bit-6.7.8.8-4.17.1

i586
libMagick++5-debuginfo-6.7.8.8-4.17.1
libMagick++5-6.7.8.8-4.17.1
ImageMagick-debuginfo-6.7.8.8-4.17.1
ImageMagick-6.7.8.8-4.17.1
libMagickCore5-debuginfo-6.7.8.8-4.17.1
ImageMagick-devel-6.7.8.8-4.17.1
ImageMagick-extra-6.7.8.8-4.17.1
libMagickWand5-debuginfo-6.7.8.8-4.17.1
libMagickCore5-6.7.8.8-4.17.1
perl-PerlMagick-debuginfo-6.7.8.8-4.17.1
ImageMagick-extra-debuginfo-6.7.8.8-4.17.1
ImageMagick-debugsource-6.7.8.8-4.17.1
perl-PerlMagick-6.7.8.8-4.17.1
libMagickWand5-6.7.8.8-4.17.1
libMagick++-devel-6.7.8.8-4.17.1

SuSE Linux 13.2
x86_64
libMagick++-devel-32bit-6.8.9.8-4.1
ImageMagick-doc-6.8.9.8-4.1
libMagickCore-6_Q16-2-debuginfo-32bit-6.8.9.8-4.1
ImageMagick-devel-32bit-6.8.9.8-4.1
libMagick++-6_Q16-5-32bit-6.8.9.8-4.1
libMagickWand-6_Q16-2-debuginfo-32bit-6.8.9.8-4.1
libMagick++-6_Q16-5-debuginfo-32bit-6.8.9.8-4.1
libMagickCore-6_Q16-2-32bit-6.8.9.8-4.1
libMagickWand-6_Q16-2-32bit-6.8.9.8-4.1

i586
libMagick++-6_Q16-5-debuginfo-6.8.9.8-4.1
ImageMagick-debugsource-6.8.9.8-4.1
perl-PerlMagick-debuginfo-6.8.9.8-4.1
libMagick++-6_Q16-5-6.8.9.8-4.1
perl-PerlMagick-6.8.9.8-4.1
libMagick++-devel-6.8.9.8-4.1
ImageMagick-extra-debuginfo-6.8.9.8-4.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-4.1
libMagickWand-6_Q16-2-6.8.9.8-4.1
ImageMagick-extra-6.8.9.8-4.1
libMagickCore-6_Q16-2-6.8.9.8-4.1
ImageMagick-debuginfo-6.8.9.8-4.1

libMagickWand-6_Q16-2-debuginfo-6.8.9.8-4.1
ImageMagick-6.8.9.8-4.1
ImageMagick-devel-6.8.9.8-4.1

142512 - SuSE Linux 13.2 openSUSE-SU-2014:1407-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-0249

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1407-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00047.html

SuSE Linux 13.2
x86_64
sssd-debuginfo-32bit-1.12.2-3.4.1
sssd-32bit-1.12.2-3.4.1

i586
python-sss_nss_idmap-debuginfo-1.12.2-3.4.1
sssd-debugsource-1.12.2-3.4.1
libnfsidmap-sss-debuginfo-1.12.2-3.4.1
libipa_hbac0-1.12.2-3.4.1
libsss_nss_idmap0-debuginfo-1.12.2-3.4.1
libnfsidmap-sss-1.12.2-3.4.1
python-sssd-config-1.12.2-3.4.1
sssd-ipa-1.12.2-3.4.1
libsss_nss_idmap0-1.12.2-3.4.1
sssd-proxy-debuginfo-1.12.2-3.4.1
sssd-wbclient-1.12.2-3.4.1
python-ipa_hbac-debuginfo-1.12.2-3.4.1
sssd-debuginfo-1.12.2-3.4.1
sssd-ldap-1.12.2-3.4.1
sssd-krb5-1.12.2-3.4.1
python-ipa_hbac-1.12.2-3.4.1
sssd-krb5-common-debuginfo-1.12.2-3.4.1
libsss_nss_idmap-devel-1.12.2-3.4.1
sssd-ipa-debuginfo-1.12.2-3.4.1
sssd-tools-debuginfo-1.12.2-3.4.1
sssd-tools-1.12.2-3.4.1
python-sssd-config-debuginfo-1.12.2-3.4.1
libsss_simpleifp0-1.12.2-3.4.1
libsss_simpleifp0-debuginfo-1.12.2-3.4.1
sssd-dbus-1.12.2-3.4.1
sssd-proxy-1.12.2-3.4.1
sssd-1.12.2-3.4.1
sssd-krb5-debuginfo-1.12.2-3.4.1
sssd-wbclient-debuginfo-1.12.2-3.4.1
libsss_idmap-devel-1.12.2-3.4.1
libsss_sudo-debuginfo-1.12.2-3.4.1
libsss_sudo-1.12.2-3.4.1

libsss_idmap0-1.12.2-3.4.1
sssd-krb5-common-1.12.2-3.4.1
sssd-dbus-debuginfo-1.12.2-3.4.1
libipa_hbac0-debuginfo-1.12.2-3.4.1
sssd-wbclient-devel-1.12.2-3.4.1
libsss_simpleifp-devel-1.12.2-3.4.1
libsss_idmap0-debuginfo-1.12.2-3.4.1
python-sss_nss_idmap-1.12.2-3.4.1
sssd-ad-1.12.2-3.4.1
sssd-ldap-debuginfo-1.12.2-3.4.1
libipa_hbac-devel-1.12.2-3.4.1
sssd-ad-debuginfo-1.12.2-3.4.1

181288 - FreeBSD kde-workspace Privilege Escalation (dafa13a8-6e9b-11e4-8ef7-5453ed2e2b49)

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

Risk Level: Low

CVE: CVE-2014-8651

Description

The scan detected that the host is missing the following update:
kde-workspace -- privilege escalation (dafa13a8-6e9b-11e4-8ef7-5453ed2e2b49)

Observation

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

http://www.vuxml.org/freebsd/dafa13a8-6e9b-11e4-8ef7-5453ed2e2b49.html

Affected packages:
kde-workspace < 4.11.13_1

184612 - Ubuntu Linux 14.10 USN-2411-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1421

Description

The scan detected that the host is missing the following update:
USN-2411-1

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/002728.html

Ubuntu 14.10

mountall_2.54ubuntu0.14.10.1

188495 - Fedora Linux 20 FEDORA-2014-14493 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14493

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/144233.html

Fedora Core 20

python-requests-kerberos-0.6-1.fc20

188496 - Fedora Linux 19 FEDORA-2014-14498 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14498

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/144237.html

Fedora Core 19

python-requests-kerberos-0.6-1.fc19

188499 - Fedora Linux 19 FEDORA-2014-14257 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-4616

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14257

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/143576.html

Fedora Core 19

python3-3.3.2-10.fc19

188500 - Fedora Linux 21 FEDORA-2014-14461 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14461

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/143515.html

Fedora Core 21

python-requests-kerberos-0.6-1.fc21

188502 - Fedora Linux 21 FEDORA-2014-14617 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-1947

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14617

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/143680.html

Fedora Core 21

GraphicsMagick-1.3.20-3.fc21

188503 - Fedora Linux 19 FEDORA-2014-14865 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8651

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14865

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/144093.html

Fedora Core 19

kde-workspace-4.11.14-1.fc19

188506 - Fedora Linux 21 FEDORA-2014-14895 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8651

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14895

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/144034.html

Fedora Core 21

kde-workspace-4.11.14-1.fc21

188507 - Fedora Linux 20 FEDORA-2014-14247 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8321, CVE-2014-8322, CVE-2014-8323, CVE-2014-8324

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14247

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/143595.html

Fedora Core 20

aircrack-ng-1.2-0.3.rc1.fc20

188509 - Fedora Linux 20 FEDORA-2014-14813 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8651

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14813

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/143781.html

Fedora Core 20

kde-workspace-4.11.14-1.fc20

188510 - Fedora Linux 20 FEDORA-2014-14506 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14506

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/144210.html

Fedora Core 20

oath-toolkit-2.4.1-6.fc20

188512 - Fedora Linux 19 FEDORA-2014-14233 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8321, CVE-2014-8322, CVE-2014-8323, CVE-2014-8324

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14233

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/143606.html

Fedora Core 19

aircrack-ng-1.2-0.3.rc1.fc19

188513 - Fedora Linux 21 FEDORA-2014-14546 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14546

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/143664.html

Fedora Core 21

oath-toolkit-2.4.1-6.fc21

188517 - Fedora Linux 21 FEDORA-2014-14697 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14697

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/143984.html

Fedora Core 21

drupal7-ckeditor-1.16-2.fc21

188518 - Fedora Linux 20 FEDORA-2014-12991 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-12991

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/143468.html

Fedora Core 20

deluge-1.3.10-1.fc20

188521 - Fedora Linux 19 FEDORA-2014-14564 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2014-14564

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/144136.html

Fedora Core 19

qpid-cpp-0.26-12.fc19

58996 - Debian Linux 7.0 DSA-3073-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-5270

Description

The scan detected that the host is missing the following update:
DSA-3073-1

Observation

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

http://www.debian.org/security/2014/dsa-3073

Debian 7.0
all
libgcrypt11_1.5.0-5+deb7u2

142513 - SuSE SLES 11 SP3, SLED 11 SP3 krb5-201410-9827 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-5351

Description

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

krb5-201410-9827

Observation

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

https://download.suse.com/Download?buildid=YfPQfzafmPw~
https://download.suse.com/Download?buildid=0hiWEpao8zE~
https://download.suse.com/Download?buildid=w0FYugibbfI~
https://download.suse.com/Download?buildid=jHRN0ckp-Qw~
https://download.suse.com/Download?buildid=63uvIFeaeNU~
https://download.suse.com/Download?buildid=-hwEv7HAN3Q~
https://download.suse.com/Download?buildid=whjps25uh-I~
https://download.suse.com/Download?buildid=wRyl4UptXq4~
https://download.suse.com/Download?buildid=L96hiaz2xkY~

SuSE SLED 11 SP3
x86_64
krb5-client-1.6.3-133.49.64.1
krb5-32bit-1.6.3-133.49.64.1
krb5-1.6.3-133.49.64.1

i586
krb5-client-1.6.3-133.49.64.1
krb5-1.6.3-133.49.64.1

SuSE SLES 11 SP3
x86_64
krb5-plugin-kdb-ldap-1.6.3-133.49.64.1
krb5-client-1.6.3-133.49.64.1
krb5-server-1.6.3-133.49.64.1
krb5-apps-clients-1.6.3-133.49.64.1
krb5-apps-servers-1.6.3-133.49.64.1
krb5-32bit-1.6.3-133.49.64.1
krb5-plugin-preauth-pkinit-1.6.3-133.49.64.1
krb5-1.6.3-133.49.64.1

noarch
krb5-doc-1.6.3-133.49.64.1

i586
krb5-apps-clients-1.6.3-133.49.64.1
krb5-client-1.6.3-133.49.64.1
krb5-plugin-kdb-ldap-1.6.3-133.49.64.1
krb5-apps-servers-1.6.3-133.49.64.1
krb5-1.6.3-133.49.64.1
krb5-plugin-preauth-pkinit-1.6.3-133.49.64.1
krb5-server-1.6.3-133.49.64.1

ENHANCED CHECKS

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

17358 - (MS14-068) Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)

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

Risk Level: High

CVE: CVE-2014-6324

Update Details

Recommendation is updated Risk is updated

17360 - (MS14-066) Microsoft Windows Schannel Remote Code Execution (2992611)

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

Risk Level: High

CVE: CVE-2014-6321

Update Details

Risk is updated

17361 - (MS14-068) Microsoft Windows Kerberos Checksum Privilege Escalation (3011780)

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

Risk Level: High

CVE: CVE-2014-6324

Update Details

Observation is updated Recommendation is updated Risk is updated

32097 - Oracle Solaris 125358-19 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-1563, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated CVE is updated FASLScript is updated

32098 - Oracle Solaris 125359-19 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-1563, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated CVE is updated FASLScript is updated

32629 - Oracle Solaris 119060-68 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-3467, CVE-2007-1667, CVE-2007-5958, CVE-2010-1166, CVE-2011-2895, 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-2013-1992, CVE-2013-1993, 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-2013-2064, CVE-2013-2066, CVE-2013-6462

Update Details

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

32633 - Oracle Solaris 119059-69 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-3467, CVE-2007-1667, CVE-2007-5958, CVE-2010-1166, CVE-2011-2895, 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-2013-1992, CVE-2013-1993, 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-2013-2064, CVE-2013-2066, CVE-2013-6462

Update Details

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

33207 - Oracle Solaris 119213-30 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-1563, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated CVE is updated FASLScript is updated

33218 - Oracle Solaris 119214-30 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-1563, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated CVE is updated FASLScript is updated

11224 - (MS11-013) Microsoft Kerberos Unkeyed Checksum (2496930)

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

Risk Level: High

CVE: CVE-2011-0043

Update Details

Recommendation is updated

11226 - (MS11-013) Vulnerabilities in Microsoft Kerberos Could Allow Elevation Of Privilege (2496930)

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

Risk Level: High

CVE: CVE-2011-0043, CVE-2011-0091

Update Details

Recommendation is updated

33106 - Oracle Solaris 148562-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2004-0452, CVE-2005-0156, CVE-2005-0448, CVE-2005-4278, CVE-2010-1158, CVE-2010-1168, CVE-2010-2761, CVE-2010-4411, CVE-2011-2939, CVE-2012-5195, CVE-2012-5526, CVE-2012-6329, CVE-2013-1667

Update Details

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

33107 - Oracle Solaris 148561-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2004-0452, CVE-2005-0156, CVE-2005-0448, CVE-2005-4278, CVE-2010-1158, CVE-2010-1168, CVE-2010-2761, CVE-2010-4411, CVE-2011-2939, CVE-2012-5195, CVE-2012-5526, CVE-2012-6329, CVE-2013-1667

Update Details

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

58987 - Debian Linux 7.0 DSA-3064-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7345, CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Update Details

CVE is updated

85821 - CentOS 6, 7 CESA-2014-1826 Update Is Not Installed

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

Risk Level: High

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

Update Details

Name is updated Observation is updated FASLScript is updated

7852 - (MS10-014) Microsoft Windows Kerberos Null Pointer Dereference Vulnerability (977290)

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

Risk Level: Medium

CVE: CVE-2010-0035

Update Details

Recommendation is updated

33145 - Oracle Solaris 150401-18 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215

Update Details

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

7888 - (MS10-014) Vulnerability In Kerberos Could Allow Denial Of Service (977290)

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

Risk Level: Medium

CVE: CVE-2010-0035

Update Details

Recommendation is updated

11225 - (MS11-013) Microsoft Kerberos Spoofing (2496930)

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

Risk Level: Medium

CVE: CVE-2011-0091

Update Details

Recommendation is updated

33057 - Oracle Solaris 147794-14 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2002-2443, CVE-2013-1417, CVE-2013-1418

Update Details

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

33066 - Oracle Solaris 147793-14 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2002-2443, CVE-2013-1417, CVE-2013-1418

Update Details

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

170415 - Amazon Linux AMI ALAS-2014-440 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4650, CVE-2014-7185

Update Details

CVE is updated

33162 - Oracle Solaris 150400-18 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5862, CVE-2013-5876, CVE-2014-0447

Update Details

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

32078 - Oracle Solaris 123938-04 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2008-4989, CVE-2014-0092

Update Details

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

32079 - Oracle Solaris 123939-04 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2008-4989, CVE-2014-0092

Update Details

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

DELETED CHECKS

32644 - Oracle Solaris 144107-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

32651 - Oracle Solaris 144106-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

ADDITIONAL NOTES

- **32644** - was flagged as obsolete by the vendor.
- **32651** - 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.

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

Copyright 2014 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates