

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

132359 - Oracle VM OVMSA-2017-0066 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-4095, CVE-2007-2241, CVE-2007-2925, CVE-2007-2926, CVE-2007-6283, CVE-2008-0122, CVE-2008-1447, CVE-2009-0025, CVE-2009-0696, CVE-2010-0097, CVE-2010-0290, CVE-2011-0414, CVE-2011-1910, CVE-2011-2464, CVE-2012-1033, CVE-2012-1667, CVE-2012-3817, CVE-2012-4244, CVE-2012-5166, CVE-2012-5688, CVE-2012-5689, CVE-2013-2266, CVE-2013-4854, CVE-2014-0591, CVE-2014-8500, CVE-2015-1349, CVE-2015-4620, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000, CVE-2015-8704, CVE-2016-1285, CVE-2016-1286, CVE-2016-2776, CVE-2016-2848, CVE-2016-8864, CVE-2016-9147, CVE-2017-3136, CVE-2017-3137

Description

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

OVMSA-2017-0066

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000681.html>

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000680.html>

OVM3.3

x86_64

bind-libs-9.8.2-0.62.rc1.el6_9.1

bind-utils-9.8.2-0.62.rc1.el6_9.1

OVM3.4

x86_64

bind-libs-9.8.2-0.62.rc1.el6_9.1

bind-utils-9.8.2-0.62.rc1.el6_9.1

145321 - SuSE SLES 11 SP4 SUSE-SU-2017:1102-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2004-0230, CVE-2012-6704, CVE-2013-6368, CVE-2015-1350, CVE-2015-8956, CVE-2015-8962, CVE-2015-8964, CVE-2016-10088, CVE-2016-3841, CVE-2016-5696, CVE-2016-7042, CVE-2016-7097, CVE-2016-7117, CVE-2016-7910, CVE-2016-7911, CVE-2016-7916, CVE-2016-8399, CVE-2016-8632, CVE-2016-8633, CVE-2016-8646, CVE-2016-9555, CVE-2016-9576, CVE-2016-9685, CVE-2016-9756, CVE-2016-9793, CVE-2016-9794, CVE-2017-5551

Description

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

SUSE-SU-2017:1102-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002828.html>

SuSE SLES 11 SP4

x86_64

kernel-rt_trace-base-3.0.101.rt130-68.1

kernel-rt_trace-devel-3.0.101.rt130-68.1

kernel-rt-devel-3.0.101.rt130-68.1

kernel-rt-3.0.101.rt130-68.1

kernel-syms-rt-3.0.101.rt130-68.1

kernel-source-rt-3.0.101.rt130-68.1

kernel-rt-base-3.0.101.rt130-68.1

kernel-rt_trace-3.0.101.rt130-68.1

191991 - Fedora Linux 25 FEDORA-2017-a3a47973eb Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449, CVE-2016-4658, CVE-2016-5131, CVE-2016-9318

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a3a47973eb

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/2017/4/?count=200&page=3>

Fedora Core 25

libxml2-2.9.4-2.fc25

192014 - Fedora Linux 24 FEDORA-2017-be8574d593 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449, CVE-2016-4658, CVE-2016-5131, CVE-2016-9318

Description

The scan detected that the host is missing the following update:
FEDORA-2017-be8574d593

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/2017/4/?count=200&page=3>

Fedora Core 24

libxml2-2.9.4-2.fc24

21706 - (MS17-010) Security Update for Windows SMB Server (4013389)

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

Description

Multiple vulnerabilities are present in some versions of Microsoft Windows.

Observation

Microsoft Windows is an industry-standard operating system.

Multiple vulnerabilities are present in some versions of Microsoft Windows. The flaws lie in the way the Microsoft Server Message Block 1.0 (SMBv1) server handles requests. Successful exploitation could allow an attacker to execute arbitrary remote code or to obtain sensitive information. Exploitation requires the malicious user to send a specially crafted packet to a SMBv1 server.

Microsoft has released MS17-010 to address this issue. The target appears to be missing this patch.

141549 - Red Hat Enterprise Linux RHSA-2017-1104 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5429, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5459, CVE-2017-5460, CVE-2017-5464, CVE-2017-5465, CVE-2017-5469

Description

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

RHSA-2017-1104

Observation

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

For more information see:

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00037.html>

RHEL6D

x86_64

firefox-debuginfo-52.1.0-2.el6_9

firefox-52.1.0-2.el6_9

i386

firefox-debuginfo-52.1.0-2.el6_9

firefox-52.1.0-2.el6_9

RHEL6S

i386

firefox-debuginfo-52.1.0-2.el6_9

firefox-52.1.0-2.el6_9

x86_64

firefox-debuginfo-52.1.0-2.el6_9
firefox-52.1.0-2.el6_9

RHEL6WS

x86_64
firefox-debuginfo-52.1.0-2.el6_9
firefox-52.1.0-2.el6_9

i386

firefox-debuginfo-52.1.0-2.el6_9
firefox-52.1.0-2.el6_9

141551 - Red Hat Enterprise Linux RHSA-2017-1100 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5461

Description

The scan detected that the host is missing the following update:
RHSA-2017-1100

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00033.html>

RHEL7S

x86_64
nss-util-3.28.4-1.0.el7_3
nss-pkcs11-devel-3.28.4-1.0.el7_3
nss-debuginfo-3.28.4-1.0.el7_3
nss-3.28.4-1.0.el7_3
nss-tools-3.28.4-1.0.el7_3
nss-devel-3.28.4-1.0.el7_3
nss-util-devel-3.28.4-1.0.el7_3
nss-util-debuginfo-3.28.4-1.0.el7_3
nss-sysinit-3.28.4-1.0.el7_3

RHEL6S

i386
nss-util-debuginfo-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-tools-3.28.4-1.el6_9
nss-debuginfo-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

x86_64

nss-util-debuginfo-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9

nss-tools-3.28.4-1.el6_9
nss-debuginfo-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

RHEL6WS

x86_64
nss-util-debuginfo-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-tools-3.28.4-1.el6_9
nss-debuginfo-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

i386

nss-util-debuginfo-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-tools-3.28.4-1.el6_9
nss-debuginfo-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

RHEL7D

x86_64
nss-util-3.28.4-1.0.el7_3
nss-pkcs11-devel-3.28.4-1.0.el7_3
nss-debuginfo-3.28.4-1.0.el7_3
nss-3.28.4-1.0.el7_3
nss-tools-3.28.4-1.0.el7_3
nss-devel-3.28.4-1.0.el7_3
nss-util-devel-3.28.4-1.0.el7_3
nss-util-debuginfo-3.28.4-1.0.el7_3
nss-sysinit-3.28.4-1.0.el7_3

RHEL6D

x86_64
nss-util-debuginfo-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-tools-3.28.4-1.el6_9
nss-debuginfo-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

i386

nss-util-debuginfo-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-tools-3.28.4-1.el6_9
nss-debuginfo-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

RHEL7WS

x86_64

nss-util-3.28.4-1.0.el7_3

nss-pkcs11-devel-3.28.4-1.0.el7_3

nss-debuginfo-3.28.4-1.0.el7_3

nss-3.28.4-1.0.el7_3

nss-tools-3.28.4-1.0.el7_3

nss-devel-3.28.4-1.0.el7_3

nss-util-devel-3.28.4-1.0.el7_3

nss-util-debuginfo-3.28.4-1.0.el7_3

nss-sysinit-3.28.4-1.0.el7_3

141552 - Red Hat Enterprise Linux RHSA-2017-1106 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5459, CVE-2017-5460, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469

Description

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

RHSA-2017-1106

Observation

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

For more information see:

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00039.html>

RHEL7D

x86_64

firefox-debuginfo-52.1.0-2.el7_3

firefox-52.1.0-2.el7_3

RHEL7S

x86_64

firefox-debuginfo-52.1.0-2.el7_3

firefox-52.1.0-2.el7_3

RHEL7WS

x86_64

firefox-debuginfo-52.1.0-2.el7_3

firefox-52.1.0-2.el7_3

141554 - Red Hat Enterprise Linux RHSA-2017-1102 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5461

Description

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

RHSA-2017-1102

Observation

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

For more information see:

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00035.html>

RHEL6_5S

x86_64

nss-util-debuginfo-3.16.1-5.el6_5

nss-util-3.16.1-5.el6_5

nss-util-devel-3.16.1-5.el6_5

RHEL6_2S

x86_64

nss-util-3.13.1-11.el6_2

nss-util-debuginfo-3.13.1-11.el6_2

nss-util-devel-3.13.1-11.el6_2

RHEL6_7S

i386

nss-util-3.21.4-1.el6_7

nss-util-devel-3.21.4-1.el6_7

nss-util-debuginfo-3.21.4-1.el6_7

x86_64

nss-util-3.21.4-1.el6_7

nss-util-devel-3.21.4-1.el6_7

nss-util-debuginfo-3.21.4-1.el6_7

RHEL6_6S

x86_64

nss-util-3.19.1-4.el6_6

nss-util-debuginfo-3.19.1-4.el6_6

nss-util-devel-3.19.1-4.el6_6

RHEL7_2S

x86_64

nss-util-devel-3.21.4-1.el7_2

nss-util-3.21.4-1.el7_2

nss-util-debuginfo-3.21.4-1.el7_2

RHEL6_4S

x86_64

nss-util-3.14.3-9.el6_4

nss-util-devel-3.14.3-9.el6_4

nss-util-debuginfo-3.14.3-9.el6_4

141557 - Red Hat Enterprise Linux RHSA-2017-1103 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5461

Description

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

RHSA-2017-1103

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00036.html>

RHEL5_9S

i386
nss-debuginfo-3.14.3-11.el5_9
nss-tools-3.14.3-11.el5_9
nss-devel-3.14.3-11.el5_9
nss-pkcs11-devel-3.14.3-11.el5_9
nss-3.14.3-11.el5_9

x86_64

nss-debuginfo-3.14.3-11.el5_9
nss-tools-3.14.3-11.el5_9
nss-devel-3.14.3-11.el5_9
nss-pkcs11-devel-3.14.3-11.el5_9
nss-3.14.3-11.el5_9

160239 - CentOS 6, 7 CESA-2017-1100 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5461

Description

The scan detected that the host is missing the following update:
CESA-2017-1100

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-April/022396.html>
<http://lists.centos.org/pipermail/centos-announce/2017-April/022397.html>
<http://lists.centos.org/pipermail/centos-announce/2017-April/022391.html>
<http://lists.centos.org/pipermail/centos-announce/2017-April/022392.html>

CentOS 7

x86_64
nss-util-3.28.4-1.0.el7_3
nss-pkcs11-devel-3.28.4-1.0.el7_3
nss-3.28.4-1.0.el7_3
nss-tools-3.28.4-1.0.el7_3
nss-util-devel-3.28.4-1.0.el7_3
nss-sysinit-3.28.4-1.0.el7_3
nss-devel-3.28.4-1.0.el7_3

i686

nss-3.28.4-1.0.el7_3
nss-pkcs11-devel-3.28.4-1.0.el7_3
nss-util-3.28.4-1.0.el7_3
nss-devel-3.28.4-1.0.el7_3
nss-util-devel-3.28.4-1.0.el7_3

CentOS 6

x86_64
nss-tools-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

i686
nss-tools-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

160246 - CentOS 6 CESA-2017-1104 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5429, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5459, CVE-2017-5460, CVE-2017-5464, CVE-2017-5465, CVE-2017-5469

Description

The scan detected that the host is missing the following update:
CESA-2017-1104

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-April/022394.html>

CentOS 6
x86_64
firefox-52.1.0-2.el6.centos

i686
firefox-52.1.0-2.el6.centos

160247 - CentOS 7 CESA-2017-1106 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5459, CVE-2017-5460, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469

Description

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

CESA-2017-1106

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-April/022398.html>

CentOS 7
x86_64
firefox-52.1.0-2.el7.centos

i686
firefox-52.1.0-2.el7.centos

163337 - Oracle Enterprise Linux ELSA-2017-1106 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5459, CVE-2017-5460, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469

Description

The scan detected that the host is missing the following update:
ELSA-2017-1106

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006874.html>

OEL7
x86_64
firefox-52.1.0-2.0.1.el7_3

163339 - Oracle Enterprise Linux ELSA-2017-1100 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5461

Description

The scan detected that the host is missing the following update:
ELSA-2017-1100

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006873.html>
<http://oss.oracle.com/pipermail/el-errata/2017-April/006877.html>

OEL7

x86_64
nss-util-3.28.4-1.0.el7_3
nss-sysinit-3.28.4-1.0.0.1.el7_3
nss-tools-3.28.4-1.0.0.1.el7_3
nss-devel-3.28.4-1.0.0.1.el7_3
nss-3.28.4-1.0.0.1.el7_3
nss-util-devel-3.28.4-1.0.el7_3
nss-pkcs11-devel-3.28.4-1.0.0.1.el7_3

OEL6

x86_64
nss-3.28.4-1.0.1.el6_9
nss-devel-3.28.4-1.0.1.el6_9
nss-sysinit-3.28.4-1.0.1.el6_9
nss-util-3.28.4-1.el6_9
nss-tools-3.28.4-1.0.1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.0.1.el6_9

i386

nss-3.28.4-1.0.1.el6_9
nss-devel-3.28.4-1.0.1.el6_9
nss-sysinit-3.28.4-1.0.1.el6_9
nss-util-3.28.4-1.el6_9
nss-tools-3.28.4-1.0.1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.0.1.el6_9

163340 - Oracle Enterprise Linux ELSA-2017-1104 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5428, CVE-2017-5429, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5459, CVE-2017-5460, CVE-2017-5464, CVE-2017-5465, CVE-2017-5469

Description

The scan detected that the host is missing the following update:
ELSA-2017-1104

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006876.html>

OEL6

x86_64
firefox-52.1.0-2.0.1.el6_9

i386

firefox-52.1.0-2.0.1.el6_9

175162 - Scientific Linux Security ERRATA Critical: firefox on SL6.x i386/x86_64 (1704-17959)

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

Risk Level: High

CVE: CVE-2017-5429, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5459, CVE-2017-5460, CVE-2017-5464, CVE-2017-5465, CVE-2017-5469

Description

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

Security ERRATA Critical: firefox on SL6.x i386/x86_64 (1704-17959)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=17959>

SL6

x86_64

firefox-debuginfo-52.1.0-2.el6_9

firefox-52.1.0-2.el6_9

i386

firefox-debuginfo-52.1.0-2.el6_9

firefox-52.1.0-2.el6_9

175164 - Scientific Linux Security ERRATA Critical: nss and nss-util on SL6.x, SL7.x i386/x86_64 (1704-19015)

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

Risk Level: High

CVE: CVE-2017-5461

Description

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

Security ERRATA Critical: nss and nss-util on SL6.x, SL7.x i386/x86_64 (1704-19015)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=19015>

SL7

x86_64

nss-util-3.28.4-1.0.el7_3

nss-pkcs11-devel-3.28.4-1.0.el7_3

nss-debuginfo-3.28.4-1.0.el7_3

nss-3.28.4-1.0.el7_3

nss-tools-3.28.4-1.0.el7_3

nss-devel-3.28.4-1.0.el7_3

nss-util-devel-3.28.4-1.0.el7_3

nss-util-debuginfo-3.28.4-1.0.el7_3

nss-sysinit-3.28.4-1.0.el7_3

SL6

x86_64

nss-util-debuginfo-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-tools-3.28.4-1.el6_9
nss-debuginfo-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

i386

nss-util-debuginfo-3.28.4-1.el6_9
nss-devel-3.28.4-1.el6_9
nss-pkcs11-devel-3.28.4-1.el6_9
nss-util-3.28.4-1.el6_9
nss-util-devel-3.28.4-1.el6_9
nss-tools-3.28.4-1.el6_9
nss-debuginfo-3.28.4-1.el6_9
nss-3.28.4-1.el6_9
nss-sysinit-3.28.4-1.el6_9

175165 - Scientific Linux Security ERRATA Critical: firefox on SL7.x x86_64 (1704-19371)

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

Risk Level: High

CVE: CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5459, CVE-2017-5460, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL7.x x86_64 (1704-19371)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=19371>

SL7
x86_64
firefox-debuginfo-52.1.0-2.el7_3
firefox-52.1.0-2.el7_3

175167 - Scientific Linux Security ERRATA Critical: nss-util on SL6.x, SL7.x x86_64 (1704-18680)

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

Risk Level: High

CVE: CVE-2017-5461

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: nss-util on SL6.x, SL7.x x86_64 (1704-18680)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=18680>

SL7

x86_64
nss-util-devel-3.21.4-1.el7_2
nss-util-3.21.4-1.el7_2
nss-util-debuginfo-3.21.4-1.el7_2

SL6

x86_64
nss-util-devel-3.16.1-5.el6_5
nss-util-debuginfo-3.19.1-4.el6_6
nss-util-devel-3.19.1-4.el6_6
nss-util-debuginfo-3.16.1-5.el6_5
nss-util-debuginfo-3.21.4-1.el6_7
nss-util-devel-3.21.4-1.el6_7
nss-util-3.19.1-4.el6_6
nss-util-3.21.4-1.el6_7
nss-util-3.16.1-5.el6_5

192000 - Fedora Linux 24 FEDORA-2017-7c9a9b2b36 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7572

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7c9a9b2b36

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/2017/4/?count=200&page=2>

Fedora Core 24

backintime-1.1.20-1.fc24

192002 - Fedora Linux 25 FEDORA-2017-8dce7a3940 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7572

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8dce7a3940

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/2017/4/?count=200&page=1>

Fedora Core 25

backintime-1.1.20-1.fc25

141550 - Red Hat Enterprise Linux RHSA-2017-1124 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Description

The scan detected that the host is missing the following update:
RHSA-2017-1124

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00045.html>

RHEL6D

x86_64

chromium-browser-debuginfo-58.0.3029.81-1.el6_9

chromium-browser-58.0.3029.81-1.el6_9

i386

chromium-browser-debuginfo-58.0.3029.81-1.el6_9

chromium-browser-58.0.3029.81-1.el6_9

RHEL6S

x86_64

chromium-browser-debuginfo-58.0.3029.81-1.el6_9

chromium-browser-58.0.3029.81-1.el6_9

i386

chromium-browser-debuginfo-58.0.3029.81-1.el6_9

chromium-browser-58.0.3029.81-1.el6_9

RHEL6WS

x86_64

chromium-browser-debuginfo-58.0.3029.81-1.el6_9

chromium-browser-58.0.3029.81-1.el6_9

i386

chromium-browser-debuginfo-58.0.3029.81-1.el6_9

chromium-browser-58.0.3029.81-1.el6_9

141553 - Red Hat Enterprise Linux RHSA-2017-1126 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
RHSA-2017-1126

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00047.html>

RHEL6_2S

x86_64
kernel-headers-2.6.32-220.71.1.el6
perf-2.6.32-220.71.1.el6
kernel-debuginfo-2.6.32-220.71.1.el6
kernel-debug-devel-2.6.32-220.71.1.el6
python-perf-debuginfo-2.6.32-220.71.1.el6
kernel-debug-debuginfo-2.6.32-220.71.1.el6
kernel-devel-2.6.32-220.71.1.el6
kernel-debuginfo-common-x86_64-2.6.32-220.71.1.el6
kernel-debug-2.6.32-220.71.1.el6
python-perf-2.6.32-220.71.1.el6
kernel-2.6.32-220.71.1.el6
perf-debuginfo-2.6.32-220.71.1.el6

noarch

kernel-doc-2.6.32-220.71.1.el6
kernel-firmware-2.6.32-220.71.1.el6

141555 - Red Hat Enterprise Linux RHSA-2017-1095 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3136, CVE-2017-3137

Description

The scan detected that the host is missing the following update:
RHSA-2017-1095

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00032.html>

RHEL7D

x86_64
bind-sdb-chroot-9.9.4-38.el7_3.3
bind-pkcs11-utils-9.9.4-38.el7_3.3
bind-debuginfo-9.9.4-38.el7_3.3
bind-libs-9.9.4-38.el7_3.3
bind-9.9.4-38.el7_3.3
bind-libs-lite-9.9.4-38.el7_3.3
bind-chroot-9.9.4-38.el7_3.3
bind-lite-devel-9.9.4-38.el7_3.3

bind-pkcs11-libs-9.9.4-38.el7_3.3
bind-pkcs11-devel-9.9.4-38.el7_3.3
bind-utils-9.9.4-38.el7_3.3
bind-pkcs11-9.9.4-38.el7_3.3
bind-devel-9.9.4-38.el7_3.3
bind-sdb-9.9.4-38.el7_3.3

noarch
bind-license-9.9.4-38.el7_3.3

RHEL7S
noarch
bind-license-9.9.4-38.el7_3.3

x86_64
bind-sdb-chroot-9.9.4-38.el7_3.3
bind-pkcs11-utils-9.9.4-38.el7_3.3
bind-debuginfo-9.9.4-38.el7_3.3
bind-libs-9.9.4-38.el7_3.3
bind-9.9.4-38.el7_3.3
bind-libs-lite-9.9.4-38.el7_3.3
bind-chroot-9.9.4-38.el7_3.3
bind-lite-devel-9.9.4-38.el7_3.3
bind-pkcs11-libs-9.9.4-38.el7_3.3
bind-pkcs11-devel-9.9.4-38.el7_3.3
bind-utils-9.9.4-38.el7_3.3
bind-pkcs11-9.9.4-38.el7_3.3
bind-devel-9.9.4-38.el7_3.3
bind-sdb-9.9.4-38.el7_3.3

RHEL7WS
x86_64
bind-sdb-chroot-9.9.4-38.el7_3.3
bind-pkcs11-utils-9.9.4-38.el7_3.3
bind-debuginfo-9.9.4-38.el7_3.3
bind-libs-9.9.4-38.el7_3.3
bind-9.9.4-38.el7_3.3
bind-libs-lite-9.9.4-38.el7_3.3
bind-chroot-9.9.4-38.el7_3.3
bind-lite-devel-9.9.4-38.el7_3.3
bind-pkcs11-libs-9.9.4-38.el7_3.3
bind-pkcs11-devel-9.9.4-38.el7_3.3
bind-utils-9.9.4-38.el7_3.3
bind-pkcs11-9.9.4-38.el7_3.3
bind-devel-9.9.4-38.el7_3.3
bind-sdb-9.9.4-38.el7_3.3

noarch
bind-license-9.9.4-38.el7_3.3

141560 - Red Hat Enterprise Linux RHSA-2017-1105 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3136, CVE-2017-3137

Description

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

RHSA-2017-1105

Observation

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

For more information see:

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00038.html>

RHEL6D

x86_64

bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-debuginfo-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

i386

bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-debuginfo-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

RHEL6S

i386

bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-debuginfo-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

x86_64

bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-debuginfo-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

RHEL6WS

x86_64

bind-debuginfo-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-9.8.2-0.62.rc1.el6_9.1

i386

bind-debuginfo-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-9.8.2-0.62.rc1.el6_9.1

141561 - Red Hat Enterprise Linux RHSA-2017-1125 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

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

RHSA-2017-1125

Observation

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

For more information see:

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00046.html>

RHEL7_2S

noarch

kernel-abi-whitelists-3.10.0-327.53.1.el7

kernel-doc-3.10.0-327.53.1.el7

x86_64

kernel-debug-debuginfo-3.10.0-327.53.1.el7

kernel-tools-libs-3.10.0-327.53.1.el7

python-perf-debuginfo-3.10.0-327.53.1.el7

perf-debuginfo-3.10.0-327.53.1.el7

kernel-debug-devel-3.10.0-327.53.1.el7

kernel-headers-3.10.0-327.53.1.el7

kernel-debuginfo-common-x86_64-3.10.0-327.53.1.el7

kernel-tools-debuginfo-3.10.0-327.53.1.el7

kernel-tools-libs-devel-3.10.0-327.53.1.el7

kernel-devel-3.10.0-327.53.1.el7

kernel-debug-3.10.0-327.53.1.el7

perf-3.10.0-327.53.1.el7

python-perf-3.10.0-327.53.1.el7

kernel-3.10.0-327.53.1.el7

kernel-debuginfo-3.10.0-327.53.1.el7

kernel-tools-3.10.0-327.53.1.el7

145315 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:1096-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0860

Description

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

SUSE-SU-2017:1096-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002827.html>

SuSE SLES 12 SP1

x86_64
update-alternatives-debugsource-1.16.10-12.6.1
update-alternatives-debuginfo-1.16.10-12.6.1
update-alternatives-1.16.10-12.6.1

SuSE SLED 12 SP1

x86_64
update-alternatives-debugsource-1.16.10-12.6.1
update-alternatives-debuginfo-1.16.10-12.6.1
update-alternatives-1.16.10-12.6.1

145318 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:1067-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4975, CVE-2015-1855, CVE-2015-3900, CVE-2015-7551, CVE-2016-2339

Description

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

SUSE-SU-2017:1067-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002820.html>

SuSE SLED 12 SP1

x86_64
ruby2.1-stdlib-debuginfo-2.1.9-15.1
ruby2.1-stdlib-2.1.9-15.1
ruby2.1-debuginfo-2.1.9-15.1
ruby2.1-debugsource-2.1.9-15.1
libruby2_1-2_1-debuginfo-2.1.9-15.1
libruby2_1-2_1-2.1.9-15.1
ruby2.1-2.1.9-15.1

SuSE SLES 12 SP2

x86_64
ruby2.1-stdlib-debuginfo-2.1.9-15.1
ruby2.1-stdlib-2.1.9-15.1
ruby2.1-debuginfo-2.1.9-15.1
ruby2.1-debugsource-2.1.9-15.1
libruby2_1-2_1-debuginfo-2.1.9-15.1
libruby2_1-2_1-2.1.9-15.1
ruby2.1-2.1.9-15.1

SuSE SLED 12 SP2

x86_64
ruby2.1-stdlib-debuginfo-2.1.9-15.1
ruby2.1-stdlib-2.1.9-15.1
ruby2.1-debuginfo-2.1.9-15.1
ruby2.1-debugsource-2.1.9-15.1
libruby2_1-2_1-debuginfo-2.1.9-15.1
libruby2_1-2_1-2.1.9-15.1
ruby2.1-2.1.9-15.1

SuSE SLES 12 SP1

x86_64
ruby2.1-stdlib-debuginfo-2.1.9-15.1
ruby2.1-stdlib-2.1.9-15.1
ruby2.1-debuginfo-2.1.9-15.1
ruby2.1-debugsource-2.1.9-15.1
libruby2_1-2_1-debuginfo-2.1.9-15.1
libruby2_1-2_1-2.1.9-15.1
ruby2.1-2.1.9-15.1

145320 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:1092-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7467

Description

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

SUSE-SU-2017:1092-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002823.html>

SuSE SLED 12 SP1

x86_64
minicom-debugsource-2.7-3.1
minicom-debuginfo-2.7-3.1
minicom-2.7-3.1

SuSE SLES 12 SP2

x86_64
minicom-debugsource-2.7-3.1
minicom-debuginfo-2.7-3.1
minicom-2.7-3.1

SuSE SLED 12 SP2

x86_64
minicom-debugsource-2.7-3.1
minicom-debuginfo-2.7-3.1
minicom-2.7-3.1

SuSE SLES 12 SP1

x86_64
minicom-debugsource-2.7-3.1
minicom-debuginfo-2.7-3.1
minicom-2.7-3.1

145323 - SuSE SLES 11 SP4 SUSE-SU-2017:1081-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9603, CVE-2017-2633, CVE-2017-6414, CVE-2017-6505, CVE-2017-7228

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1081-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002822.html>

SuSE SLES 11 SP4

x86_64
xen-doc-html-4.4.4_16-54.1
xen-libs-32bit-4.4.4_16-54.1
xen-libs-4.4.4_16-54.1
xen-tools-domU-4.4.4_16-54.1
xen-tools-4.4.4_16-54.1
xen-4.4.4_16-54.1
xen-kmp-default-4.4.4_16_3.0.101_97-54.1

i586

xen-kmp-default-4.4.4_16_3.0.101_97-54.1
xen-kmp-pae-4.4.4_16_3.0.101_97-54.1
xen-libs-4.4.4_16-54.1
xen-tools-domU-4.4.4_16-54.1

160240 - CentOS 6 CESA-2017-1105 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3136, CVE-2017-3137

Description

The scan detected that the host is missing the following update:
CESA-2017-1105

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-April/022393.html>

CentOS 6

x86_64
bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

i686

bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

160241 - CentOS 7 CESA-2017-0987 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9603

Description

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

CESA-2017-0987

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2017-April/022387.html>

CentOS 7

x86_64

qemu-kvm-1.5.3-126.el7_3.6

qemu-kvm-tools-1.5.3-126.el7_3.6

qemu-kvm-common-1.5.3-126.el7_3.6

qemu-img-1.5.3-126.el7_3.6

160243 - CentOS 7 CESA-2017-1095 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3136, CVE-2017-3137

Description

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

CESA-2017-1095

Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2017-April/022390.html>

CentOS 7

i686

bind-lite-devel-9.9.4-38.el7_3.3

bind-pkcs11-devel-9.9.4-38.el7_3.3

bind-libs-lite-9.9.4-38.el7_3.3

bind-libs-9.9.4-38.el7_3.3

bind-pkcs11-libs-9.9.4-38.el7_3.3

bind-devel-9.9.4-38.el7_3.3

noarch

bind-license-9.9.4-38.el7_3.3

x86_64

bind-9.9.4-38.el7_3.3

bind-pkcs11-utils-9.9.4-38.el7_3.3

bind-libs-9.9.4-38.el7_3.3

bind-sdb-chroot-9.9.4-38.el7_3.3

bind-libs-lite-9.9.4-38.el7_3.3
bind-chroot-9.9.4-38.el7_3.3
bind-lite-devel-9.9.4-38.el7_3.3
bind-pkcs11-libs-9.9.4-38.el7_3.3
bind-pkcs11-devel-9.9.4-38.el7_3.3
bind-utils-9.9.4-38.el7_3.3
bind-pkcs11-9.9.4-38.el7_3.3
bind-devel-9.9.4-38.el7_3.3
bind-sdb-9.9.4-38.el7_3.3

163336 - Oracle Enterprise Linux ELSA-2017-1105 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3136, CVE-2017-3137

Description

The scan detected that the host is missing the following update:
ELSA-2017-1105

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006872.html>

OEL6

x86_64
bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

i386

bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

163341 - Oracle Enterprise Linux ELSA-2017-1095 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3136, CVE-2017-3137

Description

The scan detected that the host is missing the following update:
ELSA-2017-1095

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006870.html>

OEL7

x86_64

bind-libs-lite-9.9.4-38.el7_3.3

bind-sdb-chroot-9.9.4-38.el7_3.3

bind-pkcs11-utils-9.9.4-38.el7_3.3

bind-libs-9.9.4-38.el7_3.3

bind-9.9.4-38.el7_3.3

bind-license-9.9.4-38.el7_3.3

bind-chroot-9.9.4-38.el7_3.3

bind-lite-devel-9.9.4-38.el7_3.3

bind-pkcs11-libs-9.9.4-38.el7_3.3

bind-pkcs11-devel-9.9.4-38.el7_3.3

bind-utils-9.9.4-38.el7_3.3

bind-pkcs11-9.9.4-38.el7_3.3

bind-devel-9.9.4-38.el7_3.3

bind-sdb-9.9.4-38.el7_3.3

170797 - Amazon Linux AMI ALAS-2017-820 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684, CVE-2016-9830, CVE-2017-6335

Description

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

ALAS-2017-820

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2017-820.html>

Amazon Linux AMI

i686

GraphicsMagick-devel-1.3.25-6.10.amzn1

GraphicsMagick-perl-1.3.25-6.10.amzn1

GraphicsMagick-c++-1.3.25-6.10.amzn1

GraphicsMagick-c++-devel-1.3.25-6.10.amzn1

GraphicsMagick-1.3.25-6.10.amzn1

GraphicsMagick-debuginfo-1.3.25-6.10.amzn1

noarch

GraphicsMagick-doc-1.3.25-6.10.amzn1

x86_64

GraphicsMagick-devel-1.3.25-6.10.amzn1

GraphicsMagick-perl-1.3.25-6.10.amzn1

GraphicsMagick-c++-1.3.25-6.10.amzn1

GraphicsMagick-c++-devel-1.3.25-6.10.amzn1

GraphicsMagick-1.3.25-6.10.amzn1

GraphicsMagick-debuginfo-1.3.25-6.10.amzn1

175159 - Scientific Linux Security ERRATA Important: bind on SL7.x x86_64 (1704-16936)

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

Risk Level: High

CVE: CVE-2017-3136, CVE-2017-3137

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL7.x x86_64 (1704-16936)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=16936>

SL7

x86_64

bind-sdb-chroot-9.9.4-38.el7_3.3
bind-pkcs11-utils-9.9.4-38.el7_3.3
bind-debuginfo-9.9.4-38.el7_3.3
bind-libs-9.9.4-38.el7_3.3
bind-9.9.4-38.el7_3.3
bind-libs-lite-9.9.4-38.el7_3.3
bind-chroot-9.9.4-38.el7_3.3
bind-lite-devel-9.9.4-38.el7_3.3
bind-pkcs11-libs-9.9.4-38.el7_3.3
bind-pkcs11-devel-9.9.4-38.el7_3.3
bind-utils-9.9.4-38.el7_3.3
bind-pkcs11-9.9.4-38.el7_3.3
bind-devel-9.9.4-38.el7_3.3
bind-sdb-9.9.4-38.el7_3.3

noarch

bind-license-9.9.4-38.el7_3.3

175163 - Scientific Linux Security ERRATA Important: bind on SL6.x i386/x86_64 (1704-17615)

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

Risk Level: High

CVE: CVE-2017-3136, CVE-2017-3137

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL6.x i386/x86_64 (1704-17615)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=17615>

SL6

x86_64

bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-debuginfo-9.8.2-0.62.rc1.el6_9.1

bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

i386

bind-9.8.2-0.62.rc1.el6_9.1
bind-libs-9.8.2-0.62.rc1.el6_9.1
bind-sdb-9.8.2-0.62.rc1.el6_9.1
bind-debuginfo-9.8.2-0.62.rc1.el6_9.1
bind-utils-9.8.2-0.62.rc1.el6_9.1
bind-devel-9.8.2-0.62.rc1.el6_9.1
bind-chroot-9.8.2-0.62.rc1.el6_9.1

182330 - FreeBSD libevent Multiple Vulnerabilities (b8ee7a81-a879-4358-9b30-7dd1bd4c14b1)

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197

Description

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

libevent -- multiple vulnerabilities (b8ee7a81-a879-4358-9b30-7dd1bd4c14b1)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/b8ee7a81-a879-4358-9b30-7dd1bd4c14b1.html>

Affected packages:

libevent < 2.1.6
libevent2 < 2.1.6
linux-c6-libevent2 < 2.1.6
linux-c7-libevent < 2.1.6

182335 - FreeBSD tiff Multiple Vulnerabilities (2a96e498-3234-4950-a9ad-419bc84a839d)

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

Risk Level: High

CVE: CVE-2017-5225, CVE-2017-7592, CVE-2017-7593, CVE-2017-7594, CVE-2017-7595, CVE-2017-7596, CVE-2017-7597, CVE-2017-7598, CVE-2017-7599, CVE-2017-7600, CVE-2017-7601, CVE-2017-7602

Description

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

tiff -- multiple vulnerabilities (2a96e498-3234-4950-a9ad-419bc84a839d)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/2a96e498-3234-4950-a9ad-419bc84a839d.html>

Affected packages:

tiff < 4.0.8
linux-f8-tiff < 4.0.8
linux-f10-tiff < 4.0.8

linux-c6-tiff < 4.0.8
linux-c7-tiff < 4.0.8

185664 - Ubuntu Linux 14.04 USN-3265-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5669, CVE-2017-5897, CVE-2017-5970, CVE-2017-5986, CVE-2017-6214, CVE-2017-6345, CVE-2017-6346, CVE-2017-6347, CVE-2017-6348, CVE-2017-7374

Description

The scan detected that the host is missing the following update:
USN-3265-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003824.html>

Ubuntu 14.04

linux-image-4.4.0-75-generic_4.4.0-75.96~14.04.1
linux-image-4.4.0-75-powerpc-e500mc_4.4.0-75.96~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.75.62
linux-image-powerpc-smp-lts-xenial_4.4.0.75.62
linux-image-4.4.0-75-lowlatency_4.4.0-75.96~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.75.62
linux-image-powerpc-e500mc-lts-xenial_4.4.0.75.62
linux-image-4.4.0-75-generic-lpae_4.4.0-75.96~14.04.1
linux-image-generic-lts-xenial_4.4.0.75.62
linux-image-generic-lpae-lts-xenial_4.4.0.75.62
linux-image-4.4.0-75-powerpc64-smp_4.4.0-75.96~14.04.1
linux-image-4.4.0-75-powerpc-smp_4.4.0-75.96~14.04.1

185665 - Ubuntu Linux 16.04 USN-3266-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5986

Description

The scan detected that the host is missing the following update:
USN-3266-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003826.html>

Ubuntu 16.04

linux-image-generic-hwe-16.04_4.8.0.49.21
linux-image-4.8.0-49-generic_4.8.0-49.52~16.04.1
linux-image-lowlatency-hwe-16.04_4.8.0.49.21

linux-image-4.8.0-49-lowlatency_4.8.0-49.52~16.04.1
linux-image-generic-lpae-hwe-16.04_4.8.0.49.21
linux-image-4.8.0-49-generic-lpae_4.8.0-49.52~16.04.1

185669 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10, 17.04 USN-3263-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10328

Description

The scan detected that the host is missing the following update:
USN-3263-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003819.html>

Ubuntu 12.04

libfreetype6_2.4.8-1ubuntu2.5

Ubuntu 16.04

libfreetype6_2.6.1-0.1ubuntu2.2

Ubuntu 14.04

libfreetype6_2.5.2-1ubuntu2.7

Ubuntu 16.10

libfreetype6_2.6.3-3ubuntu1.2

Ubuntu 17.04

libfreetype6_2.6.3-3ubuntu2.1

185670 - Ubuntu Linux 14.04 USN-3264-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5986

Description

The scan detected that the host is missing the following update:
USN-3264-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003821.html>

Ubuntu 14.04

linux-image-3.13.0-117-powerpc64-smp_3.13.0-117.164
linux-image-powerpc-e500mc_3.13.0.117.127
linux-image-lowlatency_3.13.0.117.127
linux-image-generic_3.13.0.117.127
linux-image-generic-lpae_3.13.0.117.127
linux-image-powerpc-smp_3.13.0.117.127
linux-image-3.13.0-117-powerpc-e500mc_3.13.0-117.164
linux-image-3.13.0-117-powerpc-smp_3.13.0-117.164
linux-image-3.13.0-117-generic_3.13.0-117.164
linux-image-powerpc-e500_3.13.0.117.127
linux-image-3.13.0-117-generic-lpae_3.13.0-117.164
linux-image-3.13.0-117-powerpc-e500_3.13.0-117.164
linux-image-powerpc64-smp_3.13.0.117.127
linux-image-3.13.0-117-lowlatency_3.13.0-117.164

185673 - Ubuntu Linux 16.04 USN-3265-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5669, CVE-2017-5897, CVE-2017-5970, CVE-2017-5986, CVE-2017-6214, CVE-2017-6345, CVE-2017-6346, CVE-2017-6347, CVE-2017-6348, CVE-2017-7374

Description

The scan detected that the host is missing the following update:
USN-3265-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003823.html>

Ubuntu 16.04

linux-image-powerpc64-smp_4.4.0.75.81
linux-image-gke_4.4.0.1012.14
linux-image-4.4.0-75-generic-lpae_4.4.0-75.96
linux-image-generic_4.4.0.75.81
linux-image-generic-lpae_4.4.0.75.81
linux-image-4.4.0-75-generic_4.4.0-75.96
linux-image-powerpc-e500mc_4.4.0.75.81
linux-image-4.4.0-1054-raspi2_4.4.0-1054.61
linux-image-4.4.0-1057-snapdragon_4.4.0-1057.61
linux-image-4.4.0-75-powerpc64-smp_4.4.0-75.96
linux-image-4.4.0-75-powerpc-smp_4.4.0-75.96
linux-image-aws_4.4.0.1016.19
linux-image-lowlatency_4.4.0.75.81
linux-image-4.4.0-75-lowlatency_4.4.0-75.96
linux-image-snapdragon_4.4.0.1057.50
linux-image-4.4.0-1012-gke_4.4.0-1012.12
linux-image-4.4.0-1016-aws_4.4.0-1016.25
linux-image-powerpc-smp_4.4.0.75.81
linux-image-raspi2_4.4.0.1054.55
linux-image-4.4.0-75-powerpc-e500mc_4.4.0-75.96

185674 - Ubuntu Linux 12.04 USN-3264-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5986

Description

The scan detected that the host is missing the following update:
USN-3264-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003822.html>

Ubuntu 12.04

linux-image-3.13.0-117-generic_3.13.0-117.164~precise1
linux-image-3.13.0-117-generic-lpae_3.13.0-117.164~precise1
linux-image-generic-lpae-lts-trusty_3.13.0.117.108
linux-image-generic-lts-trusty_3.13.0.117.108

185675 - Ubuntu Linux 16.10 USN-3266-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5986

Description

The scan detected that the host is missing the following update:
USN-3266-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003825.html>

Ubuntu 16.10

linux-image-generic-lpae_4.8.0.49.61
linux-image-lowlatency_4.8.0.49.61
linux-image-4.8.0-49-lowlatency_4.8.0-49.52
linux-image-generic_4.8.0.49.61
linux-image-4.8.0-49-powerpc-e500mc_4.8.0-49.52
linux-image-powerpc-smp_4.8.0.49.61
linux-image-raspi2_4.8.0.1035.39
linux-image-4.8.0-49-generic_4.8.0-49.52
linux-image-4.8.0-49-powerpc-smp_4.8.0-49.52
linux-image-powerpc-e500mc_4.8.0.49.61
linux-image-4.8.0-1035-raspi2_4.8.0-1035.38
linux-image-4.8.0-49-generic-lpae_4.8.0-49.52

191977 - Fedora Linux 25 FEDORA-2017-34f6e70fdd Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0553

Description

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

FEDORA-2017-34f6e70fdd

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/2017/4/?count=200&page=1>

Fedora Core 25

libnl3-3.2.29-3.fc25

191983 - Fedora Linux 25 FEDORA-2017-15e7445d67 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9275, CVE-2016-9276, CVE-2016-9480, CVE-2016-9558

Description

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

FEDORA-2017-15e7445d67

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/2017/4/?count=200&page=1>

Fedora Core 25

libdwarf-20170416-1.fc25

88860 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-112-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9042, CVE-2017-6451, CVE-2017-6452, CVE-2017-6455, CVE-2017-6458, CVE-2017-6459, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

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

SSA:2017-112-02

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=2017&m=slackware-security.648848>

Slackware 14.0
x86_64
ntp-4.2.8p10-x86_64-1

Slackware 13.37
x86_64
ntp-4.2.8p10-x86_64-1

Slackware 14.1
x86_64
ntp-4.2.8p10-x86_64-1

Slackware 13.1
x86_64
ntp-4.2.8p10-x86_64-1

Slackware 14.2
x86_64
ntp-4.2.8p10-x86_64-1

i586
ntp-4.2.8p10-i586-1

Slackware 13.0
x86_64
ntp-4.2.8p10-x86_64-1

132360 - Oracle VM OVMSA-2017-0065 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1950

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0065

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000683.html>

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000682.html>

OVM3.3
x86_64
nss-3.28.4-1.0.1.el6_9
nss-util-3.28.4-1.el6_9
nss-tools-3.28.4-1.0.1.el6_9
nss-sysinit-3.28.4-1.0.1.el6_9

OVM3.4
x86_64
nss-3.28.4-1.0.1.el6_9
nss-util-3.28.4-1.el6_9
nss-tools-3.28.4-1.0.1.el6_9
nss-sysinit-3.28.4-1.0.1.el6_9

145316 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:1094-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7392, CVE-2017-7393, CVE-2017-7394, CVE-2017-7395, CVE-2017-7396

Description

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

SUSE-SU-2017:1094-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002825.html>

SuSE SLED 12 SP2

x86_64

xorg-x11-Xvnc-1.6.0-18.11.1

xorg-x11-Xvnc-debuginfo-1.6.0-18.11.1

tigervnc-debugsource-1.6.0-18.11.1

tigervnc-debuginfo-1.6.0-18.11.1

libXvnc1-1.6.0-18.11.1

libXvnc1-debuginfo-1.6.0-18.11.1

tigervnc-1.6.0-18.11.1

SuSE SLES 12 SP2

x86_64

xorg-x11-Xvnc-1.6.0-18.11.1

xorg-x11-Xvnc-debuginfo-1.6.0-18.11.1

tigervnc-debugsource-1.6.0-18.11.1

tigervnc-debuginfo-1.6.0-18.11.1

libXvnc1-1.6.0-18.11.1

libXvnc1-debuginfo-1.6.0-18.11.1

tigervnc-1.6.0-18.11.1

145322 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:1093-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7392, CVE-2017-7393, CVE-2017-7394, CVE-2017-7395, CVE-2017-7396

Description

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

SUSE-SU-2017:1093-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002824.html>

SuSE SLES 12 SP1

x86_64

xorg-x11-Xvnc-debuginfo-1.4.3-24.1

tigervnc-debugsource-1.4.3-24.1

tigervnc-debuginfo-1.4.3-24.1
xorg-x11-Xvnc-1.4.3-24.1
tigervnc-1.4.3-24.1

SuSE SLED 12 SP1
x86_64
xorg-x11-Xvnc-debuginfo-1.4.3-24.1
tigervnc-debugsource-1.4.3-24.1
tigervnc-debuginfo-1.4.3-24.1
xorg-x11-Xvnc-1.4.3-24.1
tigervnc-1.4.3-24.1

170795 - Amazon Linux AMI ALAS-2017-816 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6451, CVE-2017-6458, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
ALAS-2017-816

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-816.html>

Amazon Linux AMI
i686
ntpdate-4.2.6p5-44.34.amzn1
ntp-4.2.6p5-44.34.amzn1
ntp-debuginfo-4.2.6p5-44.34.amzn1

noarch
ntp-doc-4.2.6p5-44.34.amzn1
ntp-perl-4.2.6p5-44.34.amzn1

x86_64
ntpdate-4.2.6p5-44.34.amzn1
ntp-4.2.6p5-44.34.amzn1
ntp-debuginfo-4.2.6p5-44.34.amzn1

170799 - Amazon Linux AMI ALAS-2017-822 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5647, CVE-2017-5648

Description

The scan detected that the host is missing the following update:
ALAS-2017-822

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-822.html>

Amazon Linux AMI

noarch
tomcat7-jsp-2.2-api-7.0.77-1.26.amzn1
tomcat7-log4j-7.0.77-1.26.amzn1
tomcat7-el-2.2-api-7.0.77-1.26.amzn1
tomcat7-servlet-3.0-api-7.0.77-1.26.amzn1
tomcat7-lib-7.0.77-1.26.amzn1
tomcat8-javadoc-8.0.43-1.70.amzn1
tomcat8-log4j-8.0.43-1.70.amzn1
tomcat8-admin-webapps-8.0.43-1.70.amzn1
tomcat8-lib-8.0.43-1.70.amzn1
tomcat7-javadoc-7.0.77-1.26.amzn1
tomcat8-servlet-3.1-api-8.0.43-1.70.amzn1
tomcat7-admin-webapps-7.0.77-1.26.amzn1
tomcat7-docs-webapp-7.0.77-1.26.amzn1
tomcat7-7.0.77-1.26.amzn1
tomcat8-el-3.0-api-8.0.43-1.70.amzn1
tomcat8-docs-webapp-8.0.43-1.70.amzn1
tomcat7-webapps-7.0.77-1.26.amzn1
tomcat8-jsp-2.3-api-8.0.43-1.70.amzn1
tomcat8-webapps-8.0.43-1.70.amzn1
tomcat8-8.0.43-1.70.amzn1

182336 - FreeBSD drupal8 Drupal Core - Critical - Access Bypass (1455c86c-26c2-11e7-9daa-6cf0497db129)

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

Risk Level: Medium

CVE: CVE-2017-6919

Description

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

drupal8 -- Drupal Core - Critical - Access Bypass (1455c86c-26c2-11e7-9daa-6cf0497db129)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/1455c86c-26c2-11e7-9daa-6cf0497db129.html>

Affected packages:

drupal8 < 8.3.1

185666 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3261-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10028, CVE-2016-10029, CVE-2016-10155, CVE-2016-7907, CVE-2016-8667, CVE-2016-8669, CVE-2016-9381, CVE-2016-9602, CVE-2016-9603, CVE-2016-9776, CVE-2016-9845, CVE-2016-9846, CVE-2016-9907, CVE-2016-9908, CVE-2016-9911, CVE-2016-9912, CVE-2016-9913, CVE-2016-9914, CVE-2016-9915, CVE-2016-9916, CVE-2016-9921, CVE-2016-9922, CVE-2017-2615, CVE-2017-2620, CVE-2017-2633, CVE-2017-5525, CVE-2017-5526, CVE-2017-5552, CVE-2017-5578, CVE-2017-5579, CVE-2017-5667, CVE-2017-5856, CVE-2017-5857, CVE-2017-5898, CVE-2017-5973, CVE-2017-5987, CVE-2017-6505

Description

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

USN-3261-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003816.html>

Ubuntu 16.04

qemu-system-ppc_2.5+dfsg-5ubuntu10.11
qemu-system_2.5+dfsg-5ubuntu10.11
qemu-system-x86_2.5+dfsg-5ubuntu10.11
qemu-system-s390x_2.5+dfsg-5ubuntu10.11
qemu-system-mips_2.5+dfsg-5ubuntu10.11
qemu-system-aarch64_2.5+dfsg-5ubuntu10.11
qemu-system-sparc_2.5+dfsg-5ubuntu10.11
qemu-system-misc_2.5+dfsg-5ubuntu10.11
qemu-system-arm_2.5+dfsg-5ubuntu10.11

Ubuntu 14.04

qemu-system-sparc_2.0.0+dfsg-2ubuntu1.33
qemu-system-misc_2.0.0+dfsg-2ubuntu1.33
qemu-system_2.0.0+dfsg-2ubuntu1.33
qemu-system-mips_2.0.0+dfsg-2ubuntu1.33
qemu-system-aarch64_2.0.0+dfsg-2ubuntu1.33
qemu-system-x86_2.0.0+dfsg-2ubuntu1.33
qemu-system-arm_2.0.0+dfsg-2ubuntu1.33
qemu-system-ppc_2.0.0+dfsg-2ubuntu1.33

Ubuntu 16.10

qemu-system-misc_2.6.1+dfsg-0ubuntu5.4
qemu-system-arm_2.6.1+dfsg-0ubuntu5.4
qemu-system-mips_2.6.1+dfsg-0ubuntu5.4
qemu-system-x86_2.6.1+dfsg-0ubuntu5.4
qemu-system_2.6.1+dfsg-0ubuntu5.4
qemu-system-ppc_2.6.1+dfsg-0ubuntu5.4
qemu-system-s390x_2.6.1+dfsg-0ubuntu5.4
qemu-system-aarch64_2.6.1+dfsg-0ubuntu5.4
qemu-system-sparc_2.6.1+dfsg-0ubuntu5.4

191984 - Fedora Linux 25 FEDORA-2017-d43d46f1ca Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9264, CVE-2016-9265, CVE-2016-9266, CVE-2016-9827, CVE-2016-9828, CVE-2016-9829, CVE-2016-9831, CVE-2017-7578

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d43d46f1ca

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/2017/4/?count=200&page=3>

Fedora Core 25

ming-0.4.8-1.fc25

192013 - Fedora Linux 24 FEDORA-2017-a66ca10c22 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7392, CVE-2017-7393, CVE-2017-7394, CVE-2017-7395, CVE-2017-7396

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a66ca10c22

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/2017/4/?count=200&page=1>

Fedora Core 24

tigervnc-1.7.1-4.fc24

130744 - Debian Linux 8.0 DSA-3830-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7867, CVE-2017-7868

Description

The scan detected that the host is missing the following update:
DSA-3830-1

Observation

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

<http://www.debian.org/security/2017/dsa-3830>

Debian 8.0

all

libicu-dev_52.1-8+deb8u5

icu-doc_52.1-8+deb8u5

libicu52_52.1-8+deb8u5

icu-devtools_52.1-8+deb8u5

libicu52-dbg_52.1-8+deb8u5

130746 - Debian Linux 8.0 DSA-3834-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5483, CVE-2017-3302, CVE-2017-3305, CVE-2017-3308, CVE-2017-3309, CVE-2017-3329, CVE-2017-3453, CVE-

2017-3456, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3600

Description

The scan detected that the host is missing the following update:
DSA-3834-1

Observation

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

<http://www.debian.org/security/2017/dsa-3834>

Debian 8.0

all

mysql-source-5.5_5.5.55-0+deb8u1

libmysqld-pic_5.5.55-0+deb8u1

mysql-server_5.5.55-0+deb8u1

mysql-server-core-5.5_5.5.55-0+deb8u1

libmysqld-dev_5.5.55-0+deb8u1

mysql-client-5.5_5.5.55-0+deb8u1

mysql-client_5.5.55-0+deb8u1

mysql-testsuite-5.5_5.5.55-0+deb8u1

mysql-testsuite_5.5.55-0+deb8u1

libmysqlclient18_5.5.55-0+deb8u1

libmysqlclient-dev_5.5.55-0+deb8u1

mysql-server-5.5_5.5.55-0+deb8u1

mysql-common_5.5.55-0+deb8u1

141548 - Red Hat Enterprise Linux RHSA-2017-1118 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
RHSA-2017-1118

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00043.html>

RHEL7D

x86_64

java-1.7.0-oracle-jdbc-1.7.0.141-1jpp.1.el7_3

java-1.7.0-oracle-plugin-1.7.0.141-1jpp.1.el7_3

java-1.7.0-oracle-src-1.7.0.141-1jpp.1.el7_3

java-1.7.0-oracle-devel-1.7.0.141-1jpp.1.el7_3

java-1.7.0-oracle-javafx-1.7.0.141-1jpp.1.el7_3

java-1.7.0-oracle-1.7.0.141-1jpp.1.el7_3

RHEL7S

x86_64

java-1.7.0-oracle-jdbc-1.7.0.141-1jpp.1.el7_3

java-1.7.0-oracle-plugin-1.7.0.141-1jpp.1.el7_3

java-1.7.0-oracle-src-1.7.0.141-1jpp.1.el7_3
java-1.7.0-oracle-devel-1.7.0.141-1jpp.1.el7_3
java-1.7.0-oracle-javafx-1.7.0.141-1jpp.1.el7_3
java-1.7.0-oracle-1.7.0.141-1jpp.1.el7_3

RHEL7WS

x86_64

java-1.7.0-oracle-jdbc-1.7.0.141-1jpp.1.el7_3
java-1.7.0-oracle-plugin-1.7.0.141-1jpp.1.el7_3
java-1.7.0-oracle-src-1.7.0.141-1jpp.1.el7_3
java-1.7.0-oracle-devel-1.7.0.141-1jpp.1.el7_3
java-1.7.0-oracle-javafx-1.7.0.141-1jpp.1.el7_3
java-1.7.0-oracle-1.7.0.141-1jpp.1.el7_3

141556 - Red Hat Enterprise Linux RHSA-2017-1117 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

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

RHSA-2017-1117

Observation

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

For more information see:

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00042.html>

RHEL7D

x86_64

java-1.8.0-oracle-devel-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-javafx-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-src-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-jdbc-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-plugin-1.8.0.131-1jpp.1.el7_3

RHEL7S

x86_64

java-1.8.0-oracle-devel-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-javafx-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-src-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-jdbc-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-plugin-1.8.0.131-1jpp.1.el7_3

RHEL7WS

x86_64

java-1.8.0-oracle-devel-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-javafx-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-src-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-jdbc-1.8.0.131-1jpp.1.el7_3
java-1.8.0-oracle-plugin-1.8.0.131-1jpp.1.el7_3

141559 - Red Hat Enterprise Linux RHSA-2017-1119 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3509, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
RHSA-2017-1119

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00044.html>

RHEL7D

x86_64

java-1.6.0-sun-demo-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-jdbc-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-plugin-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-devel-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-src-1.6.0.151-1jpp.1.el7_3

RHEL7S

x86_64

java-1.6.0-sun-demo-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-jdbc-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-plugin-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-devel-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-src-1.6.0.151-1jpp.1.el7_3

RHEL7WS

x86_64

java-1.6.0-sun-demo-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-jdbc-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-plugin-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-devel-1.6.0.151-1jpp.1.el7_3

java-1.6.0-sun-src-1.6.0.151-1jpp.1.el7_3

160242 - CentOS 6 CESA-2017-0979 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

The scan detected that the host is missing the following update:
CESA-2017-0979

Observation

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

CentOS 6

i686

libreoffice-langpack-cy-4.3.7.2-2.el6_9.1
libreoffice-langpack-fr-4.3.7.2-2.el6_9.1
libreoffice-langpack-zu-4.3.7.2-2.el6_9.1
libreoffice-langpack-da-4.3.7.2-2.el6_9.1
libreoffice-langpack-ml-4.3.7.2-2.el6_9.1
libreoffice-langpack-sv-4.3.7.2-2.el6_9.1
libreoffice-langpack-af-4.3.7.2-2.el6_9.1
libreoffice-langpack-et-4.3.7.2-2.el6_9.1
libreoffice-langpack-cs-4.3.7.2-2.el6_9.1
libreoffice-langpack-dz-4.3.7.2-2.el6_9.1
libreoffice-langpack-uk-4.3.7.2-2.el6_9.1
libreoffice-langpack-sk-4.3.7.2-2.el6_9.1
libreoffice-langpack-he-4.3.7.2-2.el6_9.1
libreoffice-core-4.3.7.2-2.el6_9.1
libreoffice-langpack-ga-4.3.7.2-2.el6_9.1
libreoffice-langpack-ro-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hant-4.3.7.2-2.el6_9.1
libreoffice-langpack-xh-4.3.7.2-2.el6_9.1
libreoffice-glade-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-BR-4.3.7.2-2.el6_9.1
libreoffice-langpack-ar-4.3.7.2-2.el6_9.1
libreoffice-langpack-lt-4.3.7.2-2.el6_9.1
libreoffice-langpack-ta-4.3.7.2-2.el6_9.1
libreoffice-langpack-bn-4.3.7.2-2.el6_9.1
libreoffice-langpack-bg-4.3.7.2-2.el6_9.1
libreoffice-langpack-st-4.3.7.2-2.el6_9.1
libreoffice-langpack-ts-4.3.7.2-2.el6_9.1
libreoffice-calc-4.3.7.2-2.el6_9.1
libreoffice-langpack-hi-4.3.7.2-2.el6_9.1
libreoffice-langpack-nb-4.3.7.2-2.el6_9.1
libreoffice-langpack-gu-4.3.7.2-2.el6_9.1
libreoffice-base-4.3.7.2-2.el6_9.1
libreoffice-langpack-as-4.3.7.2-2.el6_9.1
libreoffice-sdk-4.3.7.2-2.el6_9.1
libreoffice-xsltfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-ca-4.3.7.2-2.el6_9.1
libreoffice-langpack-nso-4.3.7.2-2.el6_9.1
libreoffice-langpack-ms-4.3.7.2-2.el6_9.1
libreoffice-langpack-ja-4.3.7.2-2.el6_9.1
libreoffice-gdb-debug-support-4.3.7.2-2.el6_9.1
libreoffice-langpack-es-4.3.7.2-2.el6_9.1
libreoffice-langpack-it-4.3.7.2-2.el6_9.1
libreoffice-writer-4.3.7.2-2.el6_9.1
libreoffice-langpack-ru-4.3.7.2-2.el6_9.1
libreoffice-langpack-ss-4.3.7.2-2.el6_9.1
libreoffice-graphicfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-sl-4.3.7.2-2.el6_9.1
libreoffice-langpack-nn-4.3.7.2-2.el6_9.1
libreoffice-langpack-en-4.3.7.2-2.el6_9.1
libreoffice-pdfimport-4.3.7.2-2.el6_9.1
libreoffice-langpack-ve-4.3.7.2-2.el6_9.1
libreoffice-langpack-nr-4.3.7.2-2.el6_9.1
libreoffice-langpack-fi-4.3.7.2-2.el6_9.1
libreoffice-langpack-th-4.3.7.2-2.el6_9.1
libreoffice-4.3.7.2-2.el6_9.1
libreoffice-impress-4.3.7.2-2.el6_9.1

libreoffice-langpack-eu-4.3.7.2-2.el6_9.1
libreoffice-langpack-ko-4.3.7.2-2.el6_9.1
libreoffice-headless-4.3.7.2-2.el6_9.1
libreoffice-bsh-4.3.7.2-2.el6_9.1
libreoffice-langpack-pa-4.3.7.2-2.el6_9.1
libreoffice-wiki-publisher-4.3.7.2-2.el6_9.1
libreoffice-langpack-mai-4.3.7.2-2.el6_9.1
libreoffice-langpack-gl-4.3.7.2-2.el6_9.1
libreoffice-langpack-te-4.3.7.2-2.el6_9.1
libreoffice-langpack-nl-4.3.7.2-2.el6_9.1
libreoffice-pyuno-4.3.7.2-2.el6_9.1
libreoffice-langpack-el-4.3.7.2-2.el6_9.1
libreoffice-langpack-tn-4.3.7.2-2.el6_9.1
libreoffice-langpack-ur-4.3.7.2-2.el6_9.1
libreoffice-langpack-sr-4.3.7.2-2.el6_9.1
libreoffice-ogltrans-4.3.7.2-2.el6_9.1
libreoffice-langpack-tr-4.3.7.2-2.el6_9.1
libreoffice-emailmerge-4.3.7.2-2.el6_9.1
libreoffice-sdk-doc-4.3.7.2-2.el6_9.1
libreoffice-filters-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-PT-4.3.7.2-2.el6_9.1
libreoffice-langpack-or-4.3.7.2-2.el6_9.1
libreoffice-langpack-kn-4.3.7.2-2.el6_9.1
libreoffice-ure-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hans-4.3.7.2-2.el6_9.1
libreoffice-draw-4.3.7.2-2.el6_9.1
libreoffice-langpack-mr-4.3.7.2-2.el6_9.1
libreoffice-nlpsolver-4.3.7.2-2.el6_9.1
libreoffice-officebean-4.3.7.2-2.el6_9.1
libreoffice-langpack-pl-4.3.7.2-2.el6_9.1
libreoffice-librelogo-4.3.7.2-2.el6_9.1
libreoffice-langpack-hr-4.3.7.2-2.el6_9.1
libreoffice-rhino-4.3.7.2-2.el6_9.1
libreoffice-langpack-de-4.3.7.2-2.el6_9.1
libreoffice-math-4.3.7.2-2.el6_9.1
libreoffice-langpack-hu-4.3.7.2-2.el6_9.1

noarch

autocorr-pl-4.3.7.2-2.el6_9.1
autocorr-cs-4.3.7.2-2.el6_9.1
autocorr-ro-4.3.7.2-2.el6_9.1
autocorr-hr-4.3.7.2-2.el6_9.1
autocorr-tr-4.3.7.2-2.el6_9.1
autocorr-de-4.3.7.2-2.el6_9.1
autocorr-sl-4.3.7.2-2.el6_9.1
autocorr-ga-4.3.7.2-2.el6_9.1
autocorr-lb-4.3.7.2-2.el6_9.1
autocorr-vi-4.3.7.2-2.el6_9.1
autocorr-sr-4.3.7.2-2.el6_9.1
autocorr-en-4.3.7.2-2.el6_9.1
libreoffice-opensymbol-fonts-4.3.7.2-2.el6_9.1
autocorr-sv-4.3.7.2-2.el6_9.1
autocorr-da-4.3.7.2-2.el6_9.1
autocorr-lt-4.3.7.2-2.el6_9.1
autocorr-fa-4.3.7.2-2.el6_9.1
autocorr-hu-4.3.7.2-2.el6_9.1
autocorr-nl-4.3.7.2-2.el6_9.1
autocorr-ca-4.3.7.2-2.el6_9.1
autocorr-pt-4.3.7.2-2.el6_9.1
autocorr-ko-4.3.7.2-2.el6_9.1

autocorr-ru-4.3.7.2-2.el6_9.1
autocorr-is-4.3.7.2-2.el6_9.1
autocorr-ja-4.3.7.2-2.el6_9.1
autocorr-sk-4.3.7.2-2.el6_9.1
autocorr-zh-4.3.7.2-2.el6_9.1
autocorr-mn-4.3.7.2-2.el6_9.1
autocorr-it-4.3.7.2-2.el6_9.1
autocorr-es-4.3.7.2-2.el6_9.1
autocorr-af-4.3.7.2-2.el6_9.1
autocorr-fr-4.3.7.2-2.el6_9.1
autocorr-bg-4.3.7.2-2.el6_9.1
autocorr-fi-4.3.7.2-2.el6_9.1

x86_64

libreoffice-langpack-cy-4.3.7.2-2.el6_9.1
libreoffice-langpack-fr-4.3.7.2-2.el6_9.1
libreoffice-langpack-zu-4.3.7.2-2.el6_9.1
libreoffice-langpack-da-4.3.7.2-2.el6_9.1
libreoffice-langpack-ml-4.3.7.2-2.el6_9.1
libreoffice-langpack-sv-4.3.7.2-2.el6_9.1
libreoffice-langpack-af-4.3.7.2-2.el6_9.1
libreoffice-langpack-et-4.3.7.2-2.el6_9.1
libreoffice-langpack-cs-4.3.7.2-2.el6_9.1
libreoffice-langpack-dz-4.3.7.2-2.el6_9.1
libreoffice-langpack-uk-4.3.7.2-2.el6_9.1
libreoffice-langpack-sk-4.3.7.2-2.el6_9.1
libreoffice-langpack-he-4.3.7.2-2.el6_9.1
libreoffice-core-4.3.7.2-2.el6_9.1
libreoffice-langpack-ga-4.3.7.2-2.el6_9.1
libreoffice-langpack-ro-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hant-4.3.7.2-2.el6_9.1
libreoffice-langpack-xh-4.3.7.2-2.el6_9.1
libreoffice-glade-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-BR-4.3.7.2-2.el6_9.1
libreoffice-langpack-ar-4.3.7.2-2.el6_9.1
libreoffice-langpack-lt-4.3.7.2-2.el6_9.1
libreoffice-langpack-ta-4.3.7.2-2.el6_9.1
libreoffice-langpack-bn-4.3.7.2-2.el6_9.1
libreoffice-langpack-bg-4.3.7.2-2.el6_9.1
libreoffice-langpack-st-4.3.7.2-2.el6_9.1
libreoffice-langpack-ts-4.3.7.2-2.el6_9.1
libreoffice-calc-4.3.7.2-2.el6_9.1
libreoffice-langpack-hi-4.3.7.2-2.el6_9.1
libreoffice-langpack-nb-4.3.7.2-2.el6_9.1
libreoffice-langpack-gu-4.3.7.2-2.el6_9.1
libreoffice-base-4.3.7.2-2.el6_9.1
libreoffice-langpack-as-4.3.7.2-2.el6_9.1
libreoffice-sdk-4.3.7.2-2.el6_9.1
libreoffice-xsltfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-ca-4.3.7.2-2.el6_9.1
libreoffice-langpack-nso-4.3.7.2-2.el6_9.1
libreoffice-langpack-ms-4.3.7.2-2.el6_9.1
libreoffice-langpack-ja-4.3.7.2-2.el6_9.1
libreoffice-gdb-debug-support-4.3.7.2-2.el6_9.1
libreoffice-langpack-es-4.3.7.2-2.el6_9.1
libreoffice-langpack-it-4.3.7.2-2.el6_9.1
libreoffice-writer-4.3.7.2-2.el6_9.1
libreoffice-langpack-ru-4.3.7.2-2.el6_9.1
libreoffice-langpack-ss-4.3.7.2-2.el6_9.1
libreoffice-graphicfilter-4.3.7.2-2.el6_9.1

libreoffice-langpack-sl-4.3.7.2-2.el6_9.1
libreoffice-langpack-nn-4.3.7.2-2.el6_9.1

160244 - CentOS 6 CESA-2017-1109 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
CESA-2017-1109

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-April/022395.html>

CentOS 6

i686

java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

noarch

java-1.8.0-openjdk-javadoc-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.131-0.b11.el6_9

x86_64

java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

160245 - CentOS 7 CESA-2017-1108 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

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

CESA-2017-1108

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-April/022399.html>

CentOS 7

i686

java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-1.8.0.131-2.b11.el7_3

noarch

java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-zip-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-1.8.0.131-2.b11.el7_3

x86_64

java-1.8.0-openjdk-demo-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-src-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-src-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-1.8.0.131-2.b11.el7_3

163335 - Oracle Enterprise Linux ELSA-2017-1109 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
ELSA-2017-1109

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006878.html>

OEL6

x86_64

java-1.8.0-openjdk-javadoc-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9

java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

i386

java-1.8.0-openjdk-javadoc-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

163338 - Oracle Enterprise Linux ELSA-2017-1108 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
ELSA-2017-1108

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-April/006875.html>

OEL7

x86_64
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-src-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-zip-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-src-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-1.8.0.131-2.b11.el7_3

170794 - Amazon Linux AMI ALAS-2017-819 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8714

Description

The scan detected that the host is missing the following update:
ALAS-2017-819

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-819.html>

Amazon Linux AMI

x86_64

R-java-devel-3.3.3-1.51.amzn1
libRmath-devel-3.3.3-1.51.amzn1
R-core-3.3.3-1.51.amzn1
R-java-3.3.3-1.51.amzn1
R-debuginfo-3.3.3-1.51.amzn1
R-3.3.3-1.51.amzn1
R-devel-3.3.3-1.51.amzn1
libRmath-3.3.3-1.51.amzn1
R-core-devel-3.3.3-1.51.amzn1
libRmath-static-3.3.3-1.51.amzn1

i686

R-java-devel-3.3.3-1.51.amzn1
libRmath-devel-3.3.3-1.51.amzn1
R-java-3.3.3-1.51.amzn1
R-3.3.3-1.51.amzn1
R-debuginfo-3.3.3-1.51.amzn1
R-core-3.3.3-1.51.amzn1
R-devel-3.3.3-1.51.amzn1
libRmath-3.3.3-1.51.amzn1
R-core-devel-3.3.3-1.51.amzn1
libRmath-static-3.3.3-1.51.amzn1

170796 - Amazon Linux AMI ALAS-2017-817 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4000

Description

The scan detected that the host is missing the following update:
ALAS-2017-817

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-817.html>

Amazon Linux AMI
noarch
cacti-1.0.4-1.14.amzn1

170798 - Amazon Linux AMI ALAS-2017-821 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5647

Description

The scan detected that the host is missing the following update:
ALAS-2017-821

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-821.html>

Amazon Linux AMI
noarch
tomcat6-servlet-2.5-api-6.0.53-1.11.amzn1
tomcat6-javadoc-6.0.53-1.11.amzn1
tomcat6-admin-webapps-6.0.53-1.11.amzn1
tomcat6-el-2.1-api-6.0.53-1.11.amzn1
tomcat6-6.0.53-1.11.amzn1
tomcat6-webapps-6.0.53-1.11.amzn1
tomcat6-lib-6.0.53-1.11.amzn1
tomcat6-jsp-2.1-api-6.0.53-1.11.amzn1
tomcat6-docs-webapp-6.0.53-1.11.amzn1

175161 - Scientific Linux Security ERRATA Moderate: libreoffice on SL6.x i386/x86_64 (1704-17275)

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libreoffice on SL6.x i386/x86_64 (1704-17275)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=17275>

SL6
i386
libreoffice-langpack-cy-4.3.7.2-2.el6_9.1
libreoffice-langpack-fr-4.3.7.2-2.el6_9.1
libreoffice-langpack-zu-4.3.7.2-2.el6_9.1

libreoffice-langpack-ml-4.3.7.2-2.el6_9.1
libreoffice-langpack-sv-4.3.7.2-2.el6_9.1
libreoffice-langpack-af-4.3.7.2-2.el6_9.1
libreoffice-langpack-et-4.3.7.2-2.el6_9.1
libreoffice-langpack-cs-4.3.7.2-2.el6_9.1
libreoffice-langpack-dz-4.3.7.2-2.el6_9.1
libreoffice-langpack-uk-4.3.7.2-2.el6_9.1
libreoffice-langpack-sk-4.3.7.2-2.el6_9.1
libreoffice-langpack-he-4.3.7.2-2.el6_9.1
libreoffice-core-4.3.7.2-2.el6_9.1
libreoffice-langpack-ga-4.3.7.2-2.el6_9.1
libreoffice-langpack-ro-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hant-4.3.7.2-2.el6_9.1
libreoffice-langpack-xh-4.3.7.2-2.el6_9.1
libreoffice-langpack-da-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-BR-4.3.7.2-2.el6_9.1
libreoffice-langpack-lt-4.3.7.2-2.el6_9.1
libreoffice-langpack-bn-4.3.7.2-2.el6_9.1
libreoffice-langpack-bg-4.3.7.2-2.el6_9.1
libreoffice-langpack-st-4.3.7.2-2.el6_9.1
libreoffice-langpack-ts-4.3.7.2-2.el6_9.1
libreoffice-langpack-hi-4.3.7.2-2.el6_9.1
libreoffice-langpack-nb-4.3.7.2-2.el6_9.1
libreoffice-langpack-sr-4.3.7.2-2.el6_9.1
libreoffice-langpack-gu-4.3.7.2-2.el6_9.1
libreoffice-gdb-debug-support-4.3.7.2-2.el6_9.1
libreoffice-base-4.3.7.2-2.el6_9.1
libreoffice-langpack-as-4.3.7.2-2.el6_9.1
libreoffice-sdk-4.3.7.2-2.el6_9.1
libreoffice-xsltfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-ca-4.3.7.2-2.el6_9.1
libreoffice-langpack-nso-4.3.7.2-2.el6_9.1
libreoffice-langpack-ms-4.3.7.2-2.el6_9.1
libreoffice-langpack-ja-4.3.7.2-2.el6_9.1
libreoffice-4.3.7.2-2.el6_9.1
libreoffice-writer-4.3.7.2-2.el6_9.1
libreoffice-langpack-es-4.3.7.2-2.el6_9.1
libreoffice-langpack-it-4.3.7.2-2.el6_9.1
libreoffice-langpack-ru-4.3.7.2-2.el6_9.1
libreoffice-langpack-ss-4.3.7.2-2.el6_9.1
libreoffice-graphicfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-sl-4.3.7.2-2.el6_9.1
libreoffice-langpack-nn-4.3.7.2-2.el6_9.1
libreoffice-langpack-en-4.3.7.2-2.el6_9.1
libreoffice-pdfimport-4.3.7.2-2.el6_9.1
libreoffice-langpack-ve-4.3.7.2-2.el6_9.1
libreoffice-langpack-nr-4.3.7.2-2.el6_9.1
libreoffice-langpack-fi-4.3.7.2-2.el6_9.1
libreoffice-langpack-th-4.3.7.2-2.el6_9.1
libreoffice-langpack-ta-4.3.7.2-2.el6_9.1
libreoffice-impress-4.3.7.2-2.el6_9.1
libreoffice-langpack-eu-4.3.7.2-2.el6_9.1
libreoffice-langpack-ko-4.3.7.2-2.el6_9.1
libreoffice-headless-4.3.7.2-2.el6_9.1
libreoffice-langpack-ar-4.3.7.2-2.el6_9.1
libreoffice-langpack-pa-4.3.7.2-2.el6_9.1
libreoffice-wiki-publisher-4.3.7.2-2.el6_9.1
libreoffice-langpack-mai-4.3.7.2-2.el6_9.1
libreoffice-bsh-4.3.7.2-2.el6_9.1
libreoffice-debuginfo-4.3.7.2-2.el6_9.1

libreoffice-langpack-gl-4.3.7.2-2.el6_9.1
libreoffice-langpack-te-4.3.7.2-2.el6_9.1
libreoffice-langpack-nl-4.3.7.2-2.el6_9.1
libreoffice-pyuno-4.3.7.2-2.el6_9.1
libreoffice-langpack-el-4.3.7.2-2.el6_9.1
libreoffice-langpack-tn-4.3.7.2-2.el6_9.1
libreoffice-langpack-ur-4.3.7.2-2.el6_9.1
libreoffice-calc-4.3.7.2-2.el6_9.1
libreoffice-ogltrans-4.3.7.2-2.el6_9.1
libreoffice-langpack-tr-4.3.7.2-2.el6_9.1
libreoffice-emailmerge-4.3.7.2-2.el6_9.1
libreoffice-sdk-doc-4.3.7.2-2.el6_9.1
libreoffice-filters-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-PT-4.3.7.2-2.el6_9.1
libreoffice-langpack-or-4.3.7.2-2.el6_9.1
libreoffice-langpack-kn-4.3.7.2-2.el6_9.1
libreoffice-ure-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hans-4.3.7.2-2.el6_9.1
libreoffice-draw-4.3.7.2-2.el6_9.1
libreoffice-langpack-mr-4.3.7.2-2.el6_9.1
libreoffice-nlpsolver-4.3.7.2-2.el6_9.1
libreoffice-officebean-4.3.7.2-2.el6_9.1
libreoffice-langpack-pl-4.3.7.2-2.el6_9.1
libreoffice-librelogo-4.3.7.2-2.el6_9.1
libreoffice-langpack-hr-4.3.7.2-2.el6_9.1
libreoffice-rhino-4.3.7.2-2.el6_9.1
libreoffice-langpack-de-4.3.7.2-2.el6_9.1
libreoffice-glade-4.3.7.2-2.el6_9.1
libreoffice-math-4.3.7.2-2.el6_9.1
libreoffice-langpack-hu-4.3.7.2-2.el6_9.1

noarch

autocorr-pl-4.3.7.2-2.el6_9.1
autocorr-cs-4.3.7.2-2.el6_9.1
autocorr-ro-4.3.7.2-2.el6_9.1
autocorr-hr-4.3.7.2-2.el6_9.1
autocorr-tr-4.3.7.2-2.el6_9.1
autocorr-de-4.3.7.2-2.el6_9.1
autocorr-sl-4.3.7.2-2.el6_9.1
autocorr-ga-4.3.7.2-2.el6_9.1
autocorr-lb-4.3.7.2-2.el6_9.1
autocorr-vi-4.3.7.2-2.el6_9.1
autocorr-sr-4.3.7.2-2.el6_9.1
autocorr-en-4.3.7.2-2.el6_9.1
libreoffice-opensymbol-fonts-4.3.7.2-2.el6_9.1
autocorr-sv-4.3.7.2-2.el6_9.1
autocorr-da-4.3.7.2-2.el6_9.1
autocorr-lt-4.3.7.2-2.el6_9.1
autocorr-fa-4.3.7.2-2.el6_9.1
autocorr-hu-4.3.7.2-2.el6_9.1
autocorr-nl-4.3.7.2-2.el6_9.1
autocorr-ca-4.3.7.2-2.el6_9.1
autocorr-pt-4.3.7.2-2.el6_9.1
autocorr-ko-4.3.7.2-2.el6_9.1
autocorr-ru-4.3.7.2-2.el6_9.1
autocorr-is-4.3.7.2-2.el6_9.1
autocorr-ja-4.3.7.2-2.el6_9.1
autocorr-sk-4.3.7.2-2.el6_9.1
autocorr-zh-4.3.7.2-2.el6_9.1
autocorr-mn-4.3.7.2-2.el6_9.1

autocorr-it-4.3.7.2-2.el6_9.1
autocorr-es-4.3.7.2-2.el6_9.1
autocorr-af-4.3.7.2-2.el6_9.1
autocorr-fr-4.3.7.2-2.el6_9.1
autocorr-bg-4.3.7.2-2.el6_9.1
autocorr-fi-4.3.7.2-2.el6_9.1

x86_64

libreoffice-langpack-cy-4.3.7.2-2.el6_9.1
libreoffice-langpack-fr-4.3.7.2-2.el6_9.1
libreoffice-langpack-zu-4.3.7.2-2.el6_9.1
libreoffice-langpack-ml-4.3.7.2-2.el6_9.1
libreoffice-langpack-sv-4.3.7.2-2.el6_9.1
libreoffice-langpack-af-4.3.7.2-2.el6_9.1
libreoffice-langpack-et-4.3.7.2-2.el6_9.1
libreoffice-langpack-cs-4.3.7.2-2.el6_9.1
libreoffice-langpack-dz-4.3.7.2-2.el6_9.1
libreoffice-langpack-uk-4.3.7.2-2.el6_9.1
libreoffice-langpack-sk-4.3.7.2-2.el6_9.1
libreoffice-langpack-he-4.3.7.2-2.el6_9.1
libreoffice-core-4.3.7.2-2.el6_9.1
libreoffice-langpack-ga-4.3.7.2-2.el6_9.1
libreoffice-langpack-ro-4.3.7.2-2.el6_9.1
libreoffice-langpack-zh-Hant-4.3.7.2-2.el6_9.1
libreoffice-langpack-xh-4.3.7.2-2.el6_9.1
libreoffice-langpack-da-4.3.7.2-2.el6_9.1
libreoffice-langpack-pt-BR-4.3.7.2-2.el6_9.1
libreoffice-langpack-lt-4.3.7.2-2.el6_9.1
libreoffice-langpack-bn-4.3.7.2-2.el6_9.1
libreoffice-langpack-bg-4.3.7.2-2.el6_9.1
libreoffice-langpack-st-4.3.7.2-2.el6_9.1
libreoffice-langpack-ts-4.3.7.2-2.el6_9.1
libreoffice-langpack-hi-4.3.7.2-2.el6_9.1
libreoffice-langpack-nb-4.3.7.2-2.el6_9.1
libreoffice-langpack-sr-4.3.7.2-2.el6_9.1
libreoffice-langpack-gu-4.3.7.2-2.el6_9.1
libreoffice-gdb-debug-support-4.3.7.2-2.el6_9.1
libreoffice-base-4.3.7.2-2.el6_9.1
libreoffice-langpack-as-4.3.7.2-2.el6_9.1
libreoffice-sdk-4.3.7.2-2.el6_9.1
libreoffice-xsltfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-ca-4.3.7.2-2.el6_9.1
libreoffice-langpack-nso-4.3.7.2-2.el6_9.1
libreoffice-langpack-ms-4.3.7.2-2.el6_9.1
libreoffice-langpack-ja-4.3.7.2-2.el6_9.1
libreoffice-4.3.7.2-2.el6_9.1
libreoffice-writer-4.3.7.2-2.el6_9.1
libreoffice-langpack-es-4.3.7.2-2.el6_9.1
libreoffice-langpack-it-4.3.7.2-2.el6_9.1
libreoffice-langpack-ru-4.3.7.2-2.el6_9.1
libreoffice-langpack-ss-4.3.7.2-2.el6_9.1
libreoffice-graphicfilter-4.3.7.2-2.el6_9.1
libreoffice-langpack-sl-4.3.7.2-2.el6_9.1
libreoffice-langpack-nn-4.3.7.2-2.el6_9.1
libreoffice-langpack-en-4.3.7.2-2.el6_9.1

182328 - FreeBSD icu Multiple Vulnerabilities (607f8b57-7454-42c6-a88a-8706f327076d)

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

Risk Level: Medium

CVE: CVE-2017-7867, CVE-2017-7868

Description

The scan detected that the host is missing the following update:
icu -- multiple vulnerabilities (607f8b57-7454-42c6-a88a-8706f327076d)

Observation

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

<http://www.vuxml.org/freebsd/607f8b57-7454-42c6-a88a-8706f327076d.html>

Affected packages:

icu < 59.0,1
linux-c6-icu < 59.0
linux-c7-icu < 59.0

191980 - Fedora Linux 26 FEDORA-2017-35e59a5ffb Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10209, CVE-2017-5601

Description

The scan detected that the host is missing the following update:
FEDORA-2017-35e59a5ffb

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/2017/4/?count=200&page=2>

Fedora Core 26

libarchive-3.2.2-4.fc26

191986 - Fedora Linux 25 FEDORA-2017-55a8f10223 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10209, CVE-2017-5601

Description

The scan detected that the host is missing the following update:
FEDORA-2017-55a8f10223

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/2017/4/?count=200&page=1>

Fedora Core 25

191988 - Fedora Linux 25 FEDORA-2017-1aa946d52b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7867, CVE-2017-7868

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1aa946d52b

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/2017/4/?count=200&page=1>

Fedora Core 25

icu-57.1-5.fc25

191994 - Fedora Linux 25 FEDORA-2017-c0ef6054d7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7233

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c0ef6054d7

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/2017/4/?count=200&page=2>

Fedora Core 25

python-django-1.9.13-1.fc25

191997 - Fedora Linux 25 FEDORA-2017-9c6430c2e2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7186

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9c6430c2e2

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/2017/4/?count=200&page=1>

Fedora Core 25

pcre2-10.23-6.fc25

192005 - Fedora Linux 26 FEDORA-2017-f997e46fa7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7233

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f997e46fa7

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/2017/4/?count=200&page=2>

Fedora Core 26

python-django-1.10.7-1.fc26

192010 - Fedora Linux 25 FEDORA-2017-b4d4a46af6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7186

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b4d4a46af6

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/2017/4/?count=200&page=1>

Fedora Core 25

pcre-8.40-7.fc25

192011 - Fedora Linux 24 FEDORA-2017-6b639afc9c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7401

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6b639afc9c

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/2017/4/?count=200&page=1>

Fedora Core 24

collectd-5.6.2-1.fc24

192016 - Fedora Linux 26 FEDORA-2017-822d460ae2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7401

Description

The scan detected that the host is missing the following update:
FEDORA-2017-822d460ae2

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/2017/4/?count=200&page=3>

Fedora Core 26

collectd-5.7.1-3.fc26

192018 - Fedora Linux 25 FEDORA-2017-80763c8c03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7401

Description

The scan detected that the host is missing the following update:
FEDORA-2017-80763c8c03

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/2017/4/?count=200&page=1>

Fedora Core 25

collectd-5.7.1-3.fc25

192020 - Fedora Linux 26 FEDORA-2017-e4c6ab648b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7186

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e4c6ab648b

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/2017/4/?count=200&page=2>

Fedora Core 26

pcrc2-10.23-6.fc26

130743 - Debian Linux 8.0 DSA-3833-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9821, CVE-2016-9822

Description

The scan detected that the host is missing the following update:
DSA-3833-1

Observation

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

<http://www.debian.org/security/2017/dsa-3833>

Debian 8.0

all

libav-dbg_6:11.9-1~deb8u1

libavformat-dev_6:11.9-1~deb8u1

libswscale3_6:11.9-1~deb8u1

libavcodec-extra_6:11.9-1~deb8u1

libavresample-dev_6:11.9-1~deb8u1

libswscale-dev_6:11.9-1~deb8u1

libavformat56_6:11.9-1~deb8u1

libavdevice-dev_6:11.9-1~deb8u1

libav-doc_6:11.9-1~deb8u1

libavcodec-dev_6:11.9-1~deb8u1

libavcodec-extra-56_6:11.9-1~deb8u1

libavfilter-dev_6:11.9-1~deb8u1

libavcodec56_6:11.9-1~deb8u1

libavresample2_6:11.9-1~deb8u1

libavfilter5_6:11.9-1~deb8u1

libav-tools_6:11.9-1~deb8u1

libavdevice55_6:11.9-1~deb8u1

libavutil-dev_6:11.9-1~deb8u1

141547 - Red Hat Enterprise Linux RHSA-2017-1108 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
RHSA-2017-1108

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00040.html>

RHEL7D

x86_64

java-1.8.0-openjdk-src-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-src-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debuginfo-1.8.0.131-2.b11.el7_3

noarch

java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-zip-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-1.8.0.131-2.b11.el7_3

RHEL7S

noarch

java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-zip-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-1.8.0.131-2.b11.el7_3

x86_64

java-1.8.0-openjdk-src-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-src-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debug-1.8.0.131-2.b11.el7_3

java-1.8.0-openjdk-accessibility-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debuginfo-1.8.0.131-2.b11.el7_3

RHEL7WS

x86_64
java-1.8.0-openjdk-src-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-src-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debuginfo-1.8.0.131-2.b11.el7_3

noarch

java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-zip-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-1.8.0.131-2.b11.el7_3

141558 - Red Hat Enterprise Linux RHSA-2017-1109 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
RHSA-2017-1109

Observation

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

<http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00041.html>

RHEL6D

i386
java-1.8.0-openjdk-debuginfo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

noarch

java-1.8.0-openjdk-javadoc-debug-1.8.0.131-0.b11.el6_9

java-1.8.0-openjdk-javadoc-1.8.0.131-0.b11.el6_9

x86_64

java-1.8.0-openjdk-debuginfo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

RHEL6S

i386

java-1.8.0-openjdk-debuginfo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

noarch

java-1.8.0-openjdk-javadoc-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.131-0.b11.el6_9

x86_64

java-1.8.0-openjdk-debuginfo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

RHEL6WS

x86_64

java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9

i386

java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9

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

Risk Level: Medium

CVE: CVE-2017-5974, CVE-2017-5975, CVE-2017-5976, CVE-2017-5977, CVE-2017-5978, CVE-2017-5979, CVE-2017-5980, CVE-2017-5981

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1095-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002826.html>

SuSE SLED 12 SP2

x86_64

zziplib-debugsource-0.13.62-9.1

libzip-0-13-debuginfo-0.13.62-9.1

libzip-0-13-0.13.62-9.1

SuSE SLED 12 SP1

x86_64

zziplib-debugsource-0.13.62-9.1

libzip-0-13-debuginfo-0.13.62-9.1

libzip-0-13-0.13.62-9.1

145319 - SuSE SLES 11 SP4 SUSE-SU-2017:1065-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7697

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:1065-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-April/002819.html>

SuSE SLES 11 SP4

i586

libsamplerate-0.1.4-3.1

x86_64

libsamplerate-32bit-0.1.4-3.1

libsamplerate-0.1.4-3.1

175160 - Scientific Linux Security ERRATA Moderate: java-1.8.0-openjdk on SL7.x x86_64 (1704-20207)

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: java-1.8.0-openjdk on SL7.x x86_64 (1704-20207)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=20207>

SL7

x86_64

java-1.8.0-openjdk-src-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-headless-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-src-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-demo-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-accessibility-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-devel-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-debuginfo-1.8.0.131-2.b11.el7_3

noarch

java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-zip-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-debug-1.8.0.131-2.b11.el7_3
java-1.8.0-openjdk-javadoc-1.8.0.131-2.b11.el7_3

175166 - Scientific Linux Security ERRATA Moderate: java-1.8.0-openjdk on SL6.x i386/x86_64 (1704-20652)

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2017-3509, CVE-2017-3511, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: java-1.8.0-openjdk on SL6.x i386/x86_64 (1704-20652)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1704&L=scientific-linux-errata&F=&S=&P=20652>

SL6

i386

java-1.8.0-openjdk-debuginfo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9

java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.131-0.b11.el6_9

x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-headless-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.131-0.b11.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.131-0.b11.el6_9

182334 - FreeBSD libsamplerate Multiple Vulnerabilities (d44129d6-b22e-4e9c-b200-6a46e8bd3e60)

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

Risk Level: Medium

CVE: CVE-2017-7697

Description

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

libsamplerate -- multiple vulnerabilities (d44129d6-b22e-4e9c-b200-6a46e8bd3e60)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/d44129d6-b22e-4e9c-b200-6a46e8bd3e60.html>

Affected packages:

libsamplerate < 0.1.9

linux-c6-libsamplerate < 0.1.9

linux-c7-libsamplerate < 0.1.9

182337 - FreeBSD libsndfile Multiple Vulnerabilities (5a97805e-93ef-4dcb-8d5e-dbcac263bfc2)

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

Risk Level: Medium

CVE: CVE-2017-7585, CVE-2017-7586, CVE-2017-7741, CVE-2017-7742

Description

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

libsndfile -- multiple vulnerabilities (5a97805e-93ef-4dcb-8d5e-dbcac263bfc2)

Observation

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

<http://www.vuxml.org/freebsd/5a97805e-93ef-4dcb-8d5e-dbcac263bfc2.html>

Affected packages:

libsndfile < 1.0.28

linux-c6-libsndfile < 1.0.28

linux-c7-libsndfile < 1.0.28

185667 - Ubuntu Linux 17.04 USN-3268-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10028, CVE-2016-8667, CVE-2016-9602, CVE-2016-9603, CVE-2016-9908, CVE-2016-9912, CVE-2016-9914, CVE-2017-5552, CVE-2017-5578, CVE-2017-5987, CVE-2017-6505

Description

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

USN-3268-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003827.html>

Ubuntu 17.04

qemu-system_2.8+dfsg-3ubuntu2.1

qemu-system-arm_2.8+dfsg-3ubuntu2.1

qemu-system-aarch64_2.8+dfsg-3ubuntu2.1

qemu-system-x86_2.8+dfsg-3ubuntu2.1

qemu-system-sparc_2.8+dfsg-3ubuntu2.1

qemu-system-ppc_2.8+dfsg-3ubuntu2.1

qemu-system-s390x_2.8+dfsg-3ubuntu2.1

qemu-system-mips_2.8+dfsg-3ubuntu2.1

qemu-system-misc_2.8+dfsg-3ubuntu2.1

191985 - Fedora Linux 24 FEDORA-2017-9a13090378 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7207

Description

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

FEDORA-2017-9a13090378

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/2017/4/?count=200&page=3>

Fedora Core 24

192008 - Fedora Linux 25 FEDORA-2017-01925dba3c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8667, CVE-2017-5579

Description

The scan detected that the host is missing the following update:
FEDORA-2017-01925dba3c

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/2017/4/?count=200&page=3>

Fedora Core 25

qemu-2.7.1-6.fc25

192019 - Fedora Linux 26 FEDORA-2017-8150618774 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10221

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8150618774

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/2017/4/?count=200&page=2>

Fedora Core 26

mupdf-1.10a-5.fc26

88859 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-108-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7467

Description

The scan detected that the host is missing the following update:
SSA:2017-108-01

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=2017&m=slackware-security.553873>

Slackware 14.0
x86_64
minicom-2.7.1-x86_64-1

Slackware 13.37
x86_64
minicom-2.7.1-x86_64-1

Slackware 14.1
x86_64
minicom-2.7.1-x86_64-1

Slackware 13.1
x86_64
minicom-2.7.1-x86_64-1

Slackware 14.2
x86_64
minicom-2.7.1-x86_64-1

i586
minicom-2.7.1-i586-1

Slackware 13.0
x86_64
minicom-2.7.1-x86_64-1

88862 - Slackware Linux 14.1 SSA:2017-112-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2017-112-01

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=2017&m=slackware-security.320508>

Slackware 14.1
x86_64
mozilla-firefox-45.9.0esr-x86_64-1

88863 - Slackware Linux 14.2 SSA:2017-114-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2017-114-01

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=2017&m=slackware-security.356755>

Slackware 14.2
x86_64
mozilla-firefox-52.1.0esr-x86_64-1

i586
mozilla-firefox-52.1.0esr-i586-1

130745 - Debian Linux 8.0 DSA-3831-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5429, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5469

Description

The scan detected that the host is missing the following update:
DSA-3831-1

Observation

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

<http://www.debian.org/security/2017/dsa-3831>

Debian 8.0
all
firefox-esr_45.9.0esr-1~deb8u1

130747 - Debian Linux 8.0 DSA-3832-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5373, CVE-2017-5375, CVE-2017-5376, CVE-2017-5378, CVE-2017-5380, CVE-2017-5383, CVE-2017-5390, CVE-2017-5396, CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
DSA-3832-1

Observation

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

For more information see:

<http://www.debian.org/security/2017/dsa-3832>

Debian 8.0
all
icedove_1:45.8.0-3~deb8u1

182327 - FreeBSD MySQL Multiple Vulnerabilities (d9e01c35-2531-11e7-b291-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-3305, CVE-2017-3308, CVE-2017-3309, CVE-2017-3329, CVE-2017-3331, CVE-2017-3450, CVE-2017-3452, CVE-2017-3453, CVE-2017-3454, CVE-2017-3455, CVE-2017-3456, CVE-2017-3457, CVE-2017-3458, CVE-2017-3459, CVE-2017-3460, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3465, CVE-2017-3467, CVE-2017-3468, CVE-2017-3599, CVE-2017-3600

Description

The scan detected that the host is missing the following update:
MySQL -- multiple vulnerabilities (d9e01c35-2531-11e7-b291-b499baebfeaf)

Observation

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

<http://www.vuxml.org/freebsd/d9e01c35-2531-11e7-b291-b499baebfeaf.html>

Affected packages:

mariadb55-server < 5.5.55
mariadb100-server < 10.0.31
mariadb101-server < 10.1.23
mysql55-server < 5.5.55
mysql56-server < 5.6.36
mysql57-server < 5.7.18

182329 - FreeBSD codeigniter Multiple Vulnerabilities (df0144fb-295e-11e7-970f-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:
codeigniter -- multiple vulnerabilities (df0144fb-295e-11e7-970f-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/df0144fb-295e-11e7-970f-002590263bf5.html>

Affected packages:

codeigniter < 3.1.4

182331 - FreeBSD weechat Multiple Vulnerabilities (81433129-2916-11e7-ad3e-00e04c1ea73d)

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

Risk Level: Low

CVE: CVE-2017-8073

Description

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

weechat -- multiple vulnerabilities (81433129-2916-11e7-ad3e-00e04c1ea73d)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/81433129-2916-11e7-ad3e-00e04c1ea73d.html>

Affected packages:

weechat < 1.7.1

182332 - FreeBSD chromium Multiple Vulnerabilities (95a74a48-2691-11e7-9e2d-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Description

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

chromium -- multiple vulnerabilities (95a74a48-2691-11e7-9e2d-e8e0b747a45a)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/95a74a48-2691-11e7-9e2d-e8e0b747a45a.html>

Affected packages:

chromium < 58.0.3029.81

chromium-pulse < 58.0.3029.81

182333 - FreeBSD graphite2 Out-of-bounds Write With Malicious Font (cf133acc-82e7-4755-a66a-5ddf90dacbe6)

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

Risk Level: Low

CVE: CVE-2017-5436

Description

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

graphite2 -- out-of-bounds write with malicious font (cf133acc-82e7-4755-a66a-5ddf90dacbe6)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/cf133acc-82e7-4755-a66a-5ddf90dacbe6.html>

Affected packages:
graphite2 < 1.3.9_1
linux-c7-graphite2 < 1.3.10

182338 - FreeBSD mozilla Multiple Vulnerabilities (5e0a038a-ca30-416d-a2f5-38cbf5e7df33)

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

Risk Level: Low

CVE: CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5450, CVE-2017-5451, CVE-2017-5452, CVE-2017-5453, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5458, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5463, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5468, CVE-2017-5469

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (5e0a038a-ca30-416d-a2f5-38cbf5e7df33)

Observation

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

<http://www.vuxml.org/freebsd/5e0a038a-ca30-416d-a2f5-38cbf5e7df33.html>

Affected packages:
firefox < 53.0_2,1
seamonkey < 2.50
linux-seamonkey < 2.50
46.0,1 <= firefox-esr < 52.1.0_2,1
firefox-esr < 45.9.0,1
46.0,2 <= linux-firefox < 52.1.0,2
linux-firefox < 45.9.0,2
46.0 <= libxul < 52.1.0
libxul < 45.9.0
46.0 <= thunderbird < 52.1.0
46.0 <= linux-thunderbird < 52.1.0
thunderbird < 45.9.0
linux-thunderbird < 45.9.0

182339 - FreeBSD NSS Multiple Vulnerabilities (4cb165f0-6e48-423e-8147-92255d35c0f7)

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

Risk Level: Low

CVE: CVE-2017-5461, CVE-2017-5462

Description

The scan detected that the host is missing the following update:
NSS -- multiple vulnerabilities (4cb165f0-6e48-423e-8147-92255d35c0f7)

Observation

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

<http://www.vuxml.org/freebsd/4cb165f0-6e48-423e-8147-92255d35c0f7.html>

Affected packages:

3.30 <= nss < 3.30.1
3.30 <= linux-f10-nss < 3.30.1
3.30 <= linux-c6-nss < 3.30.1
3.30 <= linux-c7-nss < 3.30.1
3.29 <= nss < 3.29.5
3.29 <= linux-f10-nss < 3.29.5
3.29 <= linux-c6-nss < 3.29.5
3.29 <= linux-c7-nss < 3.29.5
3.22 <= nss < 3.28.4
3.22 <= linux-f10-nss < 3.28.4
3.22 <= linux-c6-nss < 3.28.4
3.22 <= linux-c7-nss < 3.28.4
nss < 3.21.4
linux-f10-nss < 3.21.4
linux-c6-nss < 3.21.4
linux-c7-nss < 3.21.4

182340 - FreeBSD cURL TLS Session Resumption Client Cert Bypass (again) (3e2e9b44-25ce-11e7-a175-939b30e0836d)

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

Risk Level: Low

CVE: CVE-2017-7468

Description

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

cURL -- TLS session resumption client cert bypass (again) (3e2e9b44-25ce-11e7-a175-939b30e0836d)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/3e2e9b44-25ce-11e7-a175-939b30e0836d.html>

Affected packages:

7.52.0 <= curl < 7.54.0

185668 - Ubuntu Linux 17.04 USN-3262-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7468

Description

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

USN-3262-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003817.html>

Ubuntu 17.04

libcurl3_7.52.1-4ubuntu1.1

libcurl3-nss_7.52.1-4ubuntu1.1
curl_7.52.1-4ubuntu1.1
libcurl3-gnutls_7.52.1-4ubuntu1.1

185671 - Ubuntu Linux 14.04, 16.04, 16.10, 17.04 USN-3260-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5453, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5458, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5468, CVE-2017-5469

Description

The scan detected that the host is missing the following update:
USN-3260-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003820.html>

Ubuntu 16.04

firefox_53.0+build6-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_53.0+build6-0ubuntu0.14.04.1

Ubuntu 16.10

firefox_53.0+build6-0ubuntu0.16.10.1

Ubuntu 17.04

firefox_53.0+build6-0ubuntu0.17.04.1

185672 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10, 17.04 USN-3259-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
USN-3259-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003818.html>

Ubuntu 12.04

bind9_9.8.1.dfsg.P1-4ubuntu0.22

Ubuntu 16.04

bind9_9.10.3.dfsg.P4-8ubuntu1.6

Ubuntu 14.04

bind9_9.9.5.dfsg-3ubuntu0.14

Ubuntu 16.10

bind9_9.10.3.dfsg.P4-10.1ubuntu1.6

Ubuntu 17.04

bind9_9.10.3.dfsg.P4-10.1ubuntu5

185676 - Ubuntu Linux 17.04 USN-3267-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
USN-3267-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-April/003828.html>

Ubuntu 17.04

samba_4.5.8+dfsg-0ubuntu0.17.04.1

191975 - Fedora Linux 25 FEDORA-2017-06f4b88ceb 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-2017-06f4b88ceb

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/2017/4/?count=200&page=2>

Fedora Core 25

php-onelogin-php-saml-2.10.5-1.fc25

191976 - Fedora Linux 24 FEDORA-2017-db6864b797 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-2017-db6864b797

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/2017/4/?count=200&page=2>

Fedora Core 24

jenkins-xstream-1.4.7-11.jenkins1.fc24

191978 - Fedora Linux 25 FEDORA-2017-2a90185a04 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-2017-2a90185a04

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/2017/4/?count=200&page=2>

Fedora Core 25

php-pear-CAS-1.3.5-1.fc25

191979 - Fedora Linux 26 FEDORA-2017-8e4c14eeec 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-2017-8e4c14eeec

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/2017/4/?count=200&page=3>

Fedora Core 26

php-onelogin-php-saml-2.10.5-1.fc26

191981 - Fedora Linux 25 FEDORA-2017-a902f8db61 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-2017-a902f8db61

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/2017/4/?count=200&page=2>

Fedora Core 25

jenkins-xstream-1.4.7-11.jenkins1.fc25

191982 - Fedora Linux 26 FEDORA-2017-8d74747fc4 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-2017-8d74747fc4

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/2017/4/?count=200&page=3>

Fedora Core 26

xstream-1.4.9-5.fc26

191987 - Fedora Linux 25 FEDORA-2017-44e494db1e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
FEDORA-2017-44e494db1e

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/2017/4/?count=200&page=3>

Fedora Core 25

bind99-9.9.9-4.P8.fc25

191989 - Fedora Linux 25 FEDORA-2017-ee4b0f53cb Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ee4b0f53cb

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/2017/4/?count=200&page=3>

Fedora Core 25

bind-9.10.4-4.P8.fc25

191990 - Fedora Linux 24 FEDORA-2017-9042085060 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-2017-9042085060

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/2017/4/?count=200&page=1>

Fedora Core 24

nss-softokn-3.29.5-1.0.fc24

191992 - Fedora Linux 26 FEDORA-2017-f9f909a7b7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f9f909a7b7

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/2017/4/?count=200&page=2>

Fedora Core 26

bind-9.11.0-7.P5.fc26

191993 - Fedora Linux 26 FEDORA-2017-30e042c42a 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-2017-30e042c42a

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/2017/4/?count=200&page=1>

Fedora Core 26

mingw-gnutls-3.5.11-1.fc26

191995 - Fedora Linux 24 FEDORA-2017-87e23bcc34 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-2017-87e23bcc34

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/2017/4/?count=200&page=1>

Fedora Core 24

firefox-53.0-2.fc24

191996 - Fedora Linux 24 FEDORA-2017-68cdc567e9 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-2017-68cdc567e9

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/2017/4/?count=200&page=2>

Fedora Core 24

php-onelogin-php-saml-2.10.5-1.fc24

191998 - Fedora Linux 25 FEDORA-2017-25358a23ad 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-2017-25358a23ad

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/2017/4/?count=200&page=1>

Fedora Core 25

java-1.8.0-openjdk-1.8.0.131-1.b12.fc25

191999 - Fedora Linux 26 FEDORA-2017-4b71343fb8 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-2017-4b71343fb8

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/2017/4/?count=200&page=3>

Fedora Core 26

jenkins-xstream-1.4.7-11.jenkins1.fc26

192001 - Fedora Linux 26 FEDORA-2017-a354efc764 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a354efc764

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/2017/4/?count=200&page=2>

Fedora Core 26

bind99-9.9.9-5.P8.fc26

192003 - Fedora Linux 24 FEDORA-2017-5764721de5 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-2017-5764721de5

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/2017/4/?count=200&page=2>

Fedora Core 24

xstream-1.4.9-5.fc24

192004 - Fedora Linux 25 FEDORA-2017-3f40aa3d64 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9587, CVE-2017-7466

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3f40aa3d64

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/2017/4/?count=200&page=1>

Fedora Core 25

ansible-2.3.0.0-3.fc25

192007 - Fedora Linux 25 FEDORA-2017-31c64a0bbf 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-2017-31c64a0bbf

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/2017/4/?count=200&page=1>

Fedora Core 25

firefox-53.0-2.fc25

192009 - Fedora Linux 26 FEDORA-2017-2f3096ba16 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-2017-2f3096ba16

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/2017/4/?count=200&page=2>

Fedora Core 26

php-pear-CAS-1.3.5-1.fc26

192012 - Fedora Linux 24 FEDORA-2017-0a876b0ba5 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0a876b0ba5

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/2017/4/?count=200&page=2>

Fedora Core 24

bind-9.10.4-3.P8.fc24

192015 - Fedora Linux 24 FEDORA-2017-d9d620366e 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-2017-d9d620366e

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/2017/4/?count=200&page=2>

Fedora Core 24

php-pear-CAS-1.3.5-1.fc24

192017 - Fedora Linux 25 FEDORA-2017-b83c0eeab0 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-2017-b83c0eeab0

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/2017/4/?count=200&page=2>

Fedora Core 25

xstream-1.4.9-5.fc25

88861 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-112-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7418

Description

The scan detected that the host is missing the following update:
SSA:2017-112-03

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.545090>

Slackware 14.0

x86_64

proftpd-1.3.5e-x86_64-1

Slackware 13.37

x86_64

proftpd-1.3.5e-x86_64-1

Slackware 14.1

x86_64

proftpd-1.3.5e-x86_64-1

Slackware 13.1

x86_64

proftpd-1.3.5e-x86_64-1

Slackware 14.2

x86_64

proftpd-1.3.5e-x86_64-1

i586

proftpd-1.3.5e-i586-1

Slackware 13.0

x86_64

proftpd-1.3.5e-x86_64-1

192006 - Fedora Linux 25 FEDORA-2017-c6f424c3ff Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7418

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c6f424c3ff

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/2017/4/?count=200&page=3>

Fedora Core 25

proftpd-1.3.5e-1.fc25

170793 - Amazon Linux AMI ALAS-2017-818 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6188

Description

The scan detected that the host is missing the following update:
ALAS-2017-818

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-818.html>

Amazon Linux AMI

noarch

munin-async-2.0.30-5.38.amzn1

munin-cgi-2.0.30-5.38.amzn1

munin-java-plugins-2.0.30-5.38.amzn1

munin-2.0.30-5.38.amzn1

munin-node-2.0.30-5.38.amzn1

munin-ruby-plugins-2.0.30-5.38.amzn1

munin-netip-plugins-2.0.30-5.38.amzn1

munin-common-2.0.30-5.38.amzn1

munin-nginx-2.0.30-5.38.amzn1

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.

32911 - Oracle Solaris 147993-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-4528, CVE-2011-1091, CVE-2011-2943, CVE-2011-3184, CVE-2011-3185, CVE-2011-4601, CVE-2011-4602, CVE-2011-4603, CVE-2011-4922, CVE-2011-4939, CVE-2012-1178, CVE-2012-2214, CVE-2012-2318, CVE-2012-3374, CVE-2012-6152, CVE-2013-0271, CVE-2013-0272, CVE-2013-0273, CVE-2013-0274, CVE-2013-6477, CVE-2013-6478, CVE-2013-6479, CVE-2013-6481, CVE-2013-6482, CVE-2013-6483, CVE-2013-6484, CVE-2013-6485, CVE-2013-6486, CVE-2013-6487, CVE-2013-6489, CVE-2013-6490, CVE-2014-0020

[Update Details](#)

CVE is updated

32914 - Oracle Solaris 147992-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-4528, CVE-2011-1091, CVE-2011-2943, CVE-2011-3184, CVE-2011-3185, CVE-2011-4601, CVE-2011-4602, CVE-2011-4603, CVE-2011-4922, CVE-2011-4939, CVE-2012-1178, CVE-2012-2214, CVE-2012-2318, CVE-2012-3374, CVE-2012-6152, CVE-2013-0271, CVE-2013-0272, CVE-2013-0273, CVE-2013-0274, CVE-2013-6477, CVE-2013-6478, CVE-2013-6479, CVE-2013-6481, CVE-2013-6482, CVE-2013-6483, CVE-2013-6484, CVE-2013-6485, CVE-2013-6486, CVE-2013-6487, CVE-2013-6489, CVE-2013-6490, CVE-2014-0020

[Update Details](#)

CVE is updated

182067 - FreeBSD BIND,Knot,NSD,PowerDNS Denial Over Service Via Oversized Zone Transfers (7d08e608-5e95-11e6-b334-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-6170, CVE-2016-6171, CVE-2016-6172, CVE-2016-6173

[Update Details](#)

FASLScript is updated

32831 - Oracle Solaris 145334-37 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2616

[Update Details](#)

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

32839 - Oracle Solaris 145333-37 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2616

[Update Details](#)

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

32897 - Oracle Solaris 145342-06 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

32898 - Oracle Solaris 145341-06 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33082 - Oracle Solaris 145645-07 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33083 - Oracle Solaris 145644-07 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

21704 - Double Pulsar Backdoor SMB Detection

Category: Windows Host Assessment -> No Credentials Required

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript 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 2017 McAfee, Inc.

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