

MCAFFEE 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

21053 - (APSB16-38) Vulnerability In Adobe Animate

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

Risk Level: High

CVE: CVE-2016-7866

Description

A remote code execution vulnerability is present in some versions of Adobe Animate.

Observation

Adobe Animate is a software used to create web animations.

A remote code execution vulnerability is present in some versions of Adobe Animate. The flaw is due to memory corruption issues. Successful exploitation could allow an attacker to remotely execute arbitrary code.

The update provided by Adobe bulletin APSB16-38 resolves the issue. The target system is missing this update.

21054 - (APSB16-38) Vulnerability In Adobe Animate

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7866

Description

A remote code execution vulnerability is present in some versions of Adobe Animate.

Observation

Adobe Animate is a software used to create web animations.

A remote code execution vulnerability is present in some versions of Adobe Animate. The flaw is due to memory corruption issues. Successful exploitation could allow an attacker to remotely execute arbitrary code.

The update provided by Adobe bulletin APSB16-38 resolves the issue. The target system is missing this update.

130659 - Debian Linux 8.0 DSA-3744-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4658, CVE-2016-5131

Description

The scan detected that the host is missing the following update:
DSA-3744-1

Observation

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

<http://www.debian.org/security/2016/dsa-3744>

Debian 8.0
all
libxml2_2.9.1+dfsg1-5+deb8u4

130661 - Debian Linux 8.0 DSA-3746-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8808, CVE-2016-2317, CVE-2016-2318, CVE-2016-3714, CVE-2016-3715, CVE-2016-5118, CVE-2016-5240, CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684, CVE-2016-9830

Description

The scan detected that the host is missing the following update:
DSA-3746-1

Observation

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

<http://www.debian.org/security/2016/dsa-3746>

Debian 8.0
all
graphicsmagick_1.3.20-3+deb8u2

132318 - Oracle VM OVMSA-2016-0181 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-8956, CVE-2016-1583, CVE-2016-3070, CVE-2016-3157, CVE-2016-4569, CVE-2016-4578, CVE-2016-6136, CVE-2016-6480, CVE-2016-7117, CVE-2016-9555

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0181

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000608.html>

OVM3.2
x86_64
kernel-uek-firmware-2.6.39-400.293.2.el5uek
kernel-uek-2.6.39-400.293.2.el5uek

132319 - Oracle VM OVMSA-2016-0179 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-7117

Description

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

OVMSA-2016-0179

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000606.html>

OVM3.4

x86_64

kernel-uek-firmware-4.1.12-61.1.23.el6uek

kernel-uek-4.1.12-61.1.23.el6uek

132321 - Oracle VM OVMSA-2016-0180 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-3157, CVE-2016-7117

Description

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

OVMSA-2016-0180

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000607.html>

OVM3.3

x86_64

kernel-uek-firmware-3.8.13-118.15.2.el6uek

kernel-uek-3.8.13-118.15.2.el6uek

163241 - Oracle Enterprise Linux ELSA-2016-2962 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

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

ELSA-2016-2962

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006592.html>

<http://oss.oracle.com/pipermail/el-errata/2016-December/006588.html>

OEL5

i386

kernel-PAE-2.6.18-417.0.0.0.1.el5

kernel-debug-devel-2.6.18-417.el5

kernel-doc-2.6.18-417.el5

kernel-debug-devel-2.6.18-417.0.0.0.1.el5

kernel-devel-2.6.18-417.el5

kernel-debug-2.6.18-417.0.0.0.1.el5

kernel-2.6.18-417.el5

kernel-PAE-devel-2.6.18-417.0.0.0.1.el5

kernel-PAE-2.6.18-417.el5

kernel-2.6.18-417.0.0.0.1.el5

kernel-xen-devel-2.6.18-417.el5

kernel-doc-2.6.18-417.0.0.0.1.el5

kernel-devel-2.6.18-417.0.0.0.1.el5

kernel-headers-2.6.18-417.el5

kernel-xen-2.6.18-417.0.0.0.1.el5

kernel-xen-2.6.18-417.el5

kernel-PAE-devel-2.6.18-417.el5

kernel-xen-devel-2.6.18-417.0.0.0.1.el5

kernel-headers-2.6.18-417.0.0.0.1.el5

kernel-debug-2.6.18-417.el5

x86_64

kernel-debug-devel-2.6.18-417.el5

kernel-doc-2.6.18-417.el5

kernel-debug-devel-2.6.18-417.0.0.0.1.el5

kernel-devel-2.6.18-417.el5

kernel-2.6.18-417.el5

kernel-debug-2.6.18-417.0.0.0.1.el5

kernel-2.6.18-417.0.0.0.1.el5

kernel-xen-devel-2.6.18-417.el5

kernel-doc-2.6.18-417.0.0.0.1.el5

kernel-devel-2.6.18-417.0.0.0.1.el5

kernel-headers-2.6.18-417.el5

kernel-xen-2.6.18-417.0.0.0.1.el5

kernel-xen-2.6.18-417.el5

kernel-xen-devel-2.6.18-417.0.0.0.1.el5

kernel-headers-2.6.18-417.0.0.0.1.el5

kernel-debug-2.6.18-417.el5

163242 - Oracle Enterprise Linux ELSA-2016-3656 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3157, CVE-2016-7117

Description

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

ELSA-2016-3656

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006602.html>

<http://oss.oracle.com/pipermail/el-errata/2016-December/006603.html>

OEL7

x86_64

dtrace-modules-3.8.13-118.15.2.el7uek-0.4.5-3.el7

kernel-uek-firmware-3.8.13-118.15.2.el7uek

kernel-uek-debug-3.8.13-118.15.2.el7uek

kernel-uek-devel-3.8.13-118.15.2.el7uek

kernel-uek-debug-devel-3.8.13-118.15.2.el7uek

kernel-uek-3.8.13-118.15.2.el7uek

kernel-uek-doc-3.8.13-118.15.2.el7uek

OEL6

x86_64

kernel-uek-debug-3.8.13-118.15.2.el6uek

kernel-uek-firmware-3.8.13-118.15.2.el6uek

kernel-uek-devel-3.8.13-118.15.2.el6uek

kernel-uek-3.8.13-118.15.2.el6uek

kernel-uek-doc-3.8.13-118.15.2.el6uek

kernel-uek-debug-devel-3.8.13-118.15.2.el6uek

dtrace-modules-3.8.13-118.15.2.el6uek-0.4.5-3.el6

163243 - Oracle Enterprise Linux ELSA-2016-3657 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3157, CVE-2016-7117

Description

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

ELSA-2016-3657

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-December/006604.html>

<http://oss.oracle.com/pipermail/el-errata/2016-December/006605.html>

OEL5

x86_64

kernel-uek-firmware-2.6.39-400.293.2.el5uek

kernel-uek-doc-2.6.39-400.293.2.el5uek

kernel-uek-debug-devel-2.6.39-400.293.2.el5uek

kernel-uek-devel-2.6.39-400.293.2.el5uek

kernel-uek-2.6.39-400.293.2.el5uek

kernel-uek-debug-2.6.39-400.293.2.el5uek

i386

kernel-uek-firmware-2.6.39-400.293.2.el5uek

kernel-uek-doc-2.6.39-400.293.2.el5uek

kernel-uek-debug-devel-2.6.39-400.293.2.el5uek

kernel-uek-devel-2.6.39-400.293.2.el5uek

kernel-uek-2.6.39-400.293.2.el5uek

kernel-uek-debug-2.6.39-400.293.2.el5uek

OEL6

x86_64

kernel-uek-devel-2.6.39-400.293.2.el6uek

kernel-uek-2.6.39-400.293.2.el6uek

kernel-uek-firmware-2.6.39-400.293.2.el6uek

kernel-uek-debug-2.6.39-400.293.2.el6uek

kernel-uek-debug-devel-2.6.39-400.293.2.el6uek

kernel-uek-doc-2.6.39-400.293.2.el6uek

i386

kernel-uek-devel-2.6.39-400.293.2.el6uek

kernel-uek-2.6.39-400.293.2.el6uek

kernel-uek-firmware-2.6.39-400.293.2.el6uek

kernel-uek-debug-2.6.39-400.293.2.el6uek

kernel-uek-debug-devel-2.6.39-400.293.2.el6uek

kernel-uek-doc-2.6.39-400.293.2.el6uek

163247 - Oracle Enterprise Linux ELSA-2016-3655 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

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

ELSA-2016-3655

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-December/006601.html>

<http://oss.oracle.com/pipermail/el-errata/2016-December/006600.html>

OEL7

x86_64

kernel-uek-devel-4.1.12-61.1.23.el7uek

kernel-uek-firmware-4.1.12-61.1.23.el7uek

dtrace-modules-4.1.12-61.1.23.el7uek-0.5.3-2.el7

kernel-uek-4.1.12-61.1.23.el7uek

kernel-uek-debug-devel-4.1.12-61.1.23.el7uek

kernel-uek-debug-4.1.12-61.1.23.el7uek

kernel-uek-doc-4.1.12-61.1.23.el7uek

OEL6

x86_64

kernel-uek-doc-4.1.12-61.1.23.el6uek

kernel-uek-devel-4.1.12-61.1.23.el6uek

dtrace-modules-4.1.12-61.1.23.el6uek-0.5.3-2.el6

kernel-uek-4.1.12-61.1.23.el6uek

kernel-uek-firmware-4.1.12-61.1.23.el6uek

kernel-uek-debug-4.1.12-61.1.23.el6uek

kernel-uek-debug-devel-4.1.12-61.1.23.el6uek

178296 - Gentoo Linux GLSA-201612-46 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0729, CVE-2016-2099

Description

The scan detected that the host is missing the following update:
GLSA-201612-46

Observation

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

<https://security.gentoo.org/glsa/201612-46>

Affected packages:

dev-libs/xerces-c < 3.1.4-r1

21065 - IBM AIX Java Multiple Vulnerabilities (October 2016)

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Description

Multiple vulnerabilities are present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lie in Java SDK component. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

21068 - (HT207421) Apple Safari Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-4692, CVE-2016-4743, CVE-2016-7586, CVE-2016-7587, CVE-2016-7589, CVE-2016-7592, CVE-2016-7598, CVE-2016-7599, CVE-2016-7610, CVE-2016-7611, CVE-2016-7623, CVE-2016-7632, CVE-2016-7635, CVE-2016-7639, CVE-2016-7640, CVE-2016-7641, CVE-2016-7642, CVE-2016-7645, CVE-2016-7646, CVE-2016-7648, CVE-2016-7649, CVE-2016-7650, CVE-2016-7652, CVE-2016-7654, CVE-2016-7656

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

Multiple vulnerabilities are present in some versions of Apple Safari. The flaws lie in WebKit component. Successful exploitation could allow an attacker to obtain sensitive information, execute arbitrary code or cause a denial of service condition.

21070 - (HT207423) Apple macOS Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-1777, CVE-2016-1823, CVE-2016-4691, CVE-2016-4693, CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-6303, CVE-2016-6304, CVE-2016-7141, CVE-2016-7167, CVE-2016-7411, CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417, CVE-2016-7418, CVE-2016-7588, CVE-2016-7591, CVE-2016-7594, CVE-2016-7595, CVE-2016-7596, CVE-2016-7600, CVE-2016-7602, CVE-2016-7603, CVE-2016-7604, CVE-2016-7605, CVE-2016-7606, CVE-2016-7607, CVE-2016-7608, CVE-2016-7609, CVE-2016-7612, CVE-2016-7615, CVE-2016-7616, CVE-2016-7617, CVE-2016-7618, CVE-2016-7619, CVE-2016-7620, CVE-2016-7621, CVE-2016-7622, CVE-2016-7624, CVE-2016-7625, CVE-2016-7627, CVE-2016-7628, CVE-2016-7629, CVE-2016-7633, CVE-2016-7636, CVE-2016-7637, CVE-2016-7643, CVE-2016-7644, CVE-2016-7655, CVE-2016-7657, CVE-2016-7658, CVE-2016-7659, CVE-2016-7660, CVE-2016-7661, CVE-2016-7662, CVE-2016-7663, CVE-2016-7667, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-8625

Description

Multiple vulnerabilities are present in some versions of Apple macOS.

Observation

Apple macOS is the operating system developed by Apple.

Multiple vulnerabilities are present in some versions of Apple macOS. The flaw lies in several components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition, escalate privileges or remotely execute arbitrary code.

21055 - Apache Tomcat NIO HTTP Connector Information Disclosure Vulnerability

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

Risk Level: High

CVE: CVE-2016-8745

Description

An information disclosure is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

An information disclosure vulnerability is present in some versions of Apache Tomcat. The flaw lies in the NIO HTTP connector. Successful exploitation could allow an attacker to retrieve sensitive data.

21056 - (K26422113) F5 BIG-IP Libxml2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-1839

Description

A buffer overflow vulnerability is present in libxml2 in some versions of F5 BIG-IP systems.

Observation

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

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

21057 - Mozilla Firefox Multiple Vulnerabilities Prior To 50.1

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

Risk Level: High

CVE: CVE-2016-9080, CVE-2016-9893, CVE-2016-9894, CVE-2016-9895, CVE-2016-9896, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9903, CVE-2016-9904

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 several components. Successful exploitation could allow an attacker to cause a denial of service or execute arbitrary code.

21058 - Mozilla Firefox Multiple Vulnerabilities Prior To 50.1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-9080, CVE-2016-9893, CVE-2016-9894, CVE-2016-9895, CVE-2016-9896, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9903, CVE-2016-9904

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 several components. Successful exploitation could allow an attacker to cause a denial of service or execute arbitrary code.

21059 - Moxa DACenter Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-9354, CVE-2016-9356

Description

Multiple vulnerabilities are present in some versions of Moxa DACenter.

Observation

Moxa DACenter is a real time data collection software which acts as a data gateway between remote devices and databases.

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

21060 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.6

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-

2016-9902, CVE-2016-9904, CVE-2016-9905

Description

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

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or execute arbitrary code.

21061 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.6

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

Description

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

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or execute arbitrary code.

88833 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-359-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6702, CVE-2015-1283, CVE-2015-2716, CVE-2016-0718, CVE-2016-4472, CVE-2016-5300

Description

The scan detected that the host is missing the following update:
SSA:2016-359-01

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=2016&m=slackware-security.567786>

Slackware 14.0
x86_64
expat-2.2.0-x86_64-1

Slackware 13.37
x86_64
expat-2.2.0-x86_64-1

Slackware 14.1
x86_64
expat-2.2.0-x86_64-1

Slackware 13.1
x86_64
expat-2.2.0-x86_64-1

Slackware 14.2
x86_64
expat-2.2.0-x86_64-1

i586
expat-2.2.0-i586-1

Slackware 13.0
x86_64
expat-2.2.0-x86_64-1

141386 - Red Hat Enterprise Linux RHSA-2016-2973 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
RHSA-2016-2973

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2973.html>

RHEL6S
i386
thunderbird-45.6.0-1.el6_8
thunderbird-debuginfo-45.6.0-1.el6_8

x86_64
thunderbird-45.6.0-1.el6_8
thunderbird-debuginfo-45.6.0-1.el6_8

RHEL6WS
x86_64
thunderbird-45.6.0-1.el6_8
thunderbird-debuginfo-45.6.0-1.el6_8

i386
thunderbird-45.6.0-1.el6_8
thunderbird-debuginfo-45.6.0-1.el6_8

RHEL5D
x86_64
thunderbird-45.6.0-1.el5_11
thunderbird-debuginfo-45.6.0-1.el5_11

i386
thunderbird-45.6.0-1.el5_11
thunderbird-debuginfo-45.6.0-1.el5_11

RHEL7D
x86_64
thunderbird-45.6.0-1.el7_3
thunderbird-debuginfo-45.6.0-1.el7_3

RHEL6D
x86_64
thunderbird-45.6.0-1.el6_8
thunderbird-debuginfo-45.6.0-1.el6_8

i386
thunderbird-45.6.0-1.el6_8
thunderbird-debuginfo-45.6.0-1.el6_8

RHEL7WS
x86_64
thunderbird-45.6.0-1.el7_3
thunderbird-debuginfo-45.6.0-1.el7_3

141387 - Red Hat Enterprise Linux RHSA-2016-2974 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9445, CVE-2016-9447

Description

The scan detected that the host is missing the following update:
RHSA-2016-2974

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2974.html>

RHEL6D
x86_64
gststreamer-plugins-bad-free-debuginfo-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gststreamer-plugins-bad-free-0.10.19-5.el6_8
gststreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-0.10.19-5.el6_8

i386
gststreamer-plugins-bad-free-debuginfo-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gststreamer-plugins-bad-free-0.10.19-5.el6_8
gststreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-0.10.19-5.el6_8

RHEL6S
i386
gststreamer-plugins-bad-free-debuginfo-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gststreamer-plugins-bad-free-0.10.19-5.el6_8
gststreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-0.10.19-5.el6_8

x86_64
gststreamer-plugins-bad-free-debuginfo-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gststreamer-plugins-bad-free-0.10.19-5.el6_8
gststreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-0.10.19-5.el6_8

RHEL6WS

x86_64
gststreamer-plugins-bad-free-debuginfo-0.10.19-5.el6_8
gststreamer-plugins-bad-free-0.10.19-5.el6_8

i386

gststreamer-plugins-bad-free-debuginfo-0.10.19-5.el6_8
gststreamer-plugins-bad-free-0.10.19-5.el6_8

141389 - Red Hat Enterprise Linux RHSA-2016-2975 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808

Description

The scan detected that the host is missing the following update:
RHSA-2016-2975

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2975.html>

RHEL6D

x86_64
gststreamer-plugins-good-0.10.23-4.el6_8
gststreamer-plugins-good-devel-0.10.23-4.el6_8
gststreamer-plugins-good-debuginfo-0.10.23-4.el6_8

i386

gststreamer-plugins-good-0.10.23-4.el6_8
gststreamer-plugins-good-devel-0.10.23-4.el6_8
gststreamer-plugins-good-debuginfo-0.10.23-4.el6_8

RHEL6S

i386
gststreamer-plugins-good-0.10.23-4.el6_8
gststreamer-plugins-good-devel-0.10.23-4.el6_8
gststreamer-plugins-good-debuginfo-0.10.23-4.el6_8

x86_64

gststreamer-plugins-good-0.10.23-4.el6_8
gststreamer-plugins-good-devel-0.10.23-4.el6_8
gststreamer-plugins-good-debuginfo-0.10.23-4.el6_8

RHEL6WS

x86_64
gststreamer-plugins-good-debuginfo-0.10.23-4.el6_8
gststreamer-plugins-good-0.10.23-4.el6_8

i386
gstreamer-plugins-good-debuginfo-0.10.23-4.el6_8
gstreamer-plugins-good-0.10.23-4.el6_8

145104 - SuSE Linux 13.2 openSUSE-SU-2016:3228-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9933

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3228-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00133.html>

SuSE Linux 13.2
x86_64
libgd3-debuginfo-32bit-2.1.0-7.22.1
libgd3-2.1.0-7.22.1
libgd3-debuginfo-2.1.0-7.22.1
gd-devel-2.1.0-7.22.1
libgd3-32bit-2.1.0-7.22.1
gd-debugsource-2.1.0-7.22.1
gd-2.1.0-7.22.1
gd-debuginfo-2.1.0-7.22.1

i586
libgd3-2.1.0-7.22.1
libgd3-debuginfo-2.1.0-7.22.1
gd-devel-2.1.0-7.22.1
gd-debugsource-2.1.0-7.22.1
gd-2.1.0-7.22.1
gd-debuginfo-2.1.0-7.22.1

145105 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:3207-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10013, CVE-2016-10024, CVE-2016-9932

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3207-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002504.html>

SuSE SLES 12 SP1
x86_64
xen-libs-32bit-4.5.5_04-22.6.1
xen-tools-4.5.5_04-22.6.1
xen-kmp-default-4.5.5_04_k3.12.67_60.64.24-22.6.1
xen-tools-domU-4.5.5_04-22.6.1
xen-debugsource-4.5.5_04-22.6.1
xen-libs-debuginfo-32bit-4.5.5_04-22.6.1
xen-tools-domU-debuginfo-4.5.5_04-22.6.1
xen-libs-4.5.5_04-22.6.1
xen-libs-debuginfo-4.5.5_04-22.6.1
xen-tools-debuginfo-4.5.5_04-22.6.1
xen-4.5.5_04-22.6.1
xen-kmp-default-debuginfo-4.5.5_04_k3.12.67_60.64.24-22.6.1
xen-doc-html-4.5.5_04-22.6.1

SuSE SLED 12 SP1
x86_64
xen-libs-32bit-4.5.5_04-22.6.1
xen-kmp-default-4.5.5_04_k3.12.67_60.64.24-22.6.1
xen-libs-debuginfo-32bit-4.5.5_04-22.6.1
xen-libs-4.5.5_04-22.6.1
xen-kmp-default-debuginfo-4.5.5_04_k3.12.67_60.64.24-22.6.1
xen-debugsource-4.5.5_04-22.6.1
xen-4.5.5_04-22.6.1
xen-libs-debuginfo-4.5.5_04-22.6.1

145106 - SuSE Linux 13.2 openSUSE-SU-2016:3239-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9933, CVE-2016-9934, CVE-2016-9935

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3239-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00142.html>

SuSE Linux 13.2
i586
php5-fastcgi-debuginfo-5.6.1-89.1
php5-soap-debuginfo-5.6.1-89.1
php5-openssl-5.6.1-89.1
php5-intl-debuginfo-5.6.1-89.1
php5-firebird-debuginfo-5.6.1-89.1
php5-iconv-5.6.1-89.1
php5-gd-5.6.1-89.1
php5-suhosin-debuginfo-5.6.1-89.1
php5-debugsource-5.6.1-89.1
php5-pdo-debuginfo-5.6.1-89.1
php5-bcmath-5.6.1-89.1
php5-gettext-debuginfo-5.6.1-89.1
php5-mysql-5.6.1-89.1

php5-pdo-5.6.1-89.1
php5-opcache-debuginfo-5.6.1-89.1
php5-wddx-debuginfo-5.6.1-89.1
php5-pspell-debuginfo-5.6.1-89.1
php5-xmlrpc-debuginfo-5.6.1-89.1
php5-xsl-debuginfo-5.6.1-89.1
php5-sqlite-5.6.1-89.1
php5-phar-5.6.1-89.1
php5-fpm-debuginfo-5.6.1-89.1
php5-curl-5.6.1-89.1
php5-devel-5.6.1-89.1
php5-posix-5.6.1-89.1
php5-opcache-5.6.1-89.1
php5-shmop-debuginfo-5.6.1-89.1
php5-pcntl-5.6.1-89.1
php5-imap-5.6.1-89.1
php5-phar-debuginfo-5.6.1-89.1
php5-sysvmsg-5.6.1-89.1
php5-sockets-5.6.1-89.1
php5-xmlreader-5.6.1-89.1
php5-readline-5.6.1-89.1
php5-mbstring-debuginfo-5.6.1-89.1
php5-mysql-debuginfo-5.6.1-89.1
php5-suhosin-5.6.1-89.1
php5-posix-debuginfo-5.6.1-89.1
php5-pcntl-debuginfo-5.6.1-89.1
php5-fileinfo-5.6.1-89.1
php5-tokenizer-debuginfo-5.6.1-89.1
php5-calendar-5.6.1-89.1
php5-readline-debuginfo-5.6.1-89.1
php5-sqlite-debuginfo-5.6.1-89.1
php5-dom-5.6.1-89.1
php5-imap-debuginfo-5.6.1-89.1
php5-curl-debuginfo-5.6.1-89.1
php5-mbstring-5.6.1-89.1
php5-xmlreader-debuginfo-5.6.1-89.1
php5-zlib-debuginfo-5.6.1-89.1
php5-ctype-debuginfo-5.6.1-89.1
php5-ldap-5.6.1-89.1
php5-mssql-debuginfo-5.6.1-89.1
php5-bz2-debuginfo-5.6.1-89.1
php5-zip-5.6.1-89.1
php5-calendar-debuginfo-5.6.1-89.1
php5-mcrypt-debuginfo-5.6.1-89.1
php5-dba-debuginfo-5.6.1-89.1
php5-odbc-debuginfo-5.6.1-89.1
php5-iconv-debuginfo-5.6.1-89.1
php5-ftp-debuginfo-5.6.1-89.1
php5-wddx-5.6.1-89.1
php5-json-debuginfo-5.6.1-89.1
php5-gmp-5.6.1-89.1
php5-tokenizer-5.6.1-89.1
php5-dba-5.6.1-89.1
php5-xmlrpc-5.6.1-89.1
php5-exif-debuginfo-5.6.1-89.1
php5-odbc-5.6.1-89.1
php5-zip-debuginfo-5.6.1-89.1
php5-fastcgi-5.6.1-89.1
php5-snmp-5.6.1-89.1
php5-enchanted-5.6.1-89.1

php5-ldap-debuginfo-5.6.1-89.1
php5-pgsql-debuginfo-5.6.1-89.1
apache2-mod_php5-debuginfo-5.6.1-89.1
php5-sockets-debuginfo-5.6.1-89.1
php5-json-5.6.1-89.1
php5-bcmath-debuginfo-5.6.1-89.1
php5-tidy-5.6.1-89.1
php5-enchanted-debuginfo-5.6.1-89.1
php5-5.6.1-89.1
php5-zlib-5.6.1-89.1
php5-xmlwriter-debuginfo-5.6.1-89.1
php5-exif-5.6.1-89.1
php5-sysvshm-debuginfo-5.6.1-89.1
php5-sysvshm-5.6.1-89.1
php5-xmlwriter-5.6.1-89.1
php5-openssl-debuginfo-5.6.1-89.1
php5-debuginfo-5.6.1-89.1
php5-snmp-debuginfo-5.6.1-89.1
apache2-mod_php5-5.6.1-89.1
php5-sysvmsg-debuginfo-5.6.1-89.1
php5-bz2-5.6.1-89.1
php5-gmp-debuginfo-5.6.1-89.1
php5-shmop-5.6.1-89.1
php5-gd-debuginfo-5.6.1-89.1
php5-mssql-5.6.1-89.1
php5-fileinfo-debuginfo-5.6.1-89.1
php5-ftp-5.6.1-89.1
php5-sysvsem-5.6.1-89.1
php5-intl-5.6.1-89.1
php5-fpm-5.6.1-89.1
php5-sysvsem-debuginfo-5.6.1-89.1
php5-ctype-5.6.1-89.1
php5-pgsql-5.6.1-89.1
php5-gettext-5.6.1-89.1
php5-firebird-5.6.1-89.1
php5-soap-5.6.1-89.1
php5-tidy-debuginfo-5.6.1-89.1
php5-mcrypt-5.6.1-89.1
php5-ispell-5.6.1-89.1
php5-xsl-5.6.1-89.1
php5-dom-debuginfo-5.6.1-89.1

noarch

php5-pear-5.6.1-89.1

x86_64

php5-fastcgi-debuginfo-5.6.1-89.1
php5-soap-debuginfo-5.6.1-89.1
php5-openssl-5.6.1-89.1
php5-intl-debuginfo-5.6.1-89.1
php5-firebird-debuginfo-5.6.1-89.1
php5-iconv-5.6.1-89.1
php5-gd-5.6.1-89.1
php5-suhosin-debuginfo-5.6.1-89.1
php5-debugsource-5.6.1-89.1
php5-pdo-debuginfo-5.6.1-89.1
php5-bcmath-5.6.1-89.1
php5-gettext-debuginfo-5.6.1-89.1
php5-mysql-5.6.1-89.1
php5-pdo-5.6.1-89.1

php5-opcache-debuginfo-5.6.1-89.1
php5-wddx-debuginfo-5.6.1-89.1
php5-pspell-debuginfo-5.6.1-89.1
php5-xmlrpc-debuginfo-5.6.1-89.1
php5-xsl-debuginfo-5.6.1-89.1
php5-sqlite-5.6.1-89.1
php5-phar-5.6.1-89.1
php5-fpm-debuginfo-5.6.1-89.1
php5-curl-5.6.1-89.1
php5-devel-5.6.1-89.1
php5-posix-5.6.1-89.1
php5-opcache-5.6.1-89.1
php5-shmop-debuginfo-5.6.1-89.1
php5-pcntl-5.6.1-89.1
php5-imap-5.6.1-89.1
php5-phar-debuginfo-5.6.1-89.1
php5-sysvmsg-5.6.1-89.1
php5-sockets-5.6.1-89.1
php5-xmlreader-5.6.1-89.1
php5-readline-5.6.1-89.1
php5-mbstring-debuginfo-5.6.1-89.1
php5-mysql-debuginfo-5.6.1-89.1
php5-suhosin-5.6.1-89.1
php5-posix-debuginfo-5.6.1-89.1
php5-pcntl-debuginfo-5.6.1-89.1
php5-fileinfo-5.6.1-89.1
php5-tokenizer-debuginfo-5.6.1-89.1
php5-calendar-5.6.1-89.1
php5-readline-debuginfo-5.6.1-89.1
php5-sqlite-debuginfo-5.6.1-89.1
php5-dom-5.6.1-89.1
php5-imap-debuginfo-5.6.1-89.1
php5-curl-debuginfo-5.6.1-89.1
php5-mbstring-5.6.1-89.1
php5-xmlreader-debuginfo-5.6.1-89.1
php5-zlib-debuginfo-5.6.1-89.1
php5-ctype-debuginfo-5.6.1-89.1
php5-ldap-5.6.1-89.1
php5-mssql-debuginfo-5.6.1-89.1
php5-bz2-debuginfo-5.6.1-89.1
php5-zip-5.6.1-89.1
php5-calendar-debuginfo-5.6.1-89.1
php5-mcrypt-debuginfo-5.6.1-89.1
php5-dba-debuginfo-5.6.1-89.1
php5-odbc-debuginfo-5.6.1-89.1
php5-iconv-debuginfo-5.6.1-89.1
php5-ftp-debuginfo-5.6.1-89.1
php5-wddx-5.6.1-89.1
php5-json-debuginfo-5.6.1-89.1
php5-gmp-5.6.1-89.1
php5-tokenizer-5.6.1-89.1
php5-dba-5.6.1-89.1
php5-xmlrpc-5.6.1-89.1
php5-exif-debuginfo-5.6.1-89.1
php5-odbc-5.6.1-89.1
php5-zip-debuginfo-5.6.1-89.1
php5-fastcgi-5.6.1-89.1
php5-snmp-5.6.1-89.1
php5-enchanted-5.6.1-89.1
php5-ldap-debuginfo-5.6.1-89.1

php5-pgsql-debuginfo-5.6.1-89.1
apache2-mod_php5-debuginfo-5.6.1-89.1
php5-sockets-debuginfo-5.6.1-89.1
php5-json-5.6.1-89.1
php5-bcmath-debuginfo-5.6.1-89.1
php5-tidy-5.6.1-89.1
php5-enchanted-debuginfo-5.6.1-89.1
php5-5.6.1-89.1
php5-zlib-5.6.1-89.1
php5-xmlwriter-debuginfo-5.6.1-89.1
php5-exif-5.6.1-89.1
php5-sysvshm-debuginfo-5.6.1-89.1
php5-sysvshm-5.6.1-89.1
php5-xmlwriter-5.6.1-89.1
php5-openssl-debuginfo-5.6.1-89.1
php5-debuginfo-5.6.1-89.1
php5-snmp-debuginfo-5.6.1-89.1
apache2-mod_php5-5.6.1-89.1
php5-sysvmsg-debuginfo-5.6.1-89.1
php5-bz2-5.6.1-89.1
php5-gmp-debuginfo-5.6.1-89.1
php5-shmop-5.6.1-89.1
php5-gd-debuginfo-5.6.1-89.1
php5-mssql-5.6.1-89.1
php5-fileinfo-debuginfo-5.6.1-89.1
php5-ftp-5.6.1-89.1
php5-sysvsem-5.6.1-89.1
php5-intl-5.6.1-89.1
php5-fpm-5.6.1-89.1
php5-sysvsem-debuginfo-5.6.1-89.1
php5-ctype-5.6.1-89.1
php5-pgsql-5.6.1-89.1
php5-gettext-5.6.1-89.1
php5-firebird-5.6.1-89.1
php5-soap-5.6.1-89.1
php5-tidy-debuginfo-5.6.1-89.1
php5-mcrypt-5.6.1-89.1
php5-pspell-5.6.1-89.1
php5-xsl-5.6.1-89.1
php5-dom-debuginfo-5.6.1-89.1

145107 - SuSE Linux 13.2 openSUSE-SU-2016:3238-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8866, CVE-2016-9830

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:3238-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00141.html>

SuSE Linux 13.2

x86_64
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-21.1
libGraphicsMagick-Q16-3-1.3.20-21.1
GraphicsMagick-debuginfo-1.3.20-21.1
libGraphicsMagickWand-Q16-2-1.3.20-21.1
libGraphicsMagick3-config-1.3.20-21.1
GraphicsMagick-debugsource-1.3.20-21.1
libGraphicsMagick-Q16-3-debuginfo-1.3.20-21.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-21.1
libGraphicsMagick++-devel-1.3.20-21.1
perl-GraphicsMagick-1.3.20-21.1
GraphicsMagick-1.3.20-21.1
perl-GraphicsMagick-debuginfo-1.3.20-21.1
libGraphicsMagick++-Q16-3-1.3.20-21.1
GraphicsMagick-devel-1.3.20-21.1

i586
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-21.1
libGraphicsMagick-Q16-3-1.3.20-21.1
GraphicsMagick-debuginfo-1.3.20-21.1
libGraphicsMagickWand-Q16-2-1.3.20-21.1
libGraphicsMagick3-config-1.3.20-21.1
GraphicsMagick-debugsource-1.3.20-21.1
libGraphicsMagick-Q16-3-debuginfo-1.3.20-21.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-21.1
libGraphicsMagick++-devel-1.3.20-21.1
perl-GraphicsMagick-1.3.20-21.1
GraphicsMagick-1.3.20-21.1
perl-GraphicsMagick-debuginfo-1.3.20-21.1
libGraphicsMagick++-Q16-3-1.3.20-21.1
GraphicsMagick-devel-1.3.20-21.1

145108 - SuSE SLES 11 SP4 SUSE-SU-2016:3210-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3210-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002507.html>

SuSE SLES 11 SP4

i586
MozillaFirefox-45.6.0esr-62.1
MozillaFirefox-translations-45.6.0esr-62.1

x86_64
MozillaFirefox-45.6.0esr-62.1
MozillaFirefox-translations-45.6.0esr-62.1

145110 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3211-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9933

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3211-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002508.html>

SuSE SLED 12 SP2

x86_64

gd-debuginfo-2.1.0-20.1

gd-debuginfo-32bit-2.1.0-20.1

gd-2.1.0-20.1

gd-debugsource-2.1.0-20.1

gd-32bit-2.1.0-20.1

SuSE SLES 12 SP2

x86_64

gd-2.1.0-20.1

gd-debugsource-2.1.0-20.1

gd-debuginfo-2.1.0-20.1

SuSE SLES 12 SP1

x86_64

gd-2.1.0-20.1

gd-debugsource-2.1.0-20.1

gd-debuginfo-2.1.0-20.1

SuSE SLED 12 SP1

x86_64

gd-debuginfo-2.1.0-20.1

gd-debuginfo-32bit-2.1.0-20.1

gd-2.1.0-20.1

gd-debugsource-2.1.0-20.1

gd-32bit-2.1.0-20.1

145111 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:3271-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2123, CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3271-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002526.html>

SuSE SLED 12 SP2

x86_64

libdcerpc-binding0-32bit-4.4.2-31.1
libndr-nbt0-debuginfo-4.4.2-31.1
libsamba-hostconfig0-debuginfo-32bit-4.4.2-31.1
libdcerpc-binding0-debuginfo-4.4.2-31.1
libsmbclient0-32bit-4.4.2-31.1
libtevent-util0-debuginfo-32bit-4.4.2-31.1
libsmbldap0-4.4.2-31.1
libsmbconf0-debuginfo-4.4.2-31.1
libsmbldap0-debuginfo-4.4.2-31.1
libndr-krb5pac0-32bit-4.4.2-31.1
libndr0-32bit-4.4.2-31.1
libsamba-credentials0-debuginfo-32bit-4.4.2-31.1
libtevent-util0-debuginfo-4.4.2-31.1
libdcerpc0-4.4.2-31.1
samba-4.4.2-31.1
libndr-standard0-debuginfo-4.4.2-31.1
libsamba-credentials0-debuginfo-4.4.2-31.1
samba-libs-32bit-4.4.2-31.1
libndr-nbt0-4.4.2-31.1
libsamba-passsdb0-debuginfo-4.4.2-31.1
libsamba-util0-debuginfo-4.4.2-31.1
libndr-standard0-32bit-4.4.2-31.1
samba-libs-4.4.2-31.1
libndr-krb5pac0-4.4.2-31.1
libsmbconf0-debuginfo-32bit-4.4.2-31.1
libndr-nbt0-32bit-4.4.2-31.1
libsmbconf0-32bit-4.4.2-31.1
samba-winbind-debuginfo-32bit-4.4.2-31.1
libnetapi0-debuginfo-32bit-4.4.2-31.1
libsamdb0-debuginfo-32bit-4.4.2-31.1
samba-libs-debuginfo-4.4.2-31.1
libndr-krb5pac0-debuginfo-4.4.2-31.1
libndr0-4.4.2-31.1
libsamba-util0-32bit-4.4.2-31.1
libdcerpc0-debuginfo-4.4.2-31.1
libsmbldap0-32bit-4.4.2-31.1
libwbclient0-debuginfo-32bit-4.4.2-31.1
libndr-standard0-4.4.2-31.1
libndr0-debuginfo-32bit-4.4.2-31.1
samba-winbind-32bit-4.4.2-31.1
samba-debugsource-4.4.2-31.1
libsmbldap0-debuginfo-32bit-4.4.2-31.1
samba-client-debuginfo-4.4.2-31.1
libtevent-util0-4.4.2-31.1
libsamdb0-debuginfo-4.4.2-31.1
samba-winbind-debuginfo-4.4.2-31.1
libsamba-errors0-debuginfo-32bit-4.4.2-31.1
libsmbconf0-4.4.2-31.1
libsamba-credentials0-4.4.2-31.1
libwbclient0-32bit-4.4.2-31.1
libsamba-passsdb0-4.4.2-31.1
libsamba-hostconfig0-32bit-4.4.2-31.1
libdcerpc0-debuginfo-32bit-4.4.2-31.1
libsmbclient0-debuginfo-4.4.2-31.1

libnetapi0-32bit-4.4.2-31.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-31.1
libndr-standard0-debuginfo-32bit-4.4.2-31.1
samba-client-32bit-4.4.2-31.1
libsamba-passdb0-32bit-4.4.2-31.1
libsmbclient0-debuginfo-32bit-4.4.2-31.1
libwbclient0-4.4.2-31.1
libdcerpc0-32bit-4.4.2-31.1
samba-winbind-4.4.2-31.1
libndr0-debuginfo-4.4.2-31.1
libsamba-credentials0-32bit-4.4.2-31.1
libsamba-hostconfig0-debuginfo-4.4.2-31.1
samba-client-debuginfo-32bit-4.4.2-31.1
libsamba-util0-4.4.2-31.1
libsamba-errors0-debuginfo-4.4.2-31.1
libtevent-util0-32bit-4.4.2-31.1
libsamba-hostconfig0-4.4.2-31.1
samba-libs-debuginfo-32bit-4.4.2-31.1
libwbclient0-debuginfo-4.4.2-31.1
libndr-nbt0-debuginfo-32bit-4.4.2-31.1
samba-debuginfo-4.4.2-31.1
libsamdb0-32bit-4.4.2-31.1
libndr-krb5pac0-debuginfo-32bit-4.4.2-31.1
libnetapi0-debuginfo-4.4.2-31.1
libsmbclient0-4.4.2-31.1
libdcerpc-binding0-4.4.2-31.1
libsamba-passdb0-debuginfo-32bit-4.4.2-31.1
libsamba-util0-debuginfo-32bit-4.4.2-31.1
libnetapi0-4.4.2-31.1
libsamba-errors0-4.4.2-31.1
libsamba-errors0-32bit-4.4.2-31.1
samba-client-4.4.2-31.1
libsamdb0-4.4.2-31.1

noarch
samba-doc-4.4.2-31.1

SuSE SLES 12 SP2
noarch
samba-doc-4.4.2-31.1

x86_64
libndr-nbt0-32bit-4.4.2-31.1
libdcerpc-binding0-32bit-4.4.2-31.1
libndr-nbt0-debuginfo-4.4.2-31.1
libsamba-hostconfig0-debuginfo-32bit-4.4.2-31.1
libdcerpc-binding0-debuginfo-4.4.2-31.1
libsmbclient0-32bit-4.4.2-31.1
libtevent-util0-debuginfo-32bit-4.4.2-31.1
libsmbldap0-4.4.2-31.1
libsmbconf0-debuginfo-4.4.2-31.1
libsmbldap0-debuginfo-4.4.2-31.1
libndr-krb5pac0-32bit-4.4.2-31.1
libndr0-32bit-4.4.2-31.1
libsamba-credentials0-debuginfo-32bit-4.4.2-31.1
libtevent-util0-debuginfo-4.4.2-31.1
libdcerpc0-4.4.2-31.1
samba-4.4.2-31.1
libndr-standard0-debuginfo-4.4.2-31.1
samba-libs-32bit-4.4.2-31.1

libndr-nbt0-4.4.2-31.1
libsamba-passdb0-debuginfo-4.4.2-31.1
libndr-standard0-32bit-4.4.2-31.1
samba-libs-4.4.2-31.1
libsmbconf0-debuginfo-32bit-4.4.2-31.1
libndr0-4.4.2-31.1
libsmbclient0-debuginfo-4.4.2-31.1
libsmbconf0-32bit-4.4.2-31.1
samba-winbind-debuginfo-32bit-4.4.2-31.1
libnetapi0-debuginfo-32bit-4.4.2-31.1
libsamdb0-debuginfo-32bit-4.4.2-31.1
libndr-krb5pac0-debuginfo-4.4.2-31.1
libndr-krb5pac0-4.4.2-31.1
libsamba-util0-32bit-4.4.2-31.1
libdcerpc0-debuginfo-4.4.2-31.1
libsmbldap0-32bit-4.4.2-31.1
libwbclient0-debuginfo-32bit-4.4.2-31.1
libndr-standard0-4.4.2-31.1
samba-libs-debuginfo-4.4.2-31.1
libtevent-util0-32bit-4.4.2-31.1
samba-debugsource-4.4.2-31.1
libsamba-util0-debuginfo-4.4.2-31.1
samba-client-debuginfo-4.4.2-31.1
libsamdb0-debuginfo-4.4.2-31.1
libsmbldap0-debuginfo-32bit-4.4.2-31.1
samba-winbind-debuginfo-4.4.2-31.1
libsmbconf0-4.4.2-31.1
libsamba-credentials0-4.4.2-31.1
libwbclient0-32bit-4.4.2-31.1
libsamba-passdb0-4.4.2-31.1
libsamba-hostconfig0-32bit-4.4.2-31.1
libdcerpc0-debuginfo-32bit-4.4.2-31.1
libwbclient0-4.4.2-31.1
libnetapi0-32bit-4.4.2-31.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-31.1
libndr0-debuginfo-32bit-4.4.2-31.1
libndr-standard0-debuginfo-32bit-4.4.2-31.1
samba-client-32bit-4.4.2-31.1
libsamba-passdb0-32bit-4.4.2-31.1
libsamba-hostconfig0-debuginfo-4.4.2-31.1
libsmbclient0-debuginfo-32bit-4.4.2-31.1
libdcerpc0-32bit-4.4.2-31.1
samba-winbind-4.4.2-31.1
libndr0-debuginfo-4.4.2-31.1
libsamba-credentials0-32bit-4.4.2-31.1
libtevent-util0-4.4.2-31.1
samba-client-debuginfo-32bit-4.4.2-31.1
libsamba-util0-4.4.2-31.1
libsamba-errors0-debuginfo-4.4.2-31.1
libsamba-errors0-debuginfo-32bit-4.4.2-31.1
libsamba-hostconfig0-4.4.2-31.1
libsamdb0-32bit-4.4.2-31.1
samba-libs-debuginfo-32bit-4.4.2-31.1
libwbclient0-debuginfo-4.4.2-31.1
libndr-nbt0-debuginfo-32bit-4.4.2-31.1
samba-debuginfo-4.4.2-31.1
libsamba-credentials0-debuginfo-4.4.2-31.1
libndr-krb5pac0-debuginfo-32bit-4.4.2-31.1
libnetapi0-debuginfo-4.4.2-31.1
samba-winbind-32bit-4.4.2-31.1

libsmbclient0-4.4.2-31.1
libdcerpc-binding0-4.4.2-31.1
libsamba-passdb0-debuginfo-32bit-4.4.2-31.1
libsamba-util0-debuginfo-32bit-4.4.2-31.1
libnetapi0-4.4.2-31.1
libsamba-errors0-4.4.2-31.1
libsamba-errors0-32bit-4.4.2-31.1
samba-client-4.4.2-31.1
libsamdb0-4.4.2-31.1

145112 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3272-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2123, CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3272-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002527.html>

SuSE SLED 12 SP1

x86_64

libsmbclient0-4.2.4-28.3.1
libndr0-debuginfo-4.2.4-28.3.1
libsmbconf0-32bit-4.2.4-28.3.1
libdcerpc0-4.2.4-28.3.1
libndr-nbt0-debuginfo-32bit-4.2.4-28.3.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-28.3.1
libsamba-passdb0-32bit-4.2.4-28.3.1
libndr-nbt0-4.2.4-28.3.1
libsmbclient-raw0-4.2.4-28.3.1
libwbclient0-debuginfo-4.2.4-28.3.1
libndr-standard0-debuginfo-4.2.4-28.3.1
samba-client-32bit-4.2.4-28.3.1
libregistry0-debuginfo-4.2.4-28.3.1
samba-libs-32bit-4.2.4-28.3.1
samba-libs-debuginfo-32bit-4.2.4-28.3.1
samba-client-4.2.4-28.3.1
libndr-nbt0-debuginfo-4.2.4-28.3.1
libsamba-util0-debuginfo-32bit-4.2.4-28.3.1
libdcerpc0-debuginfo-32bit-4.2.4-28.3.1
libsmbclient0-debuginfo-4.2.4-28.3.1
libnetapi0-4.2.4-28.3.1
samba-client-debuginfo-4.2.4-28.3.1
libtevent-util0-debuginfo-4.2.4-28.3.1
libsamba-hostconfig0-32bit-4.2.4-28.3.1
libsamdb0-32bit-4.2.4-28.3.1
libndr-standard0-debuginfo-32bit-4.2.4-28.3.1
libtevent-util0-debuginfo-32bit-4.2.4-28.3.1
samba-4.2.4-28.3.1
samba-client-debuginfo-32bit-4.2.4-28.3.1
libsamdb0-4.2.4-28.3.1

libnetapi0-debuginfo-4.2.4-28.3.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-28.3.1
libwbclient0-debuginfo-32bit-4.2.4-28.3.1
libsmbconf0-4.2.4-28.3.1
samba-debuginfo-32bit-4.2.4-28.3.1
libndr-nbt0-32bit-4.2.4-28.3.1
libsamba-credentials0-4.2.4-28.3.1
libwbclient0-32bit-4.2.4-28.3.1
libdcerpc0-debuginfo-4.2.4-28.3.1
libndr0-debuginfo-32bit-4.2.4-28.3.1
libsamba-util0-32bit-4.2.4-28.3.1
samba-debuginfo-4.2.4-28.3.1
libregistry0-4.2.4-28.3.1
libsamba-hostconfig0-debuginfo-4.2.4-28.3.1
samba-32bit-4.2.4-28.3.1
libsamba-credentials0-debuginfo-32bit-4.2.4-28.3.1
libwbclient0-4.2.4-28.3.1
libsamba-credentials0-32bit-4.2.4-28.3.1
libndr-krb5pac0-debuginfo-32bit-4.2.4-28.3.1
libsamba-passdb0-debuginfo-4.2.4-28.3.1
samba-winbind-debuginfo-4.2.4-28.3.1
libndr0-4.2.4-28.3.1
samba-debugsource-4.2.4-28.3.1
libsmbldap0-32bit-4.2.4-28.3.1
libsmbconf0-debuginfo-32bit-4.2.4-28.3.1
libndr-krb5pac0-4.2.4-28.3.1
libsmbconf0-debuginfo-4.2.4-28.3.1
libgensec0-32bit-4.2.4-28.3.1
libsmbldap0-debuginfo-4.2.4-28.3.1
libsmbclient-raw0-debuginfo-4.2.4-28.3.1
libsmbldap0-debuginfo-32bit-4.2.4-28.3.1
libsamba-passdb0-debuginfo-32bit-4.2.4-28.3.1
libgensec0-debuginfo-32bit-4.2.4-28.3.1
libdcerpc0-32bit-4.2.4-28.3.1
libndr-krb5pac0-32bit-4.2.4-28.3.1
samba-libs-4.2.4-28.3.1
libndr-krb5pac0-debuginfo-4.2.4-28.3.1
libdcerpc-binding0-debuginfo-4.2.4-28.3.1
samba-libs-debuginfo-4.2.4-28.3.1
libtevent-util0-32bit-4.2.4-28.3.1
libgensec0-4.2.4-28.3.1
libsmbclient-raw0-32bit-4.2.4-28.3.1
samba-winbind-debuginfo-32bit-4.2.4-28.3.1
libsamba-credentials0-debuginfo-4.2.4-28.3.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-28.3.1
libndr-standard0-4.2.4-28.3.1
libnetapi0-32bit-4.2.4-28.3.1
libsmbclient0-32bit-4.2.4-28.3.1
libsamdb0-debuginfo-4.2.4-28.3.1
libsmbclient0-debuginfo-32bit-4.2.4-28.3.1
libsmbldap0-4.2.4-28.3.1
samba-winbind-32bit-4.2.4-28.3.1
libsamba-util0-debuginfo-4.2.4-28.3.1
libdcerpc-binding0-4.2.4-28.3.1
libtevent-util0-4.2.4-28.3.1
libgensec0-debuginfo-4.2.4-28.3.1
libsamba-util0-4.2.4-28.3.1
libsamdb0-debuginfo-32bit-4.2.4-28.3.1
libdcerpc-binding0-32bit-4.2.4-28.3.1
libnetapi0-debuginfo-32bit-4.2.4-28.3.1

libsamba-passdb0-4.2.4-28.3.1
samba-winbind-4.2.4-28.3.1
libndr0-32bit-4.2.4-28.3.1
libsamba-hostconfig0-4.2.4-28.3.1
libndr-standard0-32bit-4.2.4-28.3.1

noarch
samba-doc-4.2.4-28.3.1

SuSE SLES 12 SP2
x86_64
libdcerpc-at svc0-4.2.4-28.3.1
libdcerpc-at svc0-debuginfo-4.2.4-28.3.1

SuSE SLED 12 SP2
x86_64
libdcerpc-at svc0-4.2.4-28.3.1
libdcerpc-at svc0-debuginfo-4.2.4-28.3.1

SuSE SLES 12 SP1
noarch
samba-doc-4.2.4-28.3.1

x86_64
libsmbclient0-4.2.4-28.3.1
libndr0-debuginfo-4.2.4-28.3.1
libsmbconf0-32bit-4.2.4-28.3.1
libdcerpc0-4.2.4-28.3.1
libndr-nbt0-debuginfo-32bit-4.2.4-28.3.1
libsamba-hostconfig0-4.2.4-28.3.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-28.3.1
libsamba-passdb0-32bit-4.2.4-28.3.1
libndr-nbt0-4.2.4-28.3.1
libsmbclient-raw0-4.2.4-28.3.1
libndr-standard0-debuginfo-4.2.4-28.3.1
samba-client-32bit-4.2.4-28.3.1
libregistry0-debuginfo-4.2.4-28.3.1
samba-libs-32bit-4.2.4-28.3.1
samba-libs-debuginfo-32bit-4.2.4-28.3.1
samba-client-4.2.4-28.3.1
libndr-nbt0-debuginfo-4.2.4-28.3.1
libsamba-util0-debuginfo-32bit-4.2.4-28.3.1
libdcerpc0-debuginfo-32bit-4.2.4-28.3.1
libsmbclient0-debuginfo-4.2.4-28.3.1
libnetapi0-4.2.4-28.3.1
libsmbclient-raw0-32bit-4.2.4-28.3.1
libsmbclient0-debuginfo-32bit-4.2.4-28.3.1
samba-client-debuginfo-4.2.4-28.3.1
libnetapi0-32bit-4.2.4-28.3.1
libsamba-hostconfig0-32bit-4.2.4-28.3.1
libsamdb0-32bit-4.2.4-28.3.1
libndr-standard0-debuginfo-32bit-4.2.4-28.3.1
libtevent-util0-debuginfo-32bit-4.2.4-28.3.1
samba-client-debuginfo-32bit-4.2.4-28.3.1
libsamdb0-4.2.4-28.3.1
libnetapi0-debuginfo-4.2.4-28.3.1
libwbclient0-debuginfo-32bit-4.2.4-28.3.1
libsmbconf0-4.2.4-28.3.1
samba-debuginfo-32bit-4.2.4-28.3.1
libndr-krb5pac0-32bit-4.2.4-28.3.1

libsamba-credentials0-4.2.4-28.3.1
libwbclient0-32bit-4.2.4-28.3.1
libndr0-debuginfo-32bit-4.2.4-28.3.1
libsamba-util0-32bit-4.2.4-28.3.1
samba-debuginfo-4.2.4-28.3.1
libsamba-util0-debuginfo-4.2.4-28.3.1
libregistry0-4.2.4-28.3.1
libsamba-hostconfig0-debuginfo-4.2.4-28.3.1
samba-32bit-4.2.4-28.3.1
libsamba-credentials0-debuginfo-32bit-4.2.4-28.3.1
libwbclient0-4.2.4-28.3.1
libsamba-credentials0-32bit-4.2.4-28.3.1
libsamba-passdb0-debuginfo-4.2.4-28.3.1
samba-winbind-debuginfo-4.2.4-28.3.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-28.3.1
libndr0-4.2.4-28.3.1
samba-debugsource-4.2.4-28.3.1
libsmbldap0-32bit-4.2.4-28.3.1
libsmbconf0-debuginfo-32bit-4.2.4-28.3.1
libndr-krb5pac0-4.2.4-28.3.1
libsmbconf0-debuginfo-4.2.4-28.3.1
libwbclient0-debuginfo-4.2.4-28.3.1
libsmbldap0-debuginfo-4.2.4-28.3.1
libsmbclient-raw0-debuginfo-4.2.4-28.3.1
libsmbldap0-debuginfo-32bit-4.2.4-28.3.1
libsamba-passdb0-debuginfo-32bit-4.2.4-28.3.1
libgensec0-debuginfo-32bit-4.2.4-28.3.1
libdcerpc0-32bit-4.2.4-28.3.1
libndr-nbt0-32bit-4.2.4-28.3.1
samba-libs-4.2.4-28.3.1
libndr-krb5pac0-debuginfo-4.2.4-28.3.1
libdcerpc-binding0-debuginfo-4.2.4-28.3.1
samba-libs-debuginfo-4.2.4-28.3.1
libtevent-util0-32bit-4.2.4-28.3.1
libgensec0-4.2.4-28.3.1
samba-4.2.4-28.3.1
samba-winbind-debuginfo-32bit-4.2.4-28.3.1
libsamba-credentials0-debuginfo-4.2.4-28.3.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-28.3.1
libndr-standard0-4.2.4-28.3.1
libgensec0-32bit-4.2.4-28.3.1
libtevent-util0-debuginfo-4.2.4-28.3.1
libsmbclient0-32bit-4.2.4-28.3.1
libdcerpc0-debuginfo-4.2.4-28.3.1
libsmbldap0-4.2.4-28.3.1
samba-winbind-32bit-4.2.4-28.3.1
libndr-krb5pac0-debuginfo-32bit-4.2.4-28.3.1
libdcerpc-binding0-4.2.4-28.3.1
libtevent-util0-4.2.4-28.3.1
libgensec0-debuginfo-4.2.4-28.3.1
libsamba-util0-4.2.4-28.3.1
libsamdb0-debuginfo-32bit-4.2.4-28.3.1
libdcerpc-binding0-32bit-4.2.4-28.3.1
libnetapi0-debuginfo-32bit-4.2.4-28.3.1
libsamba-passdb0-4.2.4-28.3.1
samba-winbind-4.2.4-28.3.1

145114 - SuSE SLES 11 SP4 SUSE-SU-2016:3221-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10013, CVE-2016-10024, CVE-2016-9932

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3221-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002510.html>

SuSE SLES 11 SP4

x86_64
xen-libs-32bit-4.4.4_12-46.1
xen-libs-4.4.4_12-46.1
xen-doc-html-4.4.4_12-46.1
xen-kmp-default-4.4.4_12_3.0.101_91-46.1
xen-tools-domU-4.4.4_12-46.1
xen-4.4.4_12-46.1
xen-tools-4.4.4_12-46.1

i586

xen-tools-domU-4.4.4_12-46.1
xen-libs-4.4.4_12-46.1
xen-kmp-pae-4.4.4_12_3.0.101_91-46.1
xen-kmp-default-4.4.4_12_3.0.101_91-46.1

145115 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3222-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9904, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3222-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002511.html>

SuSE SLED 12 SP1

x86_64
MozillaFirefox-debugsource-45.6.0esr-96.1
MozillaFirefox-45.6.0esr-96.1
MozillaFirefox-debuginfo-45.6.0esr-96.1
MozillaFirefox-translations-45.6.0esr-96.1

SuSE SLES 12 SP2

x86_64
MozillaFirefox-debugsource-45.6.0esr-96.1
MozillaFirefox-45.6.0esr-96.1

MozillaFirefox-debuginfo-45.6.0esr-96.1
MozillaFirefox-translations-45.6.0esr-96.1

SuSE SLED 12 SP2

x86_64
MozillaFirefox-debugsource-45.6.0esr-96.1
MozillaFirefox-45.6.0esr-96.1
MozillaFirefox-debuginfo-45.6.0esr-96.1
MozillaFirefox-translations-45.6.0esr-96.1

SuSE SLES 12 SP1

x86_64
MozillaFirefox-debugsource-45.6.0esr-96.1
MozillaFirefox-45.6.0esr-96.1
MozillaFirefox-debuginfo-45.6.0esr-96.1
MozillaFirefox-translations-45.6.0esr-96.1

145116 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3250-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9957, CVE-2016-9958, CVE-2016-9959, CVE-2016-9960, CVE-2016-9961

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3250-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002517.html>

SuSE SLED 12 SP1

x86_64
libgme0-debuginfo-0.6.0-5.1
libgme0-0.6.0-5.1
libgme-debugsource-0.6.0-5.1

SuSE SLES 12 SP2

x86_64
libgme0-debuginfo-0.6.0-5.1
libgme0-0.6.0-5.1
libgme-debugsource-0.6.0-5.1

SuSE SLED 12 SP2

x86_64
libgme0-debuginfo-0.6.0-5.1
libgme0-0.6.0-5.1
libgme-debugsource-0.6.0-5.1

SuSE SLES 12 SP1

x86_64
libgme0-debuginfo-0.6.0-5.1
libgme0-0.6.0-5.1
libgme-debugsource-0.6.0-5.1

145117 - SuSE SLES 11 SP4 SUSE-SU-2016:3251-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9933

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3251-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002518.html>

SuSE SLES 11 SP4
i586
gd-2.0.36.RC1-52.29.1

x86_64
gd-2.0.36.RC1-52.29.1

145120 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:3208-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10013, CVE-2016-10024, CVE-2016-10025, CVE-2016-9932

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3208-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002505.html>

SuSE SLED 12 SP2
x86_64
xen-libs-32bit-4.7.1_04-28.1
xen-libs-debuginfo-4.7.1_04-28.1
xen-4.7.1_04-28.1
xen-debugsource-4.7.1_04-28.1
xen-libs-debuginfo-32bit-4.7.1_04-28.1
xen-libs-4.7.1_04-28.1

SuSE SLES 12 SP2
x86_64
xen-doc-html-4.7.1_04-28.1
xen-tools-4.7.1_04-28.1
xen-tools-domU-debuginfo-4.7.1_04-28.1
xen-libs-32bit-4.7.1_04-28.1
xen-tools-debuginfo-4.7.1_04-28.1
xen-libs-debuginfo-4.7.1_04-28.1

xen-4.7.1_04-28.1
xen-tools-domU-4.7.1_04-28.1
xen-debugsource-4.7.1_04-28.1
xen-libs-debuginfo-32bit-4.7.1_04-28.1
xen-libs-4.7.1_04-28.1

145122 - SuSE SLES 11 SP4 SUSE-SU-2016:3209-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3209-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002506.html>

SuSE SLES 11 SP4
i586
zlib-1.2.7-0.14.1

x86_64
zlib-1.2.7-0.14.1
zlib-32bit-1.2.7-0.14.1

160182 - CentOS 6 CESA-2016-2974 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9445, CVE-2016-9447

Description

The scan detected that the host is missing the following update:
CESA-2016-2974

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-December/022189.html>

CentOS 6
x86_64
gstreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gstreamer-plugins-bad-free-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-0.10.19-5.el6_8

i686
gstreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8

gststreamer-plugins-bad-free-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-0.10.19-5.el6_8

160183 - CentOS 5, 6, 7 CESA-2016-2973 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
CESA-2016-2973

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-December/022183.html>
<http://lists.centos.org/pipermail/centos-announce/2016-December/022186.html>
<http://lists.centos.org/pipermail/centos-announce/2016-December/022184.html>

CentOS 6
x86_64
thunderbird-45.6.0-1.el6.centos

i686
thunderbird-45.6.0-1.el6.centos

CentOS 7
x86_64
thunderbird-45.6.0-1.el7.centos

CentOS 5
x86_64
thunderbird-45.6.0-1.el5.centos

i386
thunderbird-45.6.0-1.el5.centos

160184 - CentOS 6 CESA-2016-2975 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808

Description

The scan detected that the host is missing the following update:
CESA-2016-2975

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-December/022188.html>

CentOS 6

x86_64
gstreamer-plugins-good-devel-0.10.23-4.el6_8
gstreamer-plugins-good-0.10.23-4.el6_8

i686
gstreamer-plugins-good-devel-0.10.23-4.el6_8
gstreamer-plugins-good-0.10.23-4.el6_8

163244 - Oracle Enterprise Linux ELSA-2016-2974 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9445, CVE-2016-9447

Description

The scan detected that the host is missing the following update:
ELSA-2016-2974

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006596.html>

OEL6
x86_64
gstreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gstreamer-plugins-bad-free-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-0.10.19-5.el6_8

i386
gstreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gstreamer-plugins-bad-free-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-0.10.19-5.el6_8

163245 - Oracle Enterprise Linux ELSA-2016-2973 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9905

Description

The scan detected that the host is missing the following update:
ELSA-2016-2973

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006595.html>
<http://oss.oracle.com/pipermail/el-errata/2016-December/006594.html>

OEL7
x86_64

thunderbird-45.6.0-1.0.1.el7_3

OEL6

x86_64

thunderbird-45.6.0-1.0.1.el6_8

i386

thunderbird-45.6.0-1.0.1.el6_8

163246 - Oracle Enterprise Linux ELSA-2016-2963 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9637

Description

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

ELSA-2016-2963

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-December/006589.html>

OEL5

i386

xen-libs-3.0.3-148.el5_11

xen-devel-3.0.3-148.el5_11

xen-3.0.3-148.el5_11

x86_64

xen-libs-3.0.3-148.el5_11

xen-devel-3.0.3-148.el5_11

xen-3.0.3-148.el5_11

163248 - Oracle Enterprise Linux ELSA-2016-2975 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808

Description

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

ELSA-2016-2975

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-December/006597.html>

OEL6

x86_64

gststreamer-plugins-good-devel-0.10.23-4.el6_8

gststreamer-plugins-good-0.10.23-4.el6_8

i386
gstreamer-plugins-good-devel-0.10.23-4.el6_8
gstreamer-plugins-good-0.10.23-4.el6_8

175084 - Scientific Linux Security ERRATA Important: gstreamer-plugins-good on SL6.x i386/x86_64 (1612-18190)

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808

Description

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

Security ERRATA Important: gstreamer-plugins-good on SL6.x i386/x86_64 (1612-18190)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=18190>

SL6
x86_64
gstreamer-plugins-good-0.10.23-4.el6_8
gstreamer-plugins-good-devel-0.10.23-4.el6_8
gstreamer-plugins-good-debuginfo-0.10.23-4.el6_8

i386
gstreamer-plugins-good-0.10.23-4.el6_8
gstreamer-plugins-good-devel-0.10.23-4.el6_8
gstreamer-plugins-good-debuginfo-0.10.23-4.el6_8

175086 - Scientific Linux Security ERRATA Important: gstreamer-plugins-bad-free on SL6.x i386/x86_64 (1612-17802)

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

Risk Level: High

CVE: CVE-2016-9445, CVE-2016-9447

Description

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

Security ERRATA Important: gstreamer-plugins-bad-free on SL6.x i386/x86_64 (1612-17802)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=17802>

SL6
x86_64
gstreamer-plugins-bad-free-debuginfo-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gstreamer-plugins-bad-free-0.10.19-5.el6_8
gstreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gstreamer-plugins-bad-free-devel-0.10.19-5.el6_8

i386

gststreamer-plugins-bad-free-debuginfo-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-docs-0.10.19-5.el6_8
gststreamer-plugins-bad-free-0.10.19-5.el6_8
gststreamer-plugins-bad-free-extras-0.10.19-5.el6_8
gststreamer-plugins-bad-free-devel-0.10.19-5.el6_8

175087 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-18951)

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

Risk Level: High

CVE: CVE-2016-9893, CVE-2016-9895, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9905

Description

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

Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1612-18951)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=18951>

SL5

x86_64
thunderbird-45.6.0-1.el5_11
thunderbird-debuginfo-45.6.0-1.el5_11

i386

thunderbird-45.6.0-1.el5_11
thunderbird-debuginfo-45.6.0-1.el5_11

SL7

x86_64
thunderbird-45.6.0-1.el7_3
thunderbird-debuginfo-45.6.0-1.el7_3

SL6

x86_64
thunderbird-45.6.0-1.el6_8
thunderbird-debuginfo-45.6.0-1.el6_8

i386

thunderbird-45.6.0-1.el6_8
thunderbird-debuginfo-45.6.0-1.el6_8

182221 - FreeBSD Joomla! Multiple Vulnerabilities (624b45c0-c7f3-11e6-ae1b-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-9836, CVE-2016-9837, CVE-2016-9838

Description

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

Joomla! -- multiple vulnerabilities (624b45c0-c7f3-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/624b45c0-c7f3-11e6-ae1b-002590263bf5.html>

Affected packages:

1.6.0 <= joomla3 < 3.6.5

182223 - FreeBSD Joomla! Multiple Vulnerabilities (a27d234a-c7f2-11e6-ae1b-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-8869, CVE-2016-8870, CVE-2016-9081

Description

The scan detected that the host is missing the following update:
Joomla! -- multiple vulnerabilities (a27d234a-c7f2-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/a27d234a-c7f2-11e6-ae1b-002590263bf5.html>

Affected packages:

3.4.4 <= joomla3 < 3.6.4

191533 - Fedora Linux 25 FEDORA-2016-2d0c8ba781 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9036, CVE-2016-9037

Description

The scan detected that the host is missing the following update:
FEDORA-2016-2d0c8ba781

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

msgpuck-1.1.3-1.fc25

tarantool-1.6.9.52-1.fc25

191537 - Fedora Linux 24 FEDORA-2016-badd014afe Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9036, CVE-2016-9037

Description

The scan detected that the host is missing the following update:
FEDORA-2016-badd014afe

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

msgpuck-1.1.3-1.fc24
tarantool-1.6.9.52-1.fc24

21066 - IBM AIX bellmail Privilege Escalation Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-8972

Description

A vulnerability is present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

A vulnerability is present in some versions of IBM AIX. The flaw is due to improper handling of a specially crafted command within the bellmail client. Successful exploitation could allow a local attacker to gain root privileges.

132320 - Oracle VM OVMSA-2016-0182 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0182

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000610.html>

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000609.html>

OVM3.3
x86_64
vim-minimal-7.4.629-5.el6_8.1

OVM3.4
x86_64
vim-minimal-7.4.629-5.el6_8.1

141388 - Red Hat Enterprise Linux RHSA-2016-2972 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1248

Description

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

RHSA-2016-2972

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2972.html>

RHEL6S

i386

vim-filesystem-7.4.629-5.el6_8.1

vim-common-7.4.629-5.el6_8.1

vim-debuginfo-7.4.629-5.el6_8.1

vim-minimal-7.4.629-5.el6_8.1

vim-enhanced-7.4.629-5.el6_8.1

vim-X11-7.4.629-5.el6_8.1

x86_64

vim-filesystem-7.4.629-5.el6_8.1

vim-common-7.4.629-5.el6_8.1

vim-debuginfo-7.4.629-5.el6_8.1

vim-minimal-7.4.629-5.el6_8.1

vim-enhanced-7.4.629-5.el6_8.1

vim-X11-7.4.629-5.el6_8.1

RHEL6WS

x86_64

vim-filesystem-7.4.629-5.el6_8.1

vim-common-7.4.629-5.el6_8.1

vim-debuginfo-7.4.629-5.el6_8.1

vim-minimal-7.4.629-5.el6_8.1

vim-enhanced-7.4.629-5.el6_8.1

vim-X11-7.4.629-5.el6_8.1

i386

vim-filesystem-7.4.629-5.el6_8.1

vim-common-7.4.629-5.el6_8.1

vim-debuginfo-7.4.629-5.el6_8.1

vim-minimal-7.4.629-5.el6_8.1

vim-enhanced-7.4.629-5.el6_8.1

vim-X11-7.4.629-5.el6_8.1

RHEL7D

x86_64

vim-filesystem-7.4.160-1.el7_3.1

vim-minimal-7.4.160-1.el7_3.1

vim-common-7.4.160-1.el7_3.1

vim-X11-7.4.160-1.el7_3.1

vim-enhanced-7.4.160-1.el7_3.1

vim-debuginfo-7.4.160-1.el7_3.1

RHEL6D

x86_64

vim-filesystem-7.4.629-5.el6_8.1
vim-common-7.4.629-5.el6_8.1
vim-debuginfo-7.4.629-5.el6_8.1
vim-minimal-7.4.629-5.el6_8.1
vim-enhanced-7.4.629-5.el6_8.1
vim-X11-7.4.629-5.el6_8.1

i386

vim-filesystem-7.4.629-5.el6_8.1
vim-common-7.4.629-5.el6_8.1
vim-debuginfo-7.4.629-5.el6_8.1
vim-minimal-7.4.629-5.el6_8.1
vim-enhanced-7.4.629-5.el6_8.1
vim-X11-7.4.629-5.el6_8.1

RHEL7WS

x86_64

vim-filesystem-7.4.160-1.el7_3.1
vim-minimal-7.4.160-1.el7_3.1
vim-common-7.4.160-1.el7_3.1
vim-X11-7.4.160-1.el7_3.1
vim-enhanced-7.4.160-1.el7_3.1
vim-debuginfo-7.4.160-1.el7_3.1

145109 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:3270-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7445, CVE-2016-8332, CVE-2016-9112, CVE-2016-9113, CVE-2016-9114, CVE-2016-9115, CVE-2016-9116, CVE-2016-9117, CVE-2016-9118, CVE-2016-9572, CVE-2016-9573, CVE-2016-9580, CVE-2016-9581

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3270-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002525.html>

SuSE SLED 12 SP2

x86_64

openjpeg2-debuginfo-2.1.0-3.1
libopenjp2-7-debuginfo-2.1.0-3.1
openjpeg2-debugsource-2.1.0-3.1
libopenjp2-7-2.1.0-3.1

SuSE SLES 12 SP2

x86_64

openjpeg2-debuginfo-2.1.0-3.1
libopenjp2-7-debuginfo-2.1.0-3.1
openjpeg2-debugsource-2.1.0-3.1
libopenjp2-7-2.1.0-3.1

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

Risk Level: Medium

CVE: CVE-2014-9848, CVE-2016-8707, CVE-2016-8866, CVE-2016-9556, CVE-2016-9559, CVE-2016-9773

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3258-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002522.html>

SuSE SLED 12 SP2

x86_64

libMagickWand-6_Q16-1-debuginfo-6.8.8.1-54.1

libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-54.1

libMagick++-6_Q16-3-6.8.8.1-54.1

libMagickCore-6_Q16-1-6.8.8.1-54.1

ImageMagick-6.8.8.1-54.1

ImageMagick-debugsource-6.8.8.1-54.1

libMagick++-6_Q16-3-debuginfo-6.8.8.1-54.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-54.1

libMagickWand-6_Q16-1-6.8.8.1-54.1

libMagickCore-6_Q16-1-32bit-6.8.8.1-54.1

ImageMagick-debuginfo-6.8.8.1-54.1

SuSE SLES 12 SP2

x86_64

libMagickWand-6_Q16-1-debuginfo-6.8.8.1-54.1

libMagickCore-6_Q16-1-6.8.8.1-54.1

libMagickWand-6_Q16-1-6.8.8.1-54.1

ImageMagick-debugsource-6.8.8.1-54.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-54.1

ImageMagick-debuginfo-6.8.8.1-54.1

SuSE SLES 12 SP1

x86_64

libMagickWand-6_Q16-1-debuginfo-6.8.8.1-54.1

libMagickCore-6_Q16-1-6.8.8.1-54.1

libMagickWand-6_Q16-1-6.8.8.1-54.1

ImageMagick-debugsource-6.8.8.1-54.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-54.1

ImageMagick-debuginfo-6.8.8.1-54.1

SuSE SLED 12 SP1

x86_64

libMagickWand-6_Q16-1-debuginfo-6.8.8.1-54.1

libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-54.1

libMagick++-6_Q16-3-6.8.8.1-54.1

libMagickCore-6_Q16-1-6.8.8.1-54.1

ImageMagick-6.8.8.1-54.1

ImageMagick-debugsource-6.8.8.1-54.1

libMagick++-6_Q16-3-debuginfo-6.8.8.1-54.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-54.1

libMagickWand-6_Q16-1-6.8.8.1-54.1

libMagickCore-6_Q16-1-32bit-6.8.8.1-54.1
ImageMagick-debuginfo-6.8.8.1-54.1

145119 - SuSE SLES 11 SP4 SUSE-SU-2016:3256-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7530, CVE-2016-8707, CVE-2016-8866, CVE-2016-9556, CVE-2016-9559, CVE-2016-9773

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3256-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002520.html>

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.60.1

x86_64
libMagickCore1-6.4.3.6-7.60.1
libMagickCore1-32bit-6.4.3.6-7.60.1

145121 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3268-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7098

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3268-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002523.html>

SuSE SLED 12 SP1
x86_64
wget-1.14-17.1
wget-debugsource-1.14-17.1
wget-debuginfo-1.14-17.1

SuSE SLES 12 SP2
x86_64
wget-1.14-17.1
wget-debugsource-1.14-17.1
wget-debuginfo-1.14-17.1

SuSE SLED 12 SP2

x86_64
wget-1.14-17.1
wget-debugsource-1.14-17.1
wget-debuginfo-1.14-17.1

SuSE SLES 12 SP1

x86_64
wget-1.14-17.1
wget-debugsource-1.14-17.1
wget-debuginfo-1.14-17.1

145124 - SuSE Linux 13.2 openSUSE-SU-2016:3233-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8707, CVE-2016-8862, CVE-2016-8866, CVE-2016-9556, CVE-2016-9773

Description

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

openSUSE-SU-2016:3233-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00137.html>

SuSE Linux 13.2

i586
ImageMagick-debuginfo-6.8.9.8-45.1
libMagick++-6_Q16-5-6.8.9.8-45.1
libMagickWand-6_Q16-2-debuginfo-6.8.9.8-45.1
perl-PerlMagick-debuginfo-6.8.9.8-45.1
ImageMagick-extra-6.8.9.8-45.1
libMagickWand-6_Q16-2-6.8.9.8-45.1
libMagickCore-6_Q16-2-6.8.9.8-45.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-45.1
ImageMagick-6.8.9.8-45.1
libMagick++-6_Q16-5-debuginfo-6.8.9.8-45.1
libMagick++-devel-6.8.9.8-45.1
ImageMagick-devel-6.8.9.8-45.1
ImageMagick-extra-debuginfo-6.8.9.8-45.1
ImageMagick-debugsource-6.8.9.8-45.1
perl-PerlMagick-6.8.9.8-45.1

noarch

ImageMagick-doc-6.8.9.8-45.1

x86_64

ImageMagick-debuginfo-6.8.9.8-45.1
libMagick++-6_Q16-5-6.8.9.8-45.1
libMagick++-6_Q16-5-32bit-6.8.9.8-45.1
libMagickWand-6_Q16-2-debuginfo-6.8.9.8-45.1
perl-PerlMagick-debuginfo-6.8.9.8-45.1
libMagickCore-6_Q16-2-debuginfo-32bit-6.8.9.8-45.1
ImageMagick-extra-6.8.9.8-45.1
libMagick++-6_Q16-5-debuginfo-32bit-6.8.9.8-45.1
libMagickWand-6_Q16-2-32bit-6.8.9.8-45.1

libMagickWand-6_Q16-2-6.8.9.8-45.1
libMagick++-devel-32bit-6.8.9.8-45.1
libMagickCore-6_Q16-2-6.8.9.8-45.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-45.1
libMagickWand-6_Q16-2-debuginfo-32bit-6.8.9.8-45.1
ImageMagick-6.8.9.8-45.1
libMagick++-6_Q16-5-debuginfo-6.8.9.8-45.1
libMagick++-devel-6.8.9.8-45.1
ImageMagick-devel-6.8.9.8-45.1
ImageMagick-devel-32bit-6.8.9.8-45.1
ImageMagick-extra-debuginfo-6.8.9.8-45.1
libMagickCore-6_Q16-2-32bit-6.8.9.8-45.1
ImageMagick-debugsource-6.8.9.8-45.1
perl-PerlMagick-6.8.9.8-45.1

160185 - CentOS 6, 7 CESA-2016-2972 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
CESA-2016-2972

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-December/022185.html>
<http://lists.centos.org/pipermail/centos-announce/2016-December/022187.html>

CentOS 7

x86_64
vim-filesystem-7.4.160-1.el7_3.1
vim-X11-7.4.160-1.el7_3.1
vim-common-7.4.160-1.el7_3.1
vim-minimal-7.4.160-1.el7_3.1
vim-enhanced-7.4.160-1.el7_3.1

CentOS 6

x86_64
vim-minimal-7.4.629-5.el6_8.1
vim-X11-7.4.629-5.el6_8.1
vim-filesystem-7.4.629-5.el6_8.1
vim-common-7.4.629-5.el6_8.1
vim-enhanced-7.4.629-5.el6_8.1

i686

vim-minimal-7.4.629-5.el6_8.1
vim-X11-7.4.629-5.el6_8.1
vim-filesystem-7.4.629-5.el6_8.1
vim-common-7.4.629-5.el6_8.1
vim-enhanced-7.4.629-5.el6_8.1

163240 - Oracle Enterprise Linux ELSA-2016-2972 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
ELSA-2016-2972

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006590.html>
<http://oss.oracle.com/pipermail/el-errata/2016-December/006591.html>

OEL7
x86_64
vim-enhanced-7.4.160-1.el7_3.1
vim-common-7.4.160-1.el7_3.1
vim-filesystem-7.4.160-1.el7_3.1
vim-minimal-7.4.160-1.el7_3.1
vim-X11-7.4.160-1.el7_3.1

OEL6
x86_64
vim-minimal-7.4.629-5.el6_8.1
vim-X11-7.4.629-5.el6_8.1
vim-common-7.4.629-5.el6_8.1
vim-enhanced-7.4.629-5.el6_8.1
vim-filesystem-7.4.629-5.el6_8.1

i386
vim-minimal-7.4.629-5.el6_8.1
vim-X11-7.4.629-5.el6_8.1
vim-common-7.4.629-5.el6_8.1
vim-enhanced-7.4.629-5.el6_8.1
vim-filesystem-7.4.629-5.el6_8.1

175085 - Scientific Linux Security ERRATA Moderate: vim on SL6.x, SL7.x i386/x86_64 (1612-18621)

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

Risk Level: Medium
CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: vim on SL6.x, SL7.x i386/x86_64 (1612-18621)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1612&L=scientific-linux-errata&F=&S=&P=18621>

SL7
x86_64
vim-filesystem-7.4.160-1.el7_3.1

vim-minimal-7.4.160-1.el7_3.1
vim-common-7.4.160-1.el7_3.1
vim-X11-7.4.160-1.el7_3.1
vim-enhanced-7.4.160-1.el7_3.1
vim-debuginfo-7.4.160-1.el7_3.1

SL6

x86_64
vim-filesystem-7.4.629-5.el6_8.1
vim-common-7.4.629-5.el6_8.1
vim-debuginfo-7.4.629-5.el6_8.1
vim-minimal-7.4.629-5.el6_8.1
vim-enhanced-7.4.629-5.el6_8.1
vim-X11-7.4.629-5.el6_8.1

i386

vim-filesystem-7.4.629-5.el6_8.1
vim-common-7.4.629-5.el6_8.1
vim-debuginfo-7.4.629-5.el6_8.1
vim-minimal-7.4.629-5.el6_8.1
vim-enhanced-7.4.629-5.el6_8.1
vim-X11-7.4.629-5.el6_8.1

178298 - Gentoo Linux GLSA-201612-47 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3223, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-5330, CVE-2015-7540, CVE-2015-8467, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
GLSA-201612-47

Observation

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

<https://security.gentoo.org/glsa/201612-47>

Affected packages:
net-fs/samba < 4.2.11

178299 - Gentoo Linux GLSA-201612-44 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9920

Description

The scan detected that the host is missing the following update:
GLSA-201612-44

Observation

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

<https://security.gentoo.org/glsa/201612-44>

Affected packages:
mail-client/roundcube < 1.2.3

182224 - FreeBSD vim Arbitrary Command Execution (c11629d3-c8ad-11e6-ae1b-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
vim -- arbitrary command execution (c11629d3-c8ad-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/c11629d3-c8ad-11e6-ae1b-002590263bf5.html>

Affected packages:
vim < 8.0.0056
vim-lite < 8.0.0056
neovim < 0.1.7

191535 - Fedora Linux 24 FEDORA-2016-c7e60a9fd4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5507, CVE-2016-5609, CVE-2016-5612, CVE-2016-5616, CVE-2016-5617, CVE-2016-5626, CVE-2016-5627, CVE-2016-5629, CVE-2016-5630, CVE-2016-8283, CVE-2016-8284, CVE-2016-8288

Description

The scan detected that the host is missing the following update:
FEDORA-2016-c7e60a9fd4

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 24

community-mysql-5.7.17-1.fc24

191538 - Fedora Linux 25 FEDORA-2016-3477b592e3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4330, CVE-2016-4331, CVE-2016-4332, CVE-2016-4333

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3477b592e3

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

hdf5-1.8.17-2.fc25

191547 - Fedora Linux 25 FEDORA-2016-9b83c6862d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5507, CVE-2016-5609, CVE-2016-5612, CVE-2016-5616, CVE-2016-5617, CVE-2016-5626, CVE-2016-5627, CVE-2016-5629, CVE-2016-5630, CVE-2016-8283, CVE-2016-8284, CVE-2016-8288

Description

The scan detected that the host is missing the following update:
FEDORA-2016-9b83c6862d

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

community-mysql-5.7.17-1.fc25

21043 - Joomla Elevated Privileges Vulnerability (20161201)

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

Risk Level: Medium

CVE: CVE-2016-9838

Description

A privilege escalation vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A privilege escalation vulnerability is present in some versions of Joomla! CMS. The flaw lies in the form validation process. Successful exploitation of this vulnerability could allow a malicious user to affect integrity by executing high-privileged tasks such as username and password reset.

88832 - Slackware Linux 14.0, 14.1, 14.2 SSA:2016-358-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-5387, CVE-2016-8740, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
SSA:2016-358-01

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=2016&m=slackware-security.495677>

Slackware 14.0
x86_64
httpd-2.4.25-x86_64-1

Slackware 14.2
x86_64
httpd-2.4.25-x86_64-1

i586
httpd-2.4.25-i586-1

Slackware 14.1
x86_64
httpd-2.4.25-x86_64-1

145123 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3269-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8899

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:3269-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002524.html>

SuSE SLED 12 SP1
x86_64
dnsmasq-debugsource-2.71-13.1
dnsmasq-debuginfo-2.71-13.1
dnsmasq-2.71-13.1

SuSE SLES 12 SP2
x86_64
dnsmasq-debugsource-2.71-13.1
dnsmasq-debuginfo-2.71-13.1
dnsmasq-2.71-13.1

SuSE SLED 12 SP2
x86_64

dnsmasq-debugsource-2.71-13.1
dnsmasq-debuginfo-2.71-13.1
dnsmasq-2.71-13.1

SuSE SLES 12 SP1

x86_64

dnsmasq-debugsource-2.71-13.1
dnsmasq-debuginfo-2.71-13.1
dnsmasq-2.71-13.1

178297 - Gentoo Linux GLSA-201612-48 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201612-48

Observation

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

<https://security.gentoo.org/glsa/201612-48>

Affected packages:

sys-apps/firejail < 0.9.44.2

178300 - Gentoo Linux GLSA-201612-45 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8860

Description

The scan detected that the host is missing the following update:
GLSA-201612-45

Observation

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

<https://security.gentoo.org/glsa/201612-45>

Affected packages:

net-misc/tor < 0.2.8.9

182229 - FreeBSD Apache httpd Several Vulnerabilities (862d6ab3-c75e-11e6-9f98-20cf30e32f6d)

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

Risk Level: Medium

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-5387, CVE-2016-8740, CVE-2016-8743

Description

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

Apache httpd -- several vulnerabilities (862d6ab3-c75e-11e6-9f98-20cf30e32f6d)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/862d6ab3-c75e-11e6-9f98-20cf30e32f6d.html>

Affected packages:

apache24 < 2.4.25

130660 - Debian Linux 8.0 DSA-3743-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9964

Description

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

DSA-3743-1

Observation

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

For more information see:

<http://www.debian.org/security/2016/dsa-3743>

Debian 8.0

all

python-bottle_0.12.7-1+deb8u1

145118 - SuSE Linux 13.2 openSUSE-SU-2016:3215-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8400

Description

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

openSUSE-SU-2016:3215-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00128.html>

SuSE Linux 13.2

x86_64

shellinabox-2.20-5.3.1

shellinabox-debuginfo-2.20-5.3.1

shellinabox-debugsource-2.20-5.3.1

i586
shellinabox-2.20-5.3.1
shellinabox-debuginfo-2.20-5.3.1
shellinabox-debugsource-2.20-5.3.1

88831 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-358-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012

Description

The scan detected that the host is missing the following update:
SSA:2016-358-02

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.647637>

Slackware 14.0
x86_64
openssh-7.4p1-x86_64-1

Slackware 13.37
x86_64
openssh-7.4p1-x86_64-1

Slackware 14.1
x86_64
openssh-7.4p1-x86_64-1

Slackware 13.1
x86_64
openssh-7.4p1-x86_64-1

Slackware 14.2
x86_64
openssh-7.4p1-x86_64-1

i586
openssh-7.4p1-i586-1

Slackware 13.0
x86_64
openssh-7.4p1-x86_64-1

130657 - Debian Linux 8.0 DSA-3745-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-10002

Description

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

DSA-3745-1

Observation

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

<http://www.debian.org/security/2016/dsa-3745>

Debian 8.0
all
squid3_3.4.8-6+deb8u4

130658 - Debian Linux 8.0 DSA-3747-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9963

Description

The scan detected that the host is missing the following update:
DSA-3747-1

Observation

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

<http://www.debian.org/security/2016/dsa-3747>

Debian 8.0
all
exim4_4.84.2-2+deb8u2

141390 - Red Hat Enterprise Linux RHSA-2016-2996 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2016-2996

Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2996.html>

RHEL4ES
x86_64
redhat-release-4ES-10.14

i386
redhat-release-4ES-10.14

RHEL4AS
i386
redhat-release-4AS-10.14

x86_64
redhat-release-4AS-10.14

141391 - Red Hat Enterprise Linux RHSA-2016-2997 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

RHSA-2016-2997

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2997.html>

RHEL5D
x86_64
redhat-release-5Client-5.11.0.7

i386
redhat-release-5Client-5.11.0.7

RHEL5S
i386
redhat-release-5Server-5.11.0.7

x86_64
redhat-release-5Server-5.11.0.7

182220 - FreeBSD xen-kernel X86 PV Guests May Be Able To Mask Interrupts (3ae078ca-c7eb-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-10024

Description

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

xen-kernel -- x86 PV guests may be able to mask interrupts (3ae078ca-c7eb-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/3ae078ca-c7eb-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-kernel < 4.7.1_3

182222 - FreeBSD openssh Multiple Vulnerabilities (2aedd15f-ca8b-11e6-a9a5-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2016-10009, CVE-2016-10010

Description

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

openssh -- multiple vulnerabilities (2aedd15f-ca8b-11e6-a9a5-b499baebfeaf)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/2aedd15f-ca8b-11e6-a9a5-b499baebfeaf.html>

Affected packages:

openssh-portable < 7.4

11.0 <= FreeBSD < 11.0_7

10.3 <= FreeBSD < 10.3_16

10.2 <= FreeBSD < 10.2_29

10.1 <= FreeBSD < 10.1_46

9.3 <= FreeBSD < 9.3_54

182225 - FreeBSD Joomla! Multiple Vulnerabilities (c0ef061a-c7f0-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

Joomla! -- multiple vulnerabilities (c0ef061a-c7f0-11e6-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/c0ef061a-c7f0-11e6-ae1b-002590263bf5.html>

Affected packages:

1.5.0 <= joomla3 < 3.4.7

182226 - FreeBSD upnp Multiple Vulnerabilities (244c8288-cc4a-11e6-a475-bcaec524bf84)

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

Risk Level: Low

CVE: CVE-2016-6255, CVE-2016-8863

Description

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

upnp -- multiple vulnerabilities (244c8288-cc4a-11e6-a475-bcaec524bf84)

Observation

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

<http://www.vuxml.org/freebsd/244c8288-cc4a-11e6-a475-bcaec524bf84.html>

Affected packages:
upnp < 1.6.21

182227 - FreeBSD exim DKIM Private Key Leak (e7002b26-caaa-11e6-a76a-9f7324e5534e)

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

Risk Level: Low

CVE: CVE-2016-9963

Description

The scan detected that the host is missing the following update:
exim -- DKIM private key leak (e7002b26-caaa-11e6-a76a-9f7324e5534e)

Observation

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

<http://www.vuxml.org/freebsd/e7002b26-caaa-11e6-a76a-9f7324e5534e.html>

Affected packages:
4.69 < exim < 4.87.1

182228 - FreeBSD Joomla! Multiple Vulnerabilities (f0806cad-c7f1-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
Joomla! -- multiple vulnerabilities (f0806cad-c7f1-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/f0806cad-c7f1-11e6-ae1b-002590263bf5.html>

Affected packages:
1.6.0 <= joomla3 < 3.6.1

182230 - FreeBSD cURL Buffer Overflow (42880202-c81c-11e6-a9a5-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2016-9586

Description

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

cURL -- buffer overflow (42880202-c81c-11e6-a9a5-b499baebfeaf)

Observation

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

<http://www.vuxml.org/freebsd/42880202-c81c-11e6-a9a5-b499baebfeaf.html>

Affected packages:

7.1 <= curl < 7.52

182231 - FreeBSD cURL Uninitialized Random Vulnerability (c40ca16c-4d9f-4d70-8b6c-4d53aeb8ead4)

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

Risk Level: Low

CVE: CVE-2016-9594

Description

The scan detected that the host is missing the following update:
cURL -- uninitialized random vulnerability (c40ca16c-4d9f-4d70-8b6c-4d53aeb8ead4)

Observation

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

<http://www.vuxml.org/freebsd/c40ca16c-4d9f-4d70-8b6c-4d53aeb8ead4.html>

Affected packages:

7.52.0 <= curl < 7.52.1

182232 - FreeBSD FreeBSD Multiple Vulnerabilities Of Ntp (fcedcdbb-c86e-11e6-b1cf-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311

Description

The scan detected that the host is missing the following update:
FreeBSD -- Multiple vulnerabilities of ntp (fcedcdbb-c86e-11e6-b1cf-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/fcedcdbb-c86e-11e6-b1cf-14dae9d210b8.html>

Affected packages:

11.0 <= FreeBSD < 11.0_6
10.3 <= FreeBSD < 10.3_15
10.2 <= FreeBSD < 10.2_28
10.1 <= FreeBSD < 10.1_45
9.3 <= FreeBSD < 9.3_53

182233 - FreeBSD phpmailer Remote Code Execution (c7656d4c-cb60-11e6-a9a5-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2016-10033

Description

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

phpmailer -- Remote Code Execution (c7656d4c-cb60-11e6-a9a5-b499baebfeaf)

Observation

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

<http://www.vuxml.org/freebsd/c7656d4c-cb60-11e6-a9a5-b499baebfeaf.html>

Affected packages:

phpmailer < 5.2.18

182234 - FreeBSD squid Multiple Vulnerabilities (41f8af15-c8b9-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-10002, CVE-2016-10003

Description

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

squid -- multiple vulnerabilities (41f8af15-c8b9-11e6-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/41f8af15-c8b9-11e6-ae1b-002590263bf5.html>

Affected packages:

3.1 <= squid < 3.5.23

4.0 <= squid-devel < 4.0.17

182235 - FreeBSD samba Multiple Vulnerabilities (e4bc323f-cc73-11e6-b704-000c292e4fd8)

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

Risk Level: Low

CVE: CVE-2016-2123, CVE-2016-2125, CVE-2016-2126

Description

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

samba -- multiple vulnerabilities (e4bc323f-cc73-11e6-b704-000c292e4fd8)

Observation

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

<http://www.vuxml.org/freebsd/e4bc323f-cc73-11e6-b704-000c292e4fd8.html>

Affected packages:

3.6.0 <= samba36 <= 3.6.25_4
4.0.0 <= samba4 <= 4.0.26
4.1.0 <= samba41 <= 4.1.23
4.2.0 <= samba42 <= 4.2.14
4.3.0 <= samba43 < 4.3.13
4.4.0 <= samba44 < 4.4.8
4.5.0 <= samba45 < 4.5.3

182236 - FreeBSD Pligg CMS XSS Vulnerability (c290f093-c89e-11e6-821e-68f7288bdf41)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
Pligg CMS -- XSS Vulnerability (c290f093-c89e-11e6-821e-68f7288bdf41)

Observation

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

<http://www.vuxml.org/freebsd/c290f093-c89e-11e6-821e-68f7288bdf41.html>

Affected packages:

pligg <= 2.0.2,1

191527 - Fedora Linux 25 FEDORA-2016-8d9b62c784 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
FEDORA-2016-8d9b62c784

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

httpd-2.4.25-1.fc25

191528 - Fedora Linux 24 FEDORA-2016-d22f50d985 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d22f50d985

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 24

httpd-2.4.25-1.fc24

191529 - Fedora Linux 25 FEDORA-2016-edbb33ab2e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9586

Description

The scan detected that the host is missing the following update:
FEDORA-2016-edbb33ab2e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

curl-7.51.0-4.fc25

191531 - Fedora Linux 25 FEDORA-2016-3b59109c48 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9132

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3b59109c48

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

botan-1.10.14-3.fc25

191532 - Fedora Linux 24 FEDORA-2016-608be17784 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-2016-608be17784

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 24

python-wikicms-2.1.10-1.fc24

191534 - Fedora Linux 24 FEDORA-2016-bb22a24d3d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8652

Description

The scan detected that the host is missing the following update:
FEDORA-2016-bb22a24d3d

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

dovecot-2.2.27-1.fc24

191536 - Fedora Linux 24 FEDORA-2016-8586235698 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-2016-8586235698

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 24

nagios-plugins-2.1.4-2.fc24

191539 - Fedora Linux 25 FEDORA-2016-f30fae0f67 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-2016-f30fae0f67

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

nagios-plugins-2.1.4-2.fc25

191540 - Fedora Linux 25 FEDORA-2016-92e3ea2d1b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-10013, CVE-2016-10024, CVE-2016-10025

Description

The scan detected that the host is missing the following update:
FEDORA-2016-92e3ea2d1b

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

xen-4.7.1-6.fc25

191541 - Fedora Linux 25 FEDORA-2016-dd895763ac Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9588

Description

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

FEDORA-2016-dd895763ac

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

kernel-4.8.15-300.fc25

191542 - Fedora Linux 25 FEDORA-2016-364f61377b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
FEDORA-2016-364f61377b

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

samba-4.5.3-0.fc25

191543 - Fedora Linux 25 FEDORA-2016-a1e8589ef9 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-2016-a1e8589ef9

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 25

gdk-pixbuf2-2.36.2-1.fc25

191544 - Fedora Linux 25 FEDORA-2016-3368a38282 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-2016-3368a38282

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

js-jquery-2.2.4-1.fc25

191545 - Fedora Linux 24 FEDORA-2016-7de64a450f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9132

Description

The scan detected that the host is missing the following update:
FEDORA-2016-7de64a450f

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

botan-1.10.14-3.fc24

191546 - Fedora Linux 24 FEDORA-2016-2b1f91e9bd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9588

Description

The scan detected that the host is missing the following update:
FEDORA-2016-2b1f91e9bd

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

kernel-4.8.15-200.fc24

191548 - Fedora Linux 25 FEDORA-2016-fce8b939c9 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-2016-fce8b939c9

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=1>

Fedora Core 25

python-wikitcms-2.1.10-1.fc25

191530 - Fedora Linux 24 FEDORA-2016-bcbae0781f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9637, CVE-2016-9815, CVE-2016-9816, CVE-2016-9817, CVE-2016-9818, CVE-2016-9913, CVE-2016-9914, CVE-2016-9915, CVE-2016-9916, CVE-2016-9921, CVE-2016-9922, CVE-2016-9932

Description

The scan detected that the host is missing the following update:
FEDORA-2016-bcbae0781f

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/12/?count=200&page=2>

Fedora Core 24

xen-4.6.4-4.fc24

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.

21010 - (MS16-148) Security Update for Microsoft Office (3204068)

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

Risk Level: High

CVE: CVE-2016-7257, CVE-2016-7262, CVE-2016-7263, CVE-2016-7264, CVE-2016-7265, CVE-2016-7266, CVE-2016-7267, CVE-

2016-7268, CVE-2016-7275, CVE-2016-7276, CVE-2016-7277, CVE-2016-7289, CVE-2016-7290, CVE-2016-7291, CVE-2016-7298, CVE-2016-7300

Update Details

Documentation is updated

21011 - (MS16-148) Security Update for Microsoft Office (3204068)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7257, CVE-2016-7262, CVE-2016-7263, CVE-2016-7264, CVE-2016-7265, CVE-2016-7266, CVE-2016-7267, CVE-2016-7268, CVE-2016-7275, CVE-2016-7276, CVE-2016-7277, CVE-2016-7289, CVE-2016-7290, CVE-2016-7291, CVE-2016-7298, CVE-2016-7300

Update Details

Documentation is updated

130613 - Debian Linux 8.0 DSA-3697-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7966

Update Details

Risk is updated

181727 - FreeBSD joomla Multiple Vulnerabilities (a9f60ce8-a4e0-11e5-b864-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2015-8562, CVE-2015-8563, CVE-2015-8564, CVE-2015-8565

Update Details

FASLScript is updated

191319 - Fedora Linux 25 FEDORA-2016-92c112a380 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7966, CVE-2016-7967, CVE-2016-7968

Update Details

Risk is updated

191324 - Fedora Linux 24 FEDORA-2016-1b042a79bd Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7966, CVE-2016-7967, CVE-2016-7968

Update Details

Risk is updated

191336 - Fedora Linux 24 FEDORA-2016-c9d15bbcbb Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7966, CVE-2016-7967, CVE-2016-7968

[Update Details](#)

Risk is updated

191349 - Fedora Linux 23 FEDORA-2016-f7a079f775 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7966, CVE-2016-7967, CVE-2016-7968

[Update Details](#)

Risk is updated

141353 - Red Hat Enterprise Linux RHSA-2016-2593 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7091

[Update Details](#)

Risk is updated

144918 - SuSE Linux 13.2 openSUSE-SU-2016:2498-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7787

[Update Details](#)

Risk is updated

163203 - Oracle Enterprise Linux ELSA-2016-2593 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7091

[Update Details](#)

Risk is updated

175072 - Scientific Linux Security ERRATA Low: sudo on SL7.x x86_64 (1612-4962)

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

Risk Level: Medium

CVE: CVE-2016-7091

[Update Details](#)

Risk is updated

190321 - Fedora Linux 22 FEDORA-2016-2302ed02a7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2312

[Update Details](#)

Risk is updated

190323 - Fedora Linux 23 FEDORA-2016-17670e1b90 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2312

[Update Details](#)

Risk is updated

191522 - Fedora Linux 25 FEDORA-2016-1b868c23a9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9815, CVE-2016-9816, CVE-2016-9817, CVE-2016-9818, CVE-2016-9913, CVE-2016-9914, CVE-2016-9915, CVE-2016-9916, CVE-2016-9921, CVE-2016-9922, CVE-2016-9932

[Update Details](#)

Risk is updated

191525 - Fedora Linux 23 FEDORA-2016-cc2916dcf4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9637, CVE-2016-9815, CVE-2016-9816, CVE-2016-9817, CVE-2016-9818, CVE-2016-9913, CVE-2016-9914, CVE-2016-9915, CVE-2016-9916, CVE-2016-9921, CVE-2016-9922

[Update Details](#)

Risk is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category

and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFFEE 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 2016 McAfee, Inc.

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