2018-JAN-25
FSL version 7.5.997

MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

146262 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0173-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16844

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0173-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003618.html

SuSE SLES 12 SP2
x86_64
procmail-debugsource-3.22-269.3.5
procmail-debuginfo-3.22-269.3.5
procmail-3.22-269.3.5

SuSE SLED 12 SP3
x86_64
procmail-debugsource-3.22-269.3.5
procmail-debuginfo-3.22-269.3.5
procmail-3.22-269.3.5

SuSE SLED 12 SP2
x86_64
procmail-debugsource-3.22-269.3.5
procmail-debuginfo-3.22-269.3.5
procmail-3.22-269.3.5

SuSE SLES 12 SP3
x86_64
procmail-debugsource-3.22-269.3.5
procmail-debuginfo-3.22-269.3.5
procmail-3.22-269.3.5

139089 - Oracle Solaris 11.3.28.4.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2015-3193, CVE-2015-8213, CVE-2016-0701, CVE-2016-10207, CVE-2017-13721, CVE-2017-13723, CVE-2017-

14867, CVE-2017-15298, CVE-2017-17083, CVE-2017-17084, CVE-2017-17085, CVE-2017-3732, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2017-7843, CVE-2017-9798

Description

The scan detected that the host is missing the following update:
SRU 11.3.28.4.0

Observation

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

https://support.oracle.com/rs?type=doc&id=2347232.1
https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=507462766511768&id=1448883.1&_afrWindowMode=0&_adf.ctrl-state=98kg3qcn0_33#aref_section26

139090 - Oracle Solaris 11.3.27.4.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2014-8127, CVE-2014-8128, CVE-2014-8129, CVE-2014-8130, CVE-2015-8870, CVE-2016-10092, CVE-2016-10093, CVE-2016-10094, CVE-2016-10095, CVE-2016-3186, CVE-2016-3619, CVE-2016-3620, CVE-2016-3621, CVE-2016-3622, CVE-2016-3623, CVE-2016-3624, CVE-2016-3625, CVE-2016-3631, CVE-2016-3632, CVE-2016-3633, CVE-2016-3634, CVE-2016-3658, CVE-2016-3945, CVE-2016-3990, CVE-2016-3991, CVE-2016-5102, CVE-2016-5314, CVE-2016-5315, CVE-2016-5316, CVE-2016-5317, CVE-2016-5318, CVE-2016-5319, CVE-2016-5320, CVE-2016-5321, CVE-2016-5322, CVE-2016-5323, CVE-2016-5875, CVE-2016-6223, CVE-2016-9273, CVE-2016-9297, CVE-2016-9318, CVE-2016-9532, CVE-2016-9533, CVE-2016-9534, CVE-2016-9535, CVE-2016-9536, CVE-2016-9537, CVE-2016-9538, CVE-2016-9539, CVE-2016-9540, CVE-2017-0379, CVE-2017-10155, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10279, CVE-2017-10283, CVE-2017-10286, CVE-2017-10294, CVE-2017-10314, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384, CVE-2017-10989, CVE-2017-13089, CVE-2017-13090, CVE-2017-13704, CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496, CVE-2017-16548, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653, CVE-2017-3731, CVE-2017-5225, CVE-2017-5563, CVE-2017-5969, CVE-2017-6508, 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, CVE-2017-7826, CVE-2017-7828, CVE-2017-7830, CVE-2017-9117, CVE-2017-9526, CVE-2018-2560, CVE-2018-2577, CVE-2018-2578

Description

The scan detected that the host is missing the following update:
SRU 11.3.27.4.0

Observation

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

https://support.oracle.com/rs?type=doc&id=2338177.1
https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=507462766511768&id=1448883.1&_afrWindowMode=0&_adf.ctrl-state=98kg3qcn0_33#aref_section26

141839 - Red Hat Enterprise Linux RHSA-2018-0099 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2581, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2627, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2638, CVE-2018-2639, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

The scan detected that the host is missing the following update:
RHSA-2018-0099

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00062.html

RHEL7D
x86_64
java-1.8.0-oracle-devel-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-src-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-javafx-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-jdbc-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-plugin-1.8.0.161-1jpp.2.el7

RHEL7S
x86_64
java-1.8.0-oracle-devel-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-src-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-javafx-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-jdbc-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-plugin-1.8.0.161-1jpp.2.el7

RHEL7WS
x86_64
java-1.8.0-oracle-devel-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-src-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-javafx-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-jdbc-1.8.0.161-1jpp.2.el7
java-1.8.0-oracle-plugin-1.8.0.161-1jpp.2.el7

146259 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0166-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12904

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0166-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00069.html

SuSE Linux 42.2
x86_64
newsbeuter-debugsource-2.9-2.3.1
newsbeuter-2.9-2.3.1
newsbeuter-debuginfo-2.9-2.3.1

noarch
newsbeuter-lang-2.9-2.3.1

SuSE Linux 42.3
x86_64
newsbeuter-debugsource-2.9-5.1
newsbeuter-2.9-5.1
newsbeuter-debuginfo-2.9-5.1

noarch
newsbeuter-lang-2.9-5.1

186059 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3534-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000408, CVE-2017-1000409, CVE-2017-15670, CVE-2017-15804, CVE-2017-16997, CVE-2017-17426, CVE-2018-1000001

Description

The scan detected that the host is missing the following update:
USN-3534-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004229.html

Ubuntu 16.04

libc6_2.23-0ubuntu10

Ubuntu 14.04

libc6_2.19-0ubuntu6.14

Ubuntu 17.10

libc6_2.26-0ubuntu2.1

193193 - Fedora Linux 27 FEDORA-2018-7714b514e2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16997, CVE-2018-1000001

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7714b514e2

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/2018/1/?count=200&page=1

Fedora Core 27

glibc-2.26-24.fc27

193198 - Fedora Linux 26 FEDORA-2018-8e27ad96ed Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15670, CVE-2017-15671, CVE-2017-15804, CVE-2017-16997, CVE-2018-1000001

Description

The scan detected that the host is missing the following update:
FEDORA-2018-8e27ad96ed

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/2018/1/?count=200&page=2

Fedora Core 26

glibc-2.25-13.fc26

23013 - Oracle WebCenter Content Critical Patch Update January 2018

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

Risk Level: High

CVE: CVE-2018-2564, CVE-2018-2596

Description

A vulnerability is present in Oracle WebCenter Content.

Observation

Oracle WebCenter Content is a complete Enterprise Content Management Software that provides a unified repository to the content.

A vulnerability is present in Oracle WebCenter Content. The flaw lies in the Content Server sub component. Successful exploitation could allow an attacker to gain unauthorized access to critical data.

22994 - IBM WebSphere Application Server Liberty Apache Commons Vulnerability (swg22011428)

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

Risk Level: High

CVE: CVE-2016-1000031

Description

A vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile.

Observation

IBM WebSphere Application Server Liberty Profile is a server engine for Java EE Web applications.

A vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile. The flaw lies in the Apache Commons FileUpload component. Successful exploitation could allow an attacker to execute remote arbitrary code.

22995 - Wireshark Multiple Vulnerabilities Prior To 2.4.4

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

Risk Level: High

CVE: CVE-2018-5334, CVE-2018-5335, CVE-2018-5336

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

22998 - (VMSA-2018-0005) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4949, CVE-2017-4950

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in NAT service. Successful exploitation could allow an attacker to execute code in the targeted system.

23000 - (MSPT-Jan2018) Microsoft Office Email Parsing Remote Code Execution (CVE-2018-0793)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-0793

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw lies in the Email Parsing component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

23001 - (MSPT-Jan2018) Microsoft Office RTF Handling Remote Code Execution (CVE-2018-0797)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-0797

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw lies in the RTF Handling component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

23003 - (VMSA-2018-0005) VMware Fusion Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4949, CVE-2017-4950

Description

Multiple vulnerabilities are present in some versions of VMware Fusion.

Observation

VMware Fusion is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware Fusion. The flaws are related with memory issues. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

23015 - (SB10221) McAfee SIEM Buffer Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4429

Description

A vulnerability is present in some versions of McAfee Security Information and Event Management.

Observation

McAfee Security Information and Event Management brings event, threat, and risk data together to provide strong security intelligence.

A vulnerability is present in some versions of McAfee Security Information and Event Management. The flaw lies in the GNU C Library. Successful exploitation could allow an attacker to cause a denial of service or possibly unspecified other impact.

130999 - Debian Linux 8.0, 9.0 DSA-4090-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16510, CVE-2017-17091, CVE-2017-17092, CVE-2017-17093, CVE-2017-17094, CVE-2017-9066

Description

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

DSA-4090-1

Observation

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

http://www.debian.org/security/2018/dsa-4090

Debian 8.0
all
wordpress_4.1+dfsg-1+deb8u16

Debian 9.0
all
wordpress_4.7.5+dfsg-2+deb9u2

131000 - Debian Linux 8.0, 9.0 DSA-4094-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000480

Description

The scan detected that the host is missing the following update:
DSA-4094-1

Observation

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

http://www.debian.org/security/2018/dsa-4094

Debian 8.0
all
smarty3_3.1.21-1+deb8u1

Debian 9.0
all
smarty3_3.1.31+20161214.1.c7d42e4+selfpack1-2+deb9u1

131001 - Debian Linux 8.0 DSA-4091-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2562, CVE-2018-2622, CVE-2018-2640, CVE-2018-2665, CVE-2018-2668

Description

The scan detected that the host is missing the following update:
DSA-4091-1

Observation

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

http://www.debian.org/security/2018/dsa-4091

Debian 8.0
all
libmysqld-pic_5.5.59-0+deb8u1
mysql-server-core-5.5_5.5.59-0+deb8u1
mysql-client-5.5_5.5.59-0+deb8u1
libmysqlclient18_5.5.59-0+deb8u1
mysql-testsuite_5.5.59-0+deb8u1
mysql-testsuite-5.5_5.5.59-0+deb8u1
mysql-source-5.5_5.5.59-0+deb8u1
libmysqlclient-dev_5.5.59-0+deb8u1
mysql-common_5.5.59-0+deb8u1
mysql-server-5.5_5.5.59-0+deb8u1
libmysqld-dev_5.5.59-0+deb8u1
mysql-client_5.5.59-0+deb8u1
mysql-server_5.5.59-0+deb8u1

131002 - Debian Linux 8.0, 9.0 DSA-4092-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000501

Description

The scan detected that the host is missing the following update:
DSA-4092-1

Observation

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

http://www.debian.org/security/2018/dsa-4092

Debian 8.0
all
awstats_7.2+dfsg-1+deb8u1

Debian 9.0
all
awstats_7.6+dfsg-1+deb9u1

132430 - Oracle VM OVMSA-2018-0014 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0014

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000825.html

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000824.html

OVM3.3
x86_64
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5

OVM3.4
x86_64
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5

141840 - Red Hat Enterprise Linux RHSA-2018-0101 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
RHSA-2018-0101

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00064.html

RHEL6D
x86_64
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-debuginfo-9.8.2-0.62.rc1.el6_9.5

i386
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-debuginfo-9.8.2-0.62.rc1.el6_9.5

RHEL6S
i386
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-debuginfo-9.8.2-0.62.rc1.el6_9.5

x86_64

bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-debuginfo-9.8.2-0.62.rc1.el6_9.5

RHEL6WS
x86_64
bind-debuginfo-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5

i386
bind-debuginfo-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5

141842 - Red Hat Enterprise Linux RHSA-2018-0102 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
RHSA-2018-0102

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00065.html

RHEL7D
x86_64
bind-9.9.4-51.el7_4.2
bind-utils-9.9.4-51.el7_4.2
bind-sdb-9.9.4-51.el7_4.2
bind-sdb-chroot-9.9.4-51.el7_4.2
bind-libs-lite-9.9.4-51.el7_4.2
bind-libs-9.9.4-51.el7_4.2
bind-devel-9.9.4-51.el7_4.2
bind-debuginfo-9.9.4-51.el7_4.2
bind-pkcs11-devel-9.9.4-51.el7_4.2
bind-chroot-9.9.4-51.el7_4.2
bind-pkcs11-9.9.4-51.el7_4.2
bind-pkcs11-libs-9.9.4-51.el7_4.2
bind-lite-devel-9.9.4-51.el7_4.2
bind-pkcs11-utils-9.9.4-51.el7_4.2

noarch
bind-license-9.9.4-51.el7_4.2

RHEL7S
noarch
bind-license-9.9.4-51.el7_4.2

x86_64
bind-9.9.4-51.el7_4.2
bind-utils-9.9.4-51.el7_4.2
bind-sdb-9.9.4-51.el7_4.2
bind-sdb-chroot-9.9.4-51.el7_4.2
bind-libs-lite-9.9.4-51.el7_4.2
bind-libs-9.9.4-51.el7_4.2
bind-devel-9.9.4-51.el7_4.2
bind-debuginfo-9.9.4-51.el7_4.2
bind-pkcs11-devel-9.9.4-51.el7_4.2
bind-chroot-9.9.4-51.el7_4.2
bind-pkcs11-9.9.4-51.el7_4.2
bind-pkcs11-libs-9.9.4-51.el7_4.2
bind-lite-devel-9.9.4-51.el7_4.2
bind-pkcs11-utils-9.9.4-51.el7_4.2

RHEL7WS
x86_64
bind-9.9.4-51.el7_4.2
bind-utils-9.9.4-51.el7_4.2
bind-sdb-9.9.4-51.el7_4.2
bind-sdb-chroot-9.9.4-51.el7_4.2
bind-libs-lite-9.9.4-51.el7_4.2
bind-libs-9.9.4-51.el7_4.2
bind-devel-9.9.4-51.el7_4.2
bind-debuginfo-9.9.4-51.el7_4.2
bind-pkcs11-devel-9.9.4-51.el7_4.2
bind-chroot-9.9.4-51.el7_4.2
bind-pkcs11-9.9.4-51.el7_4.2
bind-pkcs11-libs-9.9.4-51.el7_4.2
bind-lite-devel-9.9.4-51.el7_4.2
bind-pkcs11-utils-9.9.4-51.el7_4.2

noarch
bind-license-9.9.4-51.el7_4.2

141846 - Red Hat Enterprise Linux RHSA-2018-0115 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2637, CVE-2018-2641, CVE-2018-2657, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

The scan detected that the host is missing the following update:
RHSA-2018-0115

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00076.html

RHEL7D
x86_64
java-1.6.0-sun-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-src-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-plugin-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-jdbc-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-demo-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-devel-1.6.0.181-1jpp.2.el7

RHEL7S
x86_64
java-1.6.0-sun-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-src-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-plugin-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-jdbc-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-demo-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-devel-1.6.0.181-1jpp.2.el7

RHEL7WS
x86_64
java-1.6.0-sun-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-src-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-plugin-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-jdbc-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-demo-1.6.0.181-1jpp.2.el7
java-1.6.0-sun-devel-1.6.0.181-1jpp.2.el7

141848 - Red Hat Enterprise Linux RHSA-2018-0116 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15095, CVE-2017-17485, CVE-2017-7525

Description

The scan detected that the host is missing the following update:
RHSA-2018-0116

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00077.html

RHEL7S
noarch
rh-eclipse46-jackson-databind-javadoc-2.6.3-2.6.el7
rh-eclipse46-jackson-databind-2.6.3-2.6.el7

RHEL7WS
noarch
rh-eclipse46-jackson-databind-javadoc-2.6.3-2.6.el7
rh-eclipse46-jackson-databind-2.6.3-2.6.el7

RHEL7_3S
noarch
rh-eclipse46-jackson-databind-javadoc-2.6.3-2.6.el7
rh-eclipse46-jackson-databind-2.6.3-2.6.el7

141850 - Red Hat Enterprise Linux RHSA-2018-0100 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2581, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2657, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

The scan detected that the host is missing the following update:
RHSA-2018-0100

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00063.html

RHEL7D
x86_64
java-1.7.0-oracle-jdbc-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-src-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-javafx-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-plugin-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-devel-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-1.7.0.171-1jpp.1.el7

RHEL7S
x86_64
java-1.7.0-oracle-jdbc-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-src-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-javafx-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-plugin-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-devel-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-1.7.0.171-1jpp.1.el7

RHEL7WS
x86_64
java-1.7.0-oracle-jdbc-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-src-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-javafx-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-plugin-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-devel-1.7.0.171-1jpp.1.el7
java-1.7.0-oracle-1.7.0.171-1jpp.1.el7

141854 - Red Hat Enterprise Linux RHSA-2018-0095 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

The scan detected that the host is missing the following update:
RHSA-2018-0095

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00061.html

RHEL7S
noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.161-0.b14.el7_4

x86_64
java-1.8.0-openjdk-accessibility-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debuginfo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.161-0.b14.el7_4

RHEL6S
i386
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.161-3.b14.el6_9

x86_64
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9

RHEL6WS

x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9

i386
java-1.8.0-openjdk-debuginfo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9

RHEL7D
x86_64
java-1.8.0-openjdk-accessibility-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debuginfo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.161-0.b14.el7_4

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.161-0.b14.el7_4

RHEL6D
i386
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.161-3.b14.el6_9

x86_64
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9

java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9

RHEL7WS
x86_64
java-1.8.0-openjdk-accessibility-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debuginfo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.161-0.b14.el7_4

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.161-0.b14.el7_4

146254 - SuSE SLES 11 SP4 SUSE-SU-2018:0132-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000445, CVE-2017-1000476, CVE-2017-10800, CVE-2017-11141, CVE-2017-11449, CVE-2017-11529, CVE-2017-11644, CVE-2017-11724, CVE-2017-11751, CVE-2017-12430, CVE-2017-12434, CVE-2017-12564, CVE-2017-12642, CVE-2017-12667, CVE-2017-12670, CVE-2017-12672, CVE-2017-12675, CVE-2017-13060, CVE-2017-13146, CVE-2017-13648, CVE-2017-13658, CVE-2017-14249, CVE-2017-14326, CVE-2017-14533, CVE-2017-17680, CVE-2017-17881, CVE-2017-17882, CVE-2017-18022, CVE-2017-9409, CVE-2018-5246, CVE-2018-5247

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0132-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003612.html

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.78.22.1

x86_64
libMagickCore1-32bit-6.4.3.6-7.78.22.1
libMagickCore1-6.4.3.6-7.78.22.1

146255 - SuSE SLES 11 SP4 SUSE-SU-2018:0170-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10672

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0170-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003615.html

SuSE SLES 11 SP4
i586
perl-XML-LibXML-1.66-3.3.1

x86_64
perl-XML-LibXML-1.66-3.3.1

146256 - SuSE Linux 42.2 openSUSE-SU-2018:0190-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0190-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00077.html

SuSE Linux 42.2
noarch
clamav-database-201801220009-54.133.1

146257 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0123-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10672

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0123-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003608.html

SuSE SLES 12 SP2
x86_64
perl-XML-LibXML-2.0019-6.3.5
perl-XML-LibXML-debugsource-2.0019-6.3.5
perl-XML-LibXML-debuginfo-2.0019-6.3.5

SuSE SLED 12 SP3
x86_64
perl-XML-LibXML-2.0019-6.3.5
perl-XML-LibXML-debugsource-2.0019-6.3.5
perl-XML-LibXML-debuginfo-2.0019-6.3.5

SuSE SLED 12 SP2
x86_64
perl-XML-LibXML-2.0019-6.3.5
perl-XML-LibXML-debugsource-2.0019-6.3.5
perl-XML-LibXML-debuginfo-2.0019-6.3.5

SuSE SLES 12 SP3
x86_64
perl-XML-LibXML-2.0019-6.3.5
perl-XML-LibXML-debugsource-2.0019-6.3.5
perl-XML-LibXML-debuginfo-2.0019-6.3.5

146258 - SuSE SLES 11 SP4 SUSE-SU-2018:0180-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11600, CVE-2017-13167, CVE-2017-14106, CVE-2017-15102, CVE-2017-15115, CVE-2017-15868, CVE-2017-16525, CVE-2017-16527, CVE-2017-16529, CVE-2017-16531, CVE-2017-16534, CVE-2017-16535, CVE-2017-16536, CVE-2017-16537, CVE-2017-16538, CVE-2017-16649, CVE-2017-16939, CVE-2017-17450, CVE-2017-17558, CVE-2017-17805, CVE-2017-17806, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7472, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0180-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003622.html

SuSE SLES 11 SP4
x86_64
kernel-rt_trace-devel-3.0.101.rt130-69.14.1
kernel-rt_trace-3.0.101.rt130-69.14.1
kernel-rt-base-3.0.101.rt130-69.14.1
kernel-rt-3.0.101.rt130-69.14.1
kernel-source-rt-3.0.101.rt130-69.14.1
kernel-syms-rt-3.0.101.rt130-69.14.1
kernel-rt-devel-3.0.101.rt130-69.14.1
kernel-rt_trace-base-3.0.101.rt130-69.14.1

146263 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0118-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16548, CVE-2017-17433, CVE-2017-17434

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0118-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003604.html

SuSE SLES 12 SP2
x86_64
rsync-debuginfo-3.1.0-13.7.1
rsync-3.1.0-13.7.1
rsync-debugsource-3.1.0-13.7.1

SuSE SLED 12 SP3
x86_64
rsync-debuginfo-3.1.0-13.7.1
rsync-3.1.0-13.7.1
rsync-debugsource-3.1.0-13.7.1

SuSE SLED 12 SP2
x86_64
rsync-debuginfo-3.1.0-13.7.1
rsync-3.1.0-13.7.1
rsync-debugsource-3.1.0-13.7.1

SuSE SLES 12 SP3
x86_64
rsync-debuginfo-3.1.0-13.7.1
rsync-3.1.0-13.7.1
rsync-debugsource-3.1.0-13.7.1

146266 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0181-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13194

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0181-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003623.html

SuSE SLED 12 SP2
x86_64

libvpx-debugsource-1.3.0-3.3.1
libvpx1-32bit-1.3.0-3.3.1
libvpx1-debuginfo-32bit-1.3.0-3.3.1
vpx-tools-debuginfo-1.3.0-3.3.1
vpx-tools-1.3.0-3.3.1
libvpx1-debuginfo-1.3.0-3.3.1
libvpx1-1.3.0-3.3.1

SuSE SLES 12 SP3
x86_64
libvpx-debugsource-1.3.0-3.3.1
libvpx1-1.3.0-3.3.1
libvpx1-debuginfo-1.3.0-3.3.1

SuSE SLES 12 SP2
x86_64
libvpx-debugsource-1.3.0-3.3.1
libvpx1-1.3.0-3.3.1
libvpx1-debuginfo-1.3.0-3.3.1

SuSE SLED 12 SP3
x86_64
libvpx-debugsource-1.3.0-3.3.1
libvpx1-32bit-1.3.0-3.3.1
libvpx1-debuginfo-32bit-1.3.0-3.3.1
vpx-tools-debuginfo-1.3.0-3.3.1
vpx-tools-1.3.0-3.3.1
libvpx1-debuginfo-1.3.0-3.3.1
libvpx1-1.3.0-3.3.1

146267 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0122-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8816, CVE-2017-8817

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0122-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003607.html

SuSE SLES 12 SP2
x86_64
libcurl4-debuginfo-7.37.0-37.11.3
libcurl4-32bit-7.37.0-37.11.3
libcurl4-debuginfo-32bit-7.37.0-37.11.3
curl-7.37.0-37.11.3
curl-debuginfo-7.37.0-37.11.3
libcurl4-7.37.0-37.11.3
curl-debugsource-7.37.0-37.11.3

SuSE SLED 12 SP3
x86_64

libcurl4-7.37.0-37.11.3
libcurl4-32bit-7.37.0-37.11.3
libcurl4-debuginfo-7.37.0-37.11.3
curl-7.37.0-37.11.3
curl-debuginfo-7.37.0-37.11.3
libcurl4-debuginfo-32bit-7.37.0-37.11.3
curl-debugsource-7.37.0-37.11.3

SuSE SLED 12 SP2
x86_64
libcurl4-7.37.0-37.11.3
libcurl4-32bit-7.37.0-37.11.3
libcurl4-debuginfo-7.37.0-37.11.3
curl-7.37.0-37.11.3
curl-debuginfo-7.37.0-37.11.3
libcurl4-debuginfo-32bit-7.37.0-37.11.3
curl-debugsource-7.37.0-37.11.3

SuSE SLES 12 SP3
x86_64
libcurl4-debuginfo-7.37.0-37.11.3
libcurl4-32bit-7.37.0-37.11.3
libcurl4-debuginfo-32bit-7.37.0-37.11.3
curl-7.37.0-37.11.3
curl-debuginfo-7.37.0-37.11.3
libcurl4-7.37.0-37.11.3
curl-debugsource-7.37.0-37.11.3

146268 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0153-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10672

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0153-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00056.html

SuSE Linux 42.2
x86_64
perl-XML-LibXML-2.0019-7.3.1
perl-XML-LibXML-debugsource-2.0019-7.3.1
perl-XML-LibXML-debuginfo-2.0019-7.3.1

i586
perl-XML-LibXML-2.0019-7.3.1
perl-XML-LibXML-debugsource-2.0019-7.3.1
perl-XML-LibXML-debuginfo-2.0019-7.3.1

SuSE Linux 42.3
x86_64
perl-XML-LibXML-2.0019-10.1

perl-XML-LibXML-debuginfo-2.0019-10.1
perl-XML-LibXML-debugsource-2.0019-10.1

i586
perl-XML-LibXML-2.0019-10.1
perl-XML-LibXML-debuginfo-2.0019-10.1
perl-XML-LibXML-debugsource-2.0019-10.1

146270 - SuSE SLES 11 SP4 SUSE-SU-2018:0117-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16548, CVE-2017-17433, CVE-2017-17434

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0117-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003603.html

SuSE SLES 11 SP4
i586
rsync-3.0.4-2.53.3.1

x86_64
rsync-3.0.4-2.53.3.1

146271 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0130-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10800, CVE-2017-11141, CVE-2017-11529, CVE-2017-11644, CVE-2017-11724, CVE-2017-12434, CVE-2017-12564, CVE-2017-12667, CVE-2017-12670, CVE-2017-12672, CVE-2017-12675, CVE-2017-13060, CVE-2017-13146, CVE-2017-13648, CVE-2017-13658, CVE-2017-14326, CVE-2017-14533, CVE-2017-17881, CVE-2017-18022, CVE-2018-5246, CVE-2018-5247

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0130-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003611.html

SuSE SLED 12 SP2
x86_64
ImageMagick-debugsource-6.8.8.1-71.26.1
libMagick++-6_Q16-3-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.26.1

libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.26.1
ImageMagick-debuginfo-6.8.8.1-71.26.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.26.1
ImageMagick-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-6.8.8.1-71.26.1
libMagickWand-6_Q16-1-6.8.8.1-71.26.1

SuSE SLES 12 SP3
x86_64
ImageMagick-debugsource-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-6.8.8.1-71.26.1
ImageMagick-debuginfo-6.8.8.1-71.26.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.26.1
libMagickWand-6_Q16-1-6.8.8.1-71.26.1

SuSE SLES 12 SP2
x86_64
ImageMagick-debugsource-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-6.8.8.1-71.26.1
ImageMagick-debuginfo-6.8.8.1-71.26.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.26.1
libMagickWand-6_Q16-1-6.8.8.1-71.26.1

SuSE SLED 12 SP3
x86_64
ImageMagick-debugsource-6.8.8.1-71.26.1
libMagick++-6_Q16-3-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.26.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.26.1
ImageMagick-debuginfo-6.8.8.1-71.26.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.26.1
ImageMagick-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.26.1
libMagickCore-6_Q16-1-6.8.8.1-71.26.1
libMagickWand-6_Q16-1-6.8.8.1-71.26.1

146272 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0174-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5764

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0174-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003619.html

SuSE SLES 12 SP2
x86_64

rsync-debugsource-3.1.0-13.10.1
rsync-debuginfo-3.1.0-13.10.1
rsync-3.1.0-13.10.1

SuSE SLED 12 SP3
x86_64
rsync-debugsource-3.1.0-13.10.1
rsync-debuginfo-3.1.0-13.10.1
rsync-3.1.0-13.10.1

SuSE SLED 12 SP2
x86_64
rsync-debugsource-3.1.0-13.10.1
rsync-debuginfo-3.1.0-13.10.1
rsync-3.1.0-13.10.1

SuSE SLES 12 SP3
x86_64
rsync-debugsource-3.1.0-13.10.1
rsync-debuginfo-3.1.0-13.10.1
rsync-3.1.0-13.10.1

146273 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2018:0140-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0486

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0140-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003614.html

SuSE SLES 12 SP3
x86_64
libxmltooling6-debuginfo-1.5.6-3.3.2
xmltooling-debugsource-1.5.6-3.3.2
xmltooling-schemas-1.5.6-3.3.2
libxmltooling6-1.5.6-3.3.2

SuSE SLES 12 SP2
x86_64
libxmltooling6-debuginfo-1.5.6-3.3.2
xmltooling-debugsource-1.5.6-3.3.2
xmltooling-schemas-1.5.6-3.3.2
libxmltooling6-1.5.6-3.3.2

146274 - SuSE SLES 11 SP4 SUSE-SU-2018:0172-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5764

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0172-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003617.html

SuSE SLES 11 SP4
i586
rsync-3.0.4-2.53.6.1

x86_64
rsync-3.0.4-2.53.6.1

146275 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0158-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0486

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0158-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00061.html

SuSE Linux 42.2
x86_64
libxmltooling-devel-1.5.6-3.3.1
libxmltooling6-1.5.6-3.3.1
libxmltooling6-debuginfo-1.5.6-3.3.1
xmltooling-schemas-1.5.6-3.3.1
xmltooling-debugsource-1.5.6-3.3.1

SuSE Linux 42.3
x86_64
xmltooling-debugsource-1.5.6-6.1
libxmltooling-devel-1.5.6-6.1
libxmltooling6-1.5.6-6.1
xmltooling-schemas-1.5.6-6.1
libxmltooling6-debuginfo-1.5.6-6.1

146279 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0161-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8816, CVE-2017-8817

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0161-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00064.html

SuSE Linux 42.2
x86_64
libcurl4-32bit-7.37.0-16.12.1
libcurl-devel-32bit-7.37.0-16.12.1
curl-debuginfo-7.37.0-16.12.1
libcurl4-debuginfo-7.37.0-16.12.1
libcurl4-debuginfo-32bit-7.37.0-16.12.1
libcurl4-7.37.0-16.12.1
curl-debugsource-7.37.0-16.12.1
libcurl-devel-7.37.0-16.12.1
curl-7.37.0-16.12.1

i586
curl-debuginfo-7.37.0-16.12.1
libcurl4-debuginfo-7.37.0-16.12.1
libcurl4-7.37.0-16.12.1
curl-debugsource-7.37.0-16.12.1
libcurl-devel-7.37.0-16.12.1
curl-7.37.0-16.12.1

SuSE Linux 42.3
x86_64
libcurl-devel-7.37.0-27.1
libcurl4-32bit-7.37.0-27.1
curl-7.37.0-27.1
libcurl4-debuginfo-7.37.0-27.1
curl-debuginfo-7.37.0-27.1
libcurl-devel-32bit-7.37.0-27.1
libcurl4-7.37.0-27.1
libcurl4-debuginfo-32bit-7.37.0-27.1
curl-debugsource-7.37.0-27.1

i586
libcurl-devel-7.37.0-27.1
curl-7.37.0-27.1
libcurl4-debuginfo-7.37.0-27.1
curl-debuginfo-7.37.0-27.1
libcurl4-7.37.0-27.1
curl-debugsource-7.37.0-27.1

146280 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0155-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10800, CVE-2017-11141, CVE-2017-11529, CVE-2017-11644, CVE-2017-11724, CVE-2017-12434, CVE-2017-12564, CVE-2017-12667, CVE-2017-12670, CVE-2017-12672, CVE-2017-12675, CVE-2017-13060, CVE-2017-13146, CVE-2017-13648, CVE-2017-13658, CVE-2017-14326, CVE-2017-14533, CVE-2017-17881, CVE-2017-18022, CVE-2018-5246, CVE-2018-5247

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0155-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00058.html

SuSE Linux 42.2
i586
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.21.1
ImageMagick-devel-6.8.8.1-30.21.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.21.1
ImageMagick-debuginfo-6.8.8.1-30.21.1
perl-PerlMagick-debuginfo-6.8.8.1-30.21.1
ImageMagick-debugsource-6.8.8.1-30.21.1
libMagick++-devel-6.8.8.1-30.21.1
libMagickWand-6_Q16-1-6.8.8.1-30.21.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.21.1
ImageMagick-extra-6.8.8.1-30.21.1
libMagickCore-6_Q16-1-6.8.8.1-30.21.1
libMagick++-6_Q16-3-6.8.8.1-30.21.1
perl-PerlMagick-6.8.8.1-30.21.1
ImageMagick-extra-debuginfo-6.8.8.1-30.21.1
ImageMagick-6.8.8.1-30.21.1

noarch
ImageMagick-doc-6.8.8.1-30.21.1

x86_64
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-30.21.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.21.1
ImageMagick-devel-6.8.8.1-30.21.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.21.1
ImageMagick-debuginfo-6.8.8.1-30.21.1
perl-PerlMagick-debuginfo-6.8.8.1-30.21.1
ImageMagick-debugsource-6.8.8.1-30.21.1
libMagick++-devel-6.8.8.1-30.21.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-30.21.1
libMagick++-devel-32bit-6.8.8.1-30.21.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-30.21.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-30.21.1
libMagick++-6_Q16-3-32bit-6.8.8.1-30.21.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-30.21.1
libMagickWand-6_Q16-1-6.8.8.1-30.21.1
ImageMagick-devel-32bit-6.8.8.1-30.21.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.21.1
ImageMagick-extra-6.8.8.1-30.21.1
libMagickCore-6_Q16-1-6.8.8.1-30.21.1
libMagick++-6_Q16-3-6.8.8.1-30.21.1
perl-PerlMagick-6.8.8.1-30.21.1
ImageMagick-extra-debuginfo-6.8.8.1-30.21.1
ImageMagick-6.8.8.1-30.21.1

SuSE Linux 42.3
i586

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-49.1
libMagick++-devel-6.8.8.1-49.1
libMagickCore-6_Q16-1-6.8.8.1-49.1
ImageMagick-extra-debuginfo-6.8.8.1-49.1
ImageMagick-6.8.8.1-49.1
perl-PerlMagick-debuginfo-6.8.8.1-49.1
ImageMagick-devel-6.8.8.1-49.1
ImageMagick-debugsource-6.8.8.1-49.1
libMagickWand-6_Q16-1-6.8.8.1-49.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-49.1
ImageMagick-extra-6.8.8.1-49.1
perl-PerlMagick-6.8.8.1-49.1
libMagick++-6_Q16-3-6.8.8.1-49.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-49.1
ImageMagick-debuginfo-6.8.8.1-49.1

noarch
ImageMagick-doc-6.8.8.1-49.1

x86_64
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-49.1
libMagick++-devel-6.8.8.1-49.1
libMagickCore-6_Q16-1-6.8.8.1-49.1
ImageMagick-extra-debuginfo-6.8.8.1-49.1
ImageMagick-devel-32bit-6.8.8.1-49.1
ImageMagick-6.8.8.1-49.1
perl-PerlMagick-debuginfo-6.8.8.1-49.1
ImageMagick-devel-6.8.8.1-49.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-49.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-49.1
ImageMagick-debugsource-6.8.8.1-49.1
libMagick++-devel-32bit-6.8.8.1-49.1
libMagickWand-6_Q16-1-6.8.8.1-49.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-49.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-49.1
ImageMagick-extra-6.8.8.1-49.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-49.1
perl-PerlMagick-6.8.8.1-49.1
libMagick++-6_Q16-3-6.8.8.1-49.1
libMagick++-6_Q16-3-32bit-6.8.8.1-49.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-49.1
ImageMagick-debuginfo-6.8.8.1-49.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-49.1

160347 - CentOS 6 CESA-2018-0101 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
CESA-2018-0101

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022714.html

CentOS 6
x86_64
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5

i686
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5

160348 - CentOS 7 CESA-2018-0094 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2018-0094

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022711.html

CentOS 7
noarch
iwl3160-firmware-22.0.7.0-58.el7_4
iwl1000-firmware-39.31.5.1-58.el7_4
iwl2000-firmware-18.168.6.1-58.el7_4
iwl4965-firmware-228.61.2.24-58.el7_4
linux-firmware-20170606-58.gitc990aae.el7_4
iwl7265-firmware-22.0.7.0-58.el7_4
iwl7260-firmware-22.0.7.0-58.el7_4
iwl105-firmware-18.168.6.1-58.el7_4
iwl6000g2b-firmware-17.168.5.2-58.el7_4
iwl3945-firmware-15.32.2.9-58.el7_4
iwl135-firmware-18.168.6.1-58.el7_4
iwl6050-firmware-41.28.5.1-58.el7_4
iwl100-firmware-39.31.5.1-58.el7_4
iwl2030-firmware-18.168.6.1-58.el7_4
iwl6000g2a-firmware-17.168.5.3-58.el7_4
iwl6000-firmware-9.221.4.1-58.el7_4
iwl5150-firmware-8.24.2.2-58.el7_4
iwl5000-firmware-8.83.5.1_1-58.el7_4

160349 - CentOS 6, 7 CESA-2018-0095 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

The scan detected that the host is missing the following update:
CESA-2018-0095

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022713.html
http://lists.centos.org/pipermail/centos-announce/2018-January/022712.html

CentOS 7
i686
java-1.8.0-openjdk-accessibility-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.161-0.b14.el7_4

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.161-0.b14.el7_4

x86_64
java-1.8.0-openjdk-accessibility-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-accessibility-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.161-0.b14.el7_4

CentOS 6
i686
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9

java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.161-3.b14.el6_9

x86_64
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9

160350 - CentOS 7 CESA-2018-0102 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
CESA-2018-0102

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022715.html

CentOS 7
i686
bind-libs-lite-9.9.4-51.el7_4.2
bind-devel-9.9.4-51.el7_4.2
bind-lite-devel-9.9.4-51.el7_4.2
bind-pkcs11-libs-9.9.4-51.el7_4.2
bind-pkcs11-devel-9.9.4-51.el7_4.2
bind-libs-9.9.4-51.el7_4.2

noarch
bind-license-9.9.4-51.el7_4.2

x86_64
bind-9.9.4-51.el7_4.2
bind-utils-9.9.4-51.el7_4.2
bind-sdb-chroot-9.9.4-51.el7_4.2
bind-libs-lite-9.9.4-51.el7_4.2
bind-libs-9.9.4-51.el7_4.2
bind-pkcs11-libs-9.9.4-51.el7_4.2
bind-devel-9.9.4-51.el7_4.2

bind-pkcs11-devel-9.9.4-51.el7_4.2
bind-chroot-9.9.4-51.el7_4.2
bind-pkcs11-9.9.4-51.el7_4.2
bind-sdb-9.9.4-51.el7_4.2
bind-lite-devel-9.9.4-51.el7_4.2
bind-pkcs11-utils-9.9.4-51.el7_4.2

160351 - CentOS 6, 7 CESA-2018-0093 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2018-0093

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022709.html
http://lists.centos.org/pipermail/centos-announce/2018-January/022710.html

CentOS 7
x86_64
microcode_ctl-2.1-22.5.el7_4

CentOS 6
x86_64
microcode_ctl-1.17-25.4.el6_9

i686
microcode_ctl-1.17-25.4.el6_9

163529 - Oracle Enterprise Linux ELSA-2018-0102 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
ELSA-2018-0102

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007468.html

OEL7
x86_64
bind-9.9.4-51.el7_4.2
bind-lite-devel-9.9.4-51.el7_4.2
bind-utils-9.9.4-51.el7_4.2

bind-sdb-chroot-9.9.4-51.el7_4.2
bind-libs-lite-9.9.4-51.el7_4.2
bind-libs-9.9.4-51.el7_4.2
bind-pkcs11-libs-9.9.4-51.el7_4.2
bind-devel-9.9.4-51.el7_4.2
bind-pkcs11-devel-9.9.4-51.el7_4.2
bind-chroot-9.9.4-51.el7_4.2
bind-pkcs11-9.9.4-51.el7_4.2
bind-sdb-9.9.4-51.el7_4.2
bind-license-9.9.4-51.el7_4.2
bind-pkcs11-utils-9.9.4-51.el7_4.2

163530 - Oracle Enterprise Linux ELSA-2018-0101 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
ELSA-2018-0101

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007469.html

OEL6
x86_64
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5

i386
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5

163534 - Oracle Enterprise Linux ELSA-2018-0095 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

The scan detected that the host is missing the following update:
ELSA-2018-0095

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007459.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007460.html

OEL7
x86_64
java-1.8.0-openjdk-accessibility-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.161-0.b14.el7_4

OEL6
x86_64
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9

i386
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9

175312 - Scientific Linux Security ERRATA Important: bind on SL6.x i386/x86_64 (1801-7533)

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL6.x i386/x86_64 (1801-7533)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=7533

SL6
x86_64
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-debuginfo-9.8.2-0.62.rc1.el6_9.5

i386
bind-sdb-9.8.2-0.62.rc1.el6_9.5
bind-9.8.2-0.62.rc1.el6_9.5
bind-utils-9.8.2-0.62.rc1.el6_9.5
bind-chroot-9.8.2-0.62.rc1.el6_9.5
bind-devel-9.8.2-0.62.rc1.el6_9.5
bind-libs-9.8.2-0.62.rc1.el6_9.5
bind-debuginfo-9.8.2-0.62.rc1.el6_9.5

175313 - Scientific Linux Security ERRATA Important: bind on SL7.x x86_64 (1801-7212)

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

Risk Level: High

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL7.x x86_64 (1801-7212)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=7212

SL7
x86_64
bind-9.9.4-51.el7_4.2
bind-utils-9.9.4-51.el7_4.2
bind-sdb-9.9.4-51.el7_4.2
bind-sdb-chroot-9.9.4-51.el7_4.2
bind-libs-lite-9.9.4-51.el7_4.2
bind-libs-9.9.4-51.el7_4.2
bind-devel-9.9.4-51.el7_4.2

bind-debuginfo-9.9.4-51.el7_4.2
bind-pkcs11-devel-9.9.4-51.el7_4.2
bind-chroot-9.9.4-51.el7_4.2
bind-pkcs11-9.9.4-51.el7_4.2
bind-pkcs11-libs-9.9.4-51.el7_4.2
bind-lite-devel-9.9.4-51.el7_4.2
bind-pkcs11-utils-9.9.4-51.el7_4.2

noarch
bind-license-9.9.4-51.el7_4.2

175314 - Scientific Linux Security ERRATA Important: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1801-6612)

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1801-6612)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=6612

SL7
x86_64
java-1.8.0-openjdk-accessibility-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-src-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-debuginfo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-headless-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-devel-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-demo-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-accessibility-debug-1.8.0.161-0.b14.el7_4

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-1.8.0.161-0.b14.el7_4
java-1.8.0-openjdk-javadoc-zip-1.8.0.161-0.b14.el7_4

SL6
i386
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9

java-1.8.0-openjdk-debuginfo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.161-3.b14.el6_9

x86_64
java-1.8.0-openjdk-src-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-demo-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-devel-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-debug-1.8.0.161-3.b14.el6_9
java-1.8.0-openjdk-headless-1.8.0.161-3.b14.el6_9

182576 - FreeBSD MySQL Multiple Vulnerabilities (e3445736-fd01-11e7-ac58-b499baebfeaf)

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

Risk Level: High

CVE: CVE-2018-2562, CVE-2018-2565, CVE-2018-2573, CVE-2018-2576, CVE-2018-2583, CVE-2018-2586, CVE-2018-2590, CVE-2018-2591, CVE-2018-2600, CVE-2018-2612, CVE-2018-2622, CVE-2018-2640, CVE-2018-2645, CVE-2018-2646, CVE-2018-2647, CVE-2018-2665, CVE-2018-2667, CVE-2018-2668, CVE-2018-2696, CVE-2018-2703

Description

The scan detected that the host is missing the following update:
MySQL -- multiple vulnerabilities (e3445736-fd01-11e7-ac58-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/e3445736-fd01-11e7-ac58-b499baebfeaf.html

Affected packages:
mariadb55-server < 5.5.59
mariadb100-server < 10.0.34
mariadb101-server < 10.1.31
mariadb102-server < 10.2.13
mysql55-server < 5.5.59
mysql56-server < 5.6.39
mysql57-server < 5.7.21
percona55-server < 5.5.59
percona56-server < 5.6.39
percona57-server < 5.7.21

186060 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3538-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2017-15906

Description

The scan detected that the host is missing the following update:
USN-3538-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004236.html

Ubuntu 16.04

openssh-server_7.2p2-4ubuntu2.4

Ubuntu 14.04

openssh-server_6.6p1-2ubuntu2.10

Ubuntu 17.10

openssh-server_7.5p1-10ubuntu0.1

186062 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3537-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-2562, CVE-2018-2565, CVE-2018-2573, CVE-2018-2576, CVE-2018-2583, CVE-2018-2586, CVE-2018-2590, CVE-2018-2600, CVE-2018-2612, CVE-2018-2622, CVE-2018-2640, CVE-2018-2645, CVE-2018-2646, CVE-2018-2647, CVE-2018-2665, CVE-2018-2667, CVE-2018-2668, CVE-2018-2696, CVE-2018-2703

Description

The scan detected that the host is missing the following update:
USN-3537-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004235.html

Ubuntu 16.04

mysql-server-5.7_5.7.21-0ubuntu0.16.04.1

Ubuntu 14.04

mysql-server-5.5_5.5.59-0ubuntu0.14.04.1

Ubuntu 17.10

mysql-server-5.7_5.7.21-0ubuntu0.17.10.1

193190 - Fedora Linux 27 FEDORA-2018-c4e4935e01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5205, CVE-2018-5206, CVE-2018-5207, CVE-2018-5208

Description

The scan detected that the host is missing the following update:
FEDORA-2018-c4e4935e01

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/2018/1/?count=200&page=4

Fedora Core 27

irssi-1.0.6-1.fc27

193194 - Fedora Linux 27 FEDORA-2018-75e780a7c2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0903

Description

The scan detected that the host is missing the following update:
FEDORA-2018-75e780a7c2

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/2018/1/?count=200&page=1

Fedora Core 27

ruby-2.4.3-86.fc27

193197 - Fedora Linux 26 FEDORA-2018-bc08435961 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5205, CVE-2018-5206, CVE-2018-5207, CVE-2018-5208

Description

The scan detected that the host is missing the following update:
FEDORA-2018-bc08435961

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/2018/1/?count=200&page=4

Fedora Core 26

irssi-1.0.6-1.fc26

22897 - (K39428424) F5 BIG-IP SQL Injection Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-0304

Description

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

Observation

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

A SQL injection vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the management UI. Successful exploitation could allow an attacker to execute arbitrary code.

22980 - (VMSA-2017-0021) VMware Fusion Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4933, CVE-2017-4941

Description

Multiple vulnerabilities are present in some versions of VMware Fusion.

Observation

VMware Fusion is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware Fusion. The flaws lie in the VNC component. Successful exploitation could allow an attacker to execute arbitrary remote code via an authenticated VNC session.

22988 - IBM WebSphere Portal Cross-Site Scripting Vulnerability (swg22012409)

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

Risk Level: Medium

CVE: CVE-2018-1361

Description

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

Observation

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

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in Web UI. Successful exploitation could allow an attacker to perform cross-site scripting attacks.

22990 - IBM Tivoli Storage Manager Server Buffer Overflow Vulnerability (swg21998747)

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

Risk Level: Medium

CVE: CVE-2016-8998

Description

A buffer overflow vulnerability is present in some versions of IBM Tivoli Storage Manager Server.

Observation

IBM Tivoli Storage Manager is an enterprise-wide storage management application.

A buffer overflow vulnerability is present in some versions of IBM Tivoli Storage Manager Server. The flaw is due to improperly formatted SELECT command. Successful exploitation could allow an attacker to execute arbitrary code on the server.

132432 - Oracle VM OVMSA-2018-0012 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000407, CVE-2017-5753

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0012

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000822.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-112.14.13.el6uek
kernel-uek-4.1.12-112.14.13.el6uek

146281 - SuSE SLES 11 SP4 SUSE-SU-2018:0119-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5823, CVE-2016-5824, CVE-2016-5825, CVE-2016-5826, CVE-2016-5827, CVE-2016-9584

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0119-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003605.html

SuSE SLES 11 SP4
i586
libical0-0.43-1.10.6.1

x86_64
libical0-32bit-0.43-1.10.6.1
libical0-0.43-1.10.6.1

163531 - Oracle Enterprise Linux ELSA-2018-4017 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000407, CVE-2017-5753

Description

The scan detected that the host is missing the following update:
ELSA-2018-4017

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007463.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007464.html

OEL7
x86_64
kernel-uek-doc-4.1.12-112.14.13.el7uek
kernel-uek-firmware-4.1.12-112.14.13.el7uek
kernel-uek-devel-4.1.12-112.14.13.el7uek
kernel-uek-4.1.12-112.14.13.el7uek
kernel-uek-debug-devel-4.1.12-112.14.13.el7uek
kernel-uek-debug-4.1.12-112.14.13.el7uek

OEL6
x86_64
kernel-uek-debug-devel-4.1.12-112.14.13.el6uek
kernel-uek-devel-4.1.12-112.14.13.el6uek
kernel-uek-doc-4.1.12-112.14.13.el6uek
kernel-uek-4.1.12-112.14.13.el6uek
kernel-uek-firmware-4.1.12-112.14.13.el6uek
kernel-uek-debug-4.1.12-112.14.13.el6uek

22759 - (K23432135) F5 BIG-IP Apache Struts 2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-3093

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw is due to improper handling of a crafted device that provides a small report descriptor. Successful exploitation could allow a remote attacker to cause a denial of service.

22877 - Cisco ASA 5500 Software TLS Bleichenbacher Attack Vulnerability (CSCvg97652)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12373

Description

A vulnerability is present in some versions of Cisco ASA 5500 series devices.

Observation

Cisco Adaptive Security Appliance is a word-class line of network security devices.

A vulnerability is present in some versions of Cisco ASA 5500 series devices. The flaw lies in the TLS protocol implementation. Successful exploitation could allow an attacker to retrieve sensitive data.

22962 - IBM WebSphere Message Broker Apache Tomcat Vulnerability (swg22011443)

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

Risk Level: Medium

CVE: CVE-2017-5664

Description

A vulnerability is present in some versions of IBM WebSphere Message Broker.

Observation

IBM WebSphere Message Broker is a popular advanced Enterprise Service Bus.

A vulnerability is present in some versions of IBM WebSphere Message Broker. The flaw lies in the Apache Tomcat component. Successful exploitation could allow a remote attacker to bypass security restrictions.

22973 - Mozilla Firefox Multiple Vulnerabilities Prior To 57.0.4

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to disclose private information.

22974 - Mozilla Firefox Multiple Vulnerabilities Prior To 57.0.4

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to disclose private information.

22983 - IBM WebSphere Portal Information Disclosure Vulnerability (swg22011519)

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

Risk Level: Medium

CVE: CVE-2017-1698

Description

An information disclosure vulnerability is present in some versions of IBM WebSphere Portal.

Observation

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

An information disclosure vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in an error message that discloses sensitive data. Successful exploitation could allow an attacker to retrieve critical information from the target system.

22987 - (HT208403) Apple Safari Vulnerabilities Prior To 11.0.2

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

Multiple vulnerabilities are present in some versions of Apple Safari. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information.

22989 - WECON LeviStudio Multiple Buffer Overflow Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-16737, CVE-2017-16739

Description

Multiple buffer overflow vulnerabilities are present in some versions of WECON LeviStudio.

Observation

WECON LeviStudio is an HMI programming software.

Multiple buffer overflow vulnerabilities are present in some versions of WECON LeviStudio. The flaws occur due to multiple buffer overflow issues. Successful exploitation could allow an attacker to execute arbitrary code.

22991 - (SB10220) McAfee Security Information And Event Management OpenSSL Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

Multiple vulnerabilities are present in some versions of McAfee Security Information and Event Management.

Observation

McAfee Security Information and Event Management brings event, threat, and risk data together to provide strong security intelligence.

Multiple vulnerabilities are present in some versions of McAfee Security Information and Event Management. The flaws lie in OpenSSL. Successful exploitation could allow an attacker to access potentially sensitive information.

22997 - (K91229003) F5 BIG-IP Side-Channel Processor Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

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

Observation

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

Multiple vulnerabilities are present in some versions of F5 BIG-IP products. The flaws lie in several components. Successful exploitation could allow a local attacker to cause disclosure of information.

23002 - (MSPT-Jan2018) Microsoft Office for MAC Spoofing Vulnerability (CVE-2018-0819)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0819

Description

A vulnerability in some versions of Microsoft Office for MAC could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Office for MAC could lead to spoofing.

The flaw exists when Microsoft Outlook for MAC does not properly handle the encoding and display of email addresses. Successful exploitation could allow an attacker to launch a social engineering attack.

23004 - (SB10220) McAfee Threat Intelligence Exchange OpenSSL Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

Multiple vulnerabilities are present in some versions of McAfee Threat Intelligence Exchange.

Observation

McAfee Threat Intelligence Exchange Server is a real-time threat detection and response software.

Multiple vulnerabilities are present in some versions of McAfee Threat Intelligence Exchange. The flaws lie in the OpenSSL component. Successful exploitation could affect confidentiality or integrity of the system.

23012 - Cisco NX-OS Software Unauthorized User Account Deletion Vulnerability (cisco-sa-20180117-nxos1)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0092

Description

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

Observation

Cisco NX-OS is a network operating system .

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in lack of proper RBAC checks for users. Successful exploitation could allow a local attacker to bypass the security restrictions and impact the integrity of the system.

146261 - SuSE SLES 11 SP4 SUSE-SU-2018:0179-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17935, CVE-2018-5334, CVE-2018-5335, CVE-2018-5336

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0179-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003621.html

SuSE SLES 11 SP4
i586
libwiretap6-2.2.12-40.17.1
libwscodecs1-2.2.12-40.17.1
wireshark-gtk-2.2.12-40.17.1
libwsutil7-2.2.12-40.17.1
libwireshark8-2.2.12-40.17.1
wireshark-2.2.12-40.17.1

x86_64
libwiretap6-2.2.12-40.17.1

libwscodecs1-2.2.12-40.17.1
wireshark-gtk-2.2.12-40.17.1
libwsutil7-2.2.12-40.17.1
libwireshark8-2.2.12-40.17.1
wireshark-2.2.12-40.17.1

146264 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0151-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6362

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0151-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00054.html

SuSE Linux 42.2
x86_64
gd-devel-2.1.0-18.3.1
gd-32bit-2.1.0-18.3.1
gd-debugsource-2.1.0-18.3.1
gd-debuginfo-2.1.0-18.3.1
gd-debuginfo-32bit-2.1.0-18.3.1
gd-2.1.0-18.3.1

i586
gd-devel-2.1.0-18.3.1
gd-2.1.0-18.3.1
gd-debuginfo-2.1.0-18.3.1
gd-debugsource-2.1.0-18.3.1

SuSE Linux 42.3
x86_64
gd-debuginfo-2.1.0-21.1
gd-debugsource-2.1.0-21.1
gd-devel-2.1.0-21.1
gd-2.1.0-21.1
gd-32bit-2.1.0-21.1
gd-debuginfo-32bit-2.1.0-21.1

i586
gd-debugsource-2.1.0-21.1
gd-2.1.0-21.1
gd-debuginfo-2.1.0-21.1
gd-devel-2.1.0-21.1

146276 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0135-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6362

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0135-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003613.html

SuSE SLED 12 SP2
x86_64
gd-2.1.0-24.3.4
gd-32bit-2.1.0-24.3.4
gd-debugsource-2.1.0-24.3.4
gd-debuginfo-2.1.0-24.3.4
gd-debuginfo-32bit-2.1.0-24.3.4

SuSE SLES 12 SP3
x86_64
gd-debugsource-2.1.0-24.3.4
gd-2.1.0-24.3.4
gd-debuginfo-2.1.0-24.3.4

SuSE SLES 12 SP2
x86_64
gd-debugsource-2.1.0-24.3.4
gd-2.1.0-24.3.4
gd-debuginfo-2.1.0-24.3.4

SuSE SLED 12 SP3
x86_64
gd-2.1.0-24.3.4
gd-32bit-2.1.0-24.3.4
gd-debugsource-2.1.0-24.3.4
gd-debuginfo-2.1.0-24.3.4
gd-debuginfo-32bit-2.1.0-24.3.4

178579 - Gentoo Linux GLSA-201801-17 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201801-17

Observation

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

https://security.gentoo.org/glsa/201801-17

Affected packages:
app-text/poppler < 0.57.0-r1

178580 - Gentoo Linux GLSA-201801-18 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201801-18

Observation

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

https://security.gentoo.org/glsa/201801-18

Affected packages:
net-news/newsbeuter < 2.9-r3

23007 - Oracle VM VirtualBox Critical Patch Update January 2018

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

Risk Level: Medium

CVE: CVE-2017-3736, CVE-2017-5715, CVE-2018-2676, CVE-2018-2685, CVE-2018-2686, CVE-2018-2687, CVE-2018-2688, CVE-2018-2689, CVE-2018-2690, CVE-2018-2693, CVE-2018-2694, CVE-2018-2698

Description

Multiple vulnerabilities are present in some versions of Oracle VirtualBox.

Observation

Oracle VM VirtualBox is a virtualization software.

Multiple vulnerabilities are present in some versions of Oracle VirtualBox. The flaws lie in several components. Successful exploitation could allow an attacker to affect confidentiality, integrity or availability of the target system.

132429 - Oracle VM OVMSA-2018-0010 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0010

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000820.html

OVM3.4

x86_64
kernel-uek-4.1.12-112.14.11.el6uek
kernel-uek-firmware-4.1.12-112.14.11.el6uek

132431 - Oracle VM OVMSA-2018-0013 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0013

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000823.html

OVM3.4
x86_64
microcode_ctl-1.17-25.4.0.2.el6_9

132433 - Oracle VM OVMSA-2018-0011 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0011

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000821.html

OVM3.4
x86_64
microcode_ctl-1.17-25.4.0.1.el6_9

141841 - Red Hat Enterprise Linux RHSA-2018-0111 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0111

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00071.html

RHEL6_4S
x86_64
libvirt-lock-sanlock-0.10.2-18.el6_4.16
libvirt-0.10.2-18.el6_4.16
libvirt-debuginfo-0.10.2-18.el6_4.16
libvirt-python-0.10.2-18.el6_4.16
libvirt-devel-0.10.2-18.el6_4.16
libvirt-client-0.10.2-18.el6_4.16

141843 - Red Hat Enterprise Linux RHSA-2018-0112 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0112

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00070.html

RHEL6_2S
x86_64
libvirt-client-0.9.4-23.el6_2.11
libvirt-debuginfo-0.9.4-23.el6_2.11
libvirt-devel-0.9.4-23.el6_2.11
libvirt-lock-sanlock-0.9.4-23.el6_2.11
libvirt-0.9.4-23.el6_2.11
libvirt-python-0.9.4-23.el6_2.11

141844 - Red Hat Enterprise Linux RHSA-2018-0103 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0103

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00069.html

RHEL6_7S
i386
qemu-guest-agent-0.12.1.2-2.479.el6_7.6
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.6

x86_64
qemu-kvm-tools-0.12.1.2-2.479.el6_7.6
qemu-kvm-0.12.1.2-2.479.el6_7.6
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.6
qemu-img-0.12.1.2-2.479.el6_7.6
qemu-guest-agent-0.12.1.2-2.479.el6_7.6

141845 - Red Hat Enterprise Linux RHSA-2018-0105 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0105

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00068.html

RHEL6_5S
x86_64
qemu-kvm-tools-0.12.1.2-2.415.el6_5.17
qemu-kvm-0.12.1.2-2.415.el6_5.17
qemu-guest-agent-0.12.1.2-2.415.el6_5.17
qemu-kvm-debuginfo-0.12.1.2-2.415.el6_5.17
qemu-img-0.12.1.2-2.415.el6_5.17

141847 - Red Hat Enterprise Linux RHSA-2018-0106 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0106

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00066.html

RHEL6_4S
x86_64
qemu-guest-agent-win32-0.12.1.2-2.355.el6_4.10

qemu-kvm-tools-0.12.1.2-2.355.el6_4.10
qemu-img-0.12.1.2-2.355.el6_4.10
qemu-kvm-debuginfo-0.12.1.2-2.355.el6_4.10
qemu-kvm-0.12.1.2-2.355.el6_4.10
qemu-guest-agent-0.12.1.2-2.355.el6_4.10

141849 - Red Hat Enterprise Linux RHSA-2018-0107 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0107

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00067.html

RHEL6_2S
x86_64
qemu-img-0.12.1.2-2.209.el6_2.6
qemu-kvm-debuginfo-0.12.1.2-2.209.el6_2.6
qemu-kvm-0.12.1.2-2.209.el6_2.6
qemu-kvm-tools-0.12.1.2-2.209.el6_2.6

141851 - Red Hat Enterprise Linux RHSA-2018-0110 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0110

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00072.html

RHEL6_5S
x86_64
libvirt-lock-sanlock-0.10.2-29.el6_5.15
libvirt-debuginfo-0.10.2-29.el6_5.15
libvirt-devel-0.10.2-29.el6_5.15
libvirt-client-0.10.2-29.el6_5.15
libvirt-python-0.10.2-29.el6_5.15
libvirt-0.10.2-29.el6_5.15

141852 - Red Hat Enterprise Linux RHSA-2018-0109 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0109

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00073.html

RHEL6_6S
x86_64
libvirt-python-0.10.2-46.el6_6.7
libvirt-0.10.2-46.el6_6.7
libvirt-debuginfo-0.10.2-46.el6_6.7
libvirt-devel-0.10.2-46.el6_6.7
libvirt-lock-sanlock-0.10.2-46.el6_6.7
libvirt-client-0.10.2-46.el6_6.7

141853 - Red Hat Enterprise Linux RHSA-2018-0104 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0104

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00074.html

RHEL6_6S
x86_64
qemu-kvm-0.12.1.2-2.448.el6_6.5
qemu-guest-agent-0.12.1.2-2.448.el6_6.5
qemu-kvm-tools-0.12.1.2-2.448.el6_6.5
qemu-kvm-debuginfo-0.12.1.2-2.448.el6_6.5
qemu-img-0.12.1.2-2.448.el6_6.5

141855 - Red Hat Enterprise Linux RHSA-2018-0108 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0108

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00075.html

RHEL6_7S
i386
libvirt-devel-0.10.2-54.el6_7.7
libvirt-0.10.2-54.el6_7.7
libvirt-client-0.10.2-54.el6_7.7
libvirt-python-0.10.2-54.el6_7.7
libvirt-debuginfo-0.10.2-54.el6_7.7

x86_64
libvirt-lock-sanlock-0.10.2-54.el6_7.7
libvirt-devel-0.10.2-54.el6_7.7
libvirt-0.10.2-54.el6_7.7
libvirt-python-0.10.2-54.el6_7.7
libvirt-client-0.10.2-54.el6_7.7
libvirt-debuginfo-0.10.2-54.el6_7.7

146260 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0187-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2018-2676, CVE-2018-2685, CVE-2018-2686, CVE-2018-2687, CVE-2018-2688, CVE-2018-2689, CVE-2018-2690, CVE-2018-2693, CVE-2018-2694, CVE-2018-2698

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0187-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00074.html

SuSE Linux 42.2
x86_64
virtualbox-websrv-5.1.32-19.49.1
virtualbox-websrv-debuginfo-5.1.32-19.49.1
virtualbox-guest-kmp-default-5.1.32_k4.4.104_18.44-19.49.1
virtualbox-debuginfo-5.1.32-19.49.1
virtualbox-vnc-5.1.32-19.49.1
virtualbox-guest-kmp-default-debuginfo-5.1.32_k4.4.104_18.44-19.49.1
virtualbox-guest-x11-debuginfo-5.1.32-19.49.1
virtualbox-host-kmp-default-5.1.32_k4.4.104_18.44-19.49.1
virtualbox-guest-tools-5.1.32-19.49.1
virtualbox-guest-tools-debuginfo-5.1.32-19.49.1
virtualbox-host-kmp-default-debuginfo-5.1.32_k4.4.104_18.44-19.49.1
virtualbox-qt-5.1.32-19.49.1
virtualbox-qt-debuginfo-5.1.32-19.49.1

virtualbox-5.1.32-19.49.1
virtualbox-guest-x11-5.1.32-19.49.1
virtualbox-debugsource-5.1.32-19.49.1
virtualbox-devel-5.1.32-19.49.1
python-virtualbox-debuginfo-5.1.32-19.49.1
python-virtualbox-5.1.32-19.49.1

noarch
virtualbox-host-source-5.1.32-19.49.1
virtualbox-guest-source-5.1.32-19.49.1
virtualbox-guest-desktop-icons-5.1.32-19.49.1

SuSE Linux 42.3
x86_64
virtualbox-guest-tools-debuginfo-5.1.32-42.1
virtualbox-websrv-debuginfo-5.1.32-42.1
virtualbox-debuginfo-5.1.32-42.1
virtualbox-guest-kmp-default-debuginfo-5.1.32_k4.4.104_39-42.1
virtualbox-guest-kmp-default-5.1.32_k4.4.104_39-42.1
virtualbox-host-kmp-default-debuginfo-5.1.32_k4.4.104_39-42.1
virtualbox-devel-5.1.32-42.1
virtualbox-debugsource-5.1.32-42.1
python-virtualbox-debuginfo-5.1.32-42.1
virtualbox-qt-debuginfo-5.1.32-42.1
virtualbox-guest-tools-5.1.32-42.1
virtualbox-websrv-5.1.32-42.1
python-virtualbox-5.1.32-42.1
virtualbox-guest-x11-5.1.32-42.1
virtualbox-guest-x11-debuginfo-5.1.32-42.1
virtualbox-host-kmp-default-5.1.32_k4.4.104_39-42.1
virtualbox-5.1.32-42.1
virtualbox-vnc-5.1.32-42.1
virtualbox-qt-5.1.32-42.1

noarch
virtualbox-guest-desktop-icons-5.1.32-42.1
virtualbox-guest-source-5.1.32-42.1
virtualbox-host-source-5.1.32-42.1

146265 - SuSE SLES 11 SP4 SUSE-SU-2018:0178-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13733

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0178-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003620.html

SuSE SLES 11 SP4
i586
libncurses6-5.6-93.15.1

ncurses-utils-5.6-93.15.1
ncurses-devel-5.6-93.15.1
terminfo-5.6-93.15.1
libncurses5-5.6-93.15.1
terminfo-base-5.6-93.15.1
tack-5.6-93.15.1

x86_64
libncurses6-32bit-5.6-93.15.1
libncurses6-5.6-93.15.1
ncurses-utils-5.6-93.15.1
libncurses5-32bit-5.6-93.15.1
ncurses-devel-5.6-93.15.1
terminfo-5.6-93.15.1
libncurses5-5.6-93.15.1
terminfo-base-5.6-93.15.1
ncurses-devel-32bit-5.6-93.15.1
tack-5.6-93.15.1

146269 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0159-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0159-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00062.html

SuSE Linux 42.2
x86_64
ncurses-utils-5.9-55.9.1
terminfo-base-5.9-55.9.1
libncurses6-debuginfo-32bit-5.9-55.9.1
libncurses5-debuginfo-32bit-5.9-55.9.1
ncurses-devel-debuginfo-5.9-55.9.1
ncurses-utils-debuginfo-5.9-55.9.1
tack-5.9-55.9.1
ncurses-devel-debuginfo-32bit-5.9-55.9.1
terminfo-5.9-55.9.1
libncurses5-debuginfo-5.9-55.9.1
ncurses-devel-5.9-55.9.1
libncurses5-5.9-55.9.1
libncurses6-debuginfo-5.9-55.9.1
ncurses-debugsource-5.9-55.9.1
libncurses6-32bit-5.9-55.9.1
ncurses-devel-32bit-5.9-55.9.1
tack-debuginfo-5.9-55.9.1
libncurses6-5.9-55.9.1
libncurses5-32bit-5.9-55.9.1

i586

ncurses-utils-5.9-55.9.1
terminfo-base-5.9-55.9.1
ncurses-devel-debuginfo-5.9-55.9.1
ncurses-utils-debuginfo-5.9-55.9.1
tack-5.9-55.9.1
terminfo-5.9-55.9.1
libncurses5-debuginfo-5.9-55.9.1
ncurses-devel-5.9-55.9.1
libncurses5-5.9-55.9.1
libncurses6-debuginfo-5.9-55.9.1
ncurses-debugsource-5.9-55.9.1
tack-debuginfo-5.9-55.9.1
libncurses6-5.9-55.9.1

SuSE Linux 42.3
x86_64
ncurses-devel-32bit-5.9-62.1
libncurses5-debuginfo-5.9-62.1
ncurses-devel-debuginfo-32bit-5.9-62.1
ncurses-devel-debuginfo-5.9-62.1
libncurses5-debuginfo-32bit-5.9-62.1
terminfo-base-5.9-62.1
libncurses6-debuginfo-5.9-62.1
libncurses5-5.9-62.1
ncurses-utils-5.9-62.1
terminfo-5.9-62.1
libncurses6-debuginfo-32bit-5.9-62.1
ncurses-utils-debuginfo-5.9-62.1
libncurses5-32bit-5.9-62.1
ncurses-devel-5.9-62.1
libncurses6-5.9-62.1
tack-5.9-62.1
tack-debuginfo-5.9-62.1
libncurses6-32bit-5.9-62.1
ncurses-debugsource-5.9-62.1

i586
libncurses5-debuginfo-5.9-62.1
ncurses-devel-debuginfo-5.9-62.1
terminfo-base-5.9-62.1
libncurses6-debuginfo-5.9-62.1
libncurses5-5.9-62.1
ncurses-utils-5.9-62.1
terminfo-5.9-62.1
ncurses-utils-debuginfo-5.9-62.1
ncurses-devel-5.9-62.1
libncurses6-5.9-62.1
tack-5.9-62.1
tack-debuginfo-5.9-62.1
ncurses-debugsource-5.9-62.1

146277 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0149-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10369

Description

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

openSUSE-SU-2018:0149-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00052.html

SuSE Linux 42.2
x86_64
lxterminal-0.2.0-4.3.1
lxterminal-debugsource-0.2.0-4.3.1
lxterminal-debuginfo-0.2.0-4.3.1

noarch
lxterminal-lang-0.2.0-4.3.1

SuSE Linux 42.3
x86_64
lxterminal-0.2.0-7.1
lxterminal-debuginfo-0.2.0-7.1
lxterminal-debugsource-0.2.0-7.1

noarch
lxterminal-lang-0.2.0-7.1

146278 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0120-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0120-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003606.html

SuSE SLES 12 SP2
x86_64
libncurses5-debuginfo-32bit-5.9-55.1
ncurses-utils-debuginfo-5.9-55.1
libncurses5-5.9-55.1
ncurses-devel-debuginfo-32bit-5.9-55.1
libncurses6-debuginfo-32bit-5.9-55.1
ncurses-devel-5.9-55.1
libncurses6-32bit-5.9-55.1
libncurses6-debuginfo-5.9-55.1
libncurses5-debuginfo-5.9-55.1
terminfo-5.9-55.1
tack-5.9-55.1
tack-debuginfo-5.9-55.1
ncurses-devel-debuginfo-5.9-55.1

libncurses6-5.9-55.1
ncurses-utils-5.9-55.1
libncurses5-32bit-5.9-55.1
ncurses-devel-32bit-5.9-55.1
ncurses-debugsource-5.9-55.1
terminfo-base-5.9-55.1

SuSE SLED 12 SP3
x86_64
libncurses5-debuginfo-32bit-5.9-55.1
ncurses-devel-debuginfo-5.9-55.1
ncurses-utils-debuginfo-5.9-55.1
libncurses5-5.9-55.1
libncurses6-32bit-5.9-55.1
libncurses6-debuginfo-5.9-55.1
libncurses5-debuginfo-5.9-55.1
terminfo-5.9-55.1
ncurses-devel-5.9-55.1
tack-debuginfo-5.9-55.1
libncurses6-debuginfo-32bit-5.9-55.1
libncurses6-5.9-55.1
ncurses-utils-5.9-55.1
libncurses5-32bit-5.9-55.1
ncurses-debugsource-5.9-55.1
terminfo-base-5.9-55.1
tack-5.9-55.1

SuSE SLED 12 SP2
x86_64
libncurses5-debuginfo-32bit-5.9-55.1
ncurses-devel-debuginfo-5.9-55.1
ncurses-utils-debuginfo-5.9-55.1
libncurses5-5.9-55.1
libncurses6-32bit-5.9-55.1
libncurses6-debuginfo-5.9-55.1
libncurses5-debuginfo-5.9-55.1
terminfo-5.9-55.1
ncurses-devel-5.9-55.1
tack-debuginfo-5.9-55.1
libncurses6-debuginfo-32bit-5.9-55.1
libncurses6-5.9-55.1
ncurses-utils-5.9-55.1
libncurses5-32bit-5.9-55.1
ncurses-debugsource-5.9-55.1
terminfo-base-5.9-55.1
tack-5.9-55.1

SuSE SLES 12 SP3
x86_64
libncurses5-debuginfo-32bit-5.9-55.1
ncurses-utils-debuginfo-5.9-55.1
libncurses5-5.9-55.1
ncurses-devel-debuginfo-32bit-5.9-55.1
libncurses6-debuginfo-32bit-5.9-55.1
ncurses-devel-5.9-55.1
libncurses6-32bit-5.9-55.1
libncurses6-debuginfo-5.9-55.1
libncurses5-debuginfo-5.9-55.1
terminfo-5.9-55.1
tack-5.9-55.1

tack-debuginfo-5.9-55.1
ncurses-devel-debuginfo-5.9-55.1
libncurses6-5.9-55.1
ncurses-utils-5.9-55.1
libncurses5-32bit-5.9-55.1
ncurses-devel-32bit-5.9-55.1
ncurses-debugsource-5.9-55.1
terminfo-base-5.9-55.1

163528 - Oracle Enterprise Linux ELSA-2018-4018 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
ELSA-2018-4018

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007466.html

OEL7
x86_64
microcode_ctl-2.1-22.5.0.3.el7_4

163532 - Oracle Enterprise Linux ELSA-2018-4019 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
ELSA-2018-4019

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007467.html

OEL6
x86_64
microcode_ctl-1.17-25.4.0.2.el6_9

i386
microcode_ctl-1.17-25.4.0.2.el6_9

163533 - Oracle Enterprise Linux ELSA-2018-0093 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
ELSA-2018-0093

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007461.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007462.html

OEL7
x86_64
microcode_ctl-2.1-22.5.0.2.el7_4

OEL6
x86_64
microcode_ctl-1.17-25.4.0.1.el6_9

i386
microcode_ctl-1.17-25.4.0.1.el6_9

175315 - Scientific Linux Security ERRATA Important: linux-firmware on SL7.x (noarch) (1801-6269)

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: linux-firmware on SL7.x (noarch) (1801-6269)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=6269

SL7
noarch
iwl3160-firmware-22.0.7.0-58.el7_4
iwl1000-firmware-39.31.5.1-58.el7_4
iwl2000-firmware-18.168.6.1-58.el7_4
iwl4965-firmware-228.61.2.24-58.el7_4
linux-firmware-20170606-58.gitc990aae.el7_4
iwl7265-firmware-22.0.7.0-58.el7_4
iwl7260-firmware-22.0.7.0-58.el7_4
iwl105-firmware-18.168.6.1-58.el7_4
iwl6000g2b-firmware-17.168.5.2-58.el7_4
iwl3945-firmware-15.32.2.9-58.el7_4
iwl135-firmware-18.168.6.1-58.el7_4
iwl6050-firmware-41.28.5.1-58.el7_4
iwl100-firmware-39.31.5.1-58.el7_4
iwl2030-firmware-18.168.6.1-58.el7_4

iwl6000g2a-firmware-17.168.5.3-58.el7_4
iwl6000-firmware-9.221.4.1-58.el7_4
iwl5150-firmware-8.24.2.2-58.el7_4
iwl5000-firmware-8.83.5.1_1-58.el7_4

175316 - Scientific Linux Security ERRATA Important: microcode_ctl on SL6.x, SL7.x i386/x86_64 (1801-5918)

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: microcode_ctl on SL6.x, SL7.x i386/x86_64 (1801-5918)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=5918

SL7
x86_64
microcode_ctl-2.1-12.el7_2.3
microcode_ctl-2.1-22.5.el7_4
microcode_ctl-debuginfo-2.1-16.5.el7_3
microcode_ctl-debuginfo-2.1-12.el7_2.3
microcode_ctl-debuginfo-2.1-22.5.el7_4
microcode_ctl-2.1-16.5.el7_3

SL6
x86_64
microcode_ctl-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-20.2.el6_7
microcode_ctl-1.17-19.2.el6_6
microcode_ctl-1.17-20.2.el6_7
microcode_ctl-debuginfo-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-19.2.el6_6

i386
microcode_ctl-1.17-25.4.el6_9
microcode_ctl-debuginfo-1.17-25.4.el6_9

186052 - Ubuntu Linux 14.04 USN-3540-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3540-2

Observation

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

For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004241.html

Ubuntu 14.04

linux-image-4.4.0-111-lowlatency_4.4.0-111.134~14.04.1
linux-image-4.4.0-111-powerpc64-smp_4.4.0-111.134~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.111.95
linux-image-powerpc-e500mc-lts-xenial_4.4.0.111.95
linux-image-aws_4.4.0.1011.11
linux-image-4.4.0-111-powerpc-smp_4.4.0-111.134~14.04.1
linux-image-4.4.0-111-powerpc-e500mc_4.4.0-111.134~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.111.95
linux-image-powerpc64-emb-lts-xenial_4.4.0.111.95
linux-image-4.4.0-111-generic_4.4.0-111.134~14.04.1
linux-image-4.4.0-111-powerpc64-emb_4.4.0-111.134~14.04.1
linux-image-generic-lts-xenial_4.4.0.111.95
linux-image-powerpc-smp-lts-xenial_4.4.0.111.95
linux-image-4.4.0-1011-aws_4.4.0-1011.11

186053 - Ubuntu Linux 17.10 USN-3541-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3541-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004239.html

Ubuntu 17.10

linux-image-generic_4.13.0.31.33
linux-image-4.13.0-31-lowlatency_4.13.0-31.34
linux-image-4.13.0-31-generic_4.13.0-31.34
linux-image-lowlatency_4.13.0.31.33

186058 - Ubuntu Linux 16.04 USN-3541-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3541-2

Observation

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

For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004242.html

Ubuntu 16.04

linux-image-gke_4.13.0.1007.9
linux-image-4.13.0-31-generic_4.13.0-31.34~16.04.1
linux-image-lowlatency-hwe-16.04_4.13.0.31.51
linux-image-gcp_4.13.0.1007.9
linux-image-4.13.0-1006-azure_4.13.0-1006.8
linux-image-4.13.0-1007-gcp_4.13.0-1007.10
linux-image-4.13.0-31-lowlatency_4.13.0-31.34~16.04.1
linux-image-azure_4.13.0.1006.7
linux-image-oem_4.13.0.1017.21
linux-image-generic-hwe-16.04_4.13.0.31.51
linux-image-4.13.0-1017-oem_4.13.0-1017.18

186061 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3531-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
USN-3531-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004233.html

Ubuntu 16.04

intel-microcode_3.20180108.0+really20170707ubuntu16.04.1

Ubuntu 14.04

intel-microcode_3.20180108.0+really20170707ubuntu14.04.1

Ubuntu 17.10

intel-microcode_3.20180108.0+really20170707ubuntu17.10.1

186064 - Ubuntu Linux 12.04 USN-3542-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753

Description

The scan detected that the host is missing the following update:
USN-3542-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004243.html

Ubuntu 12.04

linux-image-generic-lts-trusty_3.13.0.140.131
linux-image-3.13.0-140-generic_3.13.0-140.189~precise1

186066 - Ubuntu Linux 14.04 USN-3542-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753

Description

The scan detected that the host is missing the following update:
USN-3542-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004240.html

Ubuntu 14.04

linux-image-generic_3.13.0.141.151
linux-image-3.13.0-141-generic_3.13.0-141.190
linux-image-lowlatency_3.13.0.141.151
linux-image-3.13.0-141-lowlatency_3.13.0-141.190

186067 - Ubuntu Linux 16.04 USN-3540-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3540-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004238.html

Ubuntu 16.04

linux-image-4.4.0-9023-euclid_4.4.0-9023.24
linux-image-powerpc64-emb_4.4.0.112.118
linux-image-4.4.0-112-powerpc-e500mc_4.4.0-112.135

linux-image-4.4.0-112-lowlatency_4.4.0-112.135
linux-image-aws_4.4.0.1049.51
linux-image-powerpc-e500mc_4.4.0.112.118
linux-image-powerpc64-smp_4.4.0.112.118
linux-image-4.4.0-112-powerpc-smp_4.4.0-112.135
linux-image-4.4.0-112-powerpc64-emb_4.4.0-112.135
linux-image-4.4.0-112-generic-lpae_4.4.0-112.135
linux-image-4.4.0-1049-aws_4.4.0-1049.58
linux-image-4.4.0-112-powerpc64-smp_4.4.0-112.135
linux-image-euclid_4.4.0.9023.24
linux-image-generic-lpae_4.4.0.112.118
linux-image-4.4.0-112-generic_4.4.0-112.135
linux-image-powerpc-smp_4.4.0.112.118
linux-image-generic_4.4.0.112.118
linux-image-lowlatency_4.4.0.112.118

193188 - Fedora Linux 27 FEDORA-2018-6cb474b8ff Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9964

Description

The scan detected that the host is missing the following update:
FEDORA-2018-6cb474b8ff

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/2018/1/?count=200&page=1

Fedora Core 27

python-bottle-0.12.13-1.fc27

193189 - Fedora Linux 26 FEDORA-2018-690989736a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753

Description

The scan detected that the host is missing the following update:
FEDORA-2018-690989736a

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/2018/1/?count=200&page=3

Fedora Core 26

webkitgtk4-2.18.5-1.fc26

193195 - Fedora Linux 26 FEDORA-2018-909707fc68 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9964

Description

The scan detected that the host is missing the following update:
FEDORA-2018-909707fc68

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/2018/1/?count=200&page=2

Fedora Core 26

python-bottle-0.12.13-1.fc26

193196 - Fedora Linux 27 FEDORA-2017-15efa72a0c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14992

Description

The scan detected that the host is missing the following update:
FEDORA-2017-15efa72a0c

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/2018/1/?count=200&page=4

Fedora Core 27

docker-1.13.1-44.git584d391.fc27

193201 - Fedora Linux 27 FEDORA-2018-b528f28c59 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15370, CVE-2017-15371

Description

The scan detected that the host is missing the following update:
FEDORA-2018-b528f28c59

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/2018/1/?count=200&page=1

Fedora Core 27

sox-14.4.2.0-14.fc27

193209 - Fedora Linux 26 FEDORA-2018-b26768593c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15370, CVE-2017-15371

Description

The scan detected that the host is missing the following update:
FEDORA-2018-b26768593c

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/2018/1/?count=200&page=2

Fedora Core 26

sox-14.4.2.0-14.fc26

22789 - (K03331206) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2016-4955

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the NTP component. Successful exploitation could allow attacker to cause a denial of service condition on the target system.

88909 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2018-017-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
SSA:2018-017-01

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=2018&m=slackware-security.552055

Slackware 14.0
x86_64
bind-9.9.11_P1-x86_64-1

Slackware 13.37
x86_64
bind-9.9.11_P1-x86_64-1

Slackware 14.1
x86_64
bind-9.9.11_P1-x86_64-1

Slackware 13.1
x86_64
bind-9.9.11_P1-x86_64-1

Slackware 14.2
x86_64
bind-9.10.6_P1-x86_64-1

i586
bind-9.10.6_P1-i586-1

Slackware 13.0
x86_64
bind-9.9.11_P1-x86_64-1

88910 - Slackware Linux 14.2 SSA:2018-020-01 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:2018-020-01

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=2018&m=slackware-security.325546

Slackware 14.2
x86_64
mozilla-firefox-52.6.0esr-x86_64-1

i586
mozilla-firefox-52.6.0esr-i586-1

130998 - Debian Linux 8.0, 9.0 DSA-4093-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5704

Description

The scan detected that the host is missing the following update:
DSA-4093-1

Observation

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

http://www.debian.org/security/2018/dsa-4093

Debian 8.0
all
openocd_0.8.0-4+deb7u1

Debian 9.0
all
openocd_0.9.0-1+deb8u1

182573 - FreeBSD wordpress Multiple Issues (c04dc18f-fcde-11e7-bdf6-00e04c1ea73d)

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:
wordpress -- multiple issues (c04dc18f-fcde-11e7-bdf6-00e04c1ea73d)

Observation

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

http://www.vuxml.org/freebsd/c04dc18f-fcde-11e7-bdf6-00e04c1ea73d.html

Affected packages:
wordpress < 4.9.2,1
fr-wordpress < 4.9.2,1
de-wordpress < 4.9.2
zh_CN-wordpress < 4.9.2
zh_TW-wordpress < 4.9.2
ja-wordpress < 4.9.2
ru_RU-wordpress < 4.9.2

182574 - FreeBSD powerdns-recursor Insufficient Validation Of DNSSEC Signatures (24a82876-002e-11e8-9a95-0cc47a02c232)

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

Risk Level: Low

CVE: CVE-2018-1000003

Description

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

powerdns-recursor -- insufficient validation of DNSSEC signatures (24a82876-002e-11e8-9a95-0cc47a02c232)

Observation

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

http://www.vuxml.org/freebsd/24a82876-002e-11e8-9a95-0cc47a02c232.html

Affected packages:
powerdns-recursor < 4.1.1

182575 - FreeBSD unbound Vulnerability In The Processing Of Wildcard Synthesized NSEC Records (8d3bae09-fd28-11e7-95f2-005056925db4)

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

Risk Level: Low

CVE: CVE-2017-15105

Description

The scan detected that the host is missing the following update:
unbound -- vulnerability in the processing of wildcard synthesized NSEC records (8d3bae09-fd28-11e7-95f2-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/8d3bae09-fd28-11e7-95f2-005056925db4.html

Affected packages:
unbound < 1.6.8

182577 - FreeBSD chromium Multiple Vulnerabilities (e264e74e-ffe0-11e7-8b91-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-15429

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (e264e74e-ffe0-11e7-8b91-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/e264e74e-ffe0-11e7-8b91-e8e0b747a45a.html

Affected packages:
chromium < 63.0.3239.108

182578 - FreeBSD phpbb3 Multiple Issues (8e89a89a-fd15-11e7-bdf6-00e04c1ea73d)

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:
phpbb3 -- multiple issues (8e89a89a-fd15-11e7-bdf6-00e04c1ea73d)

Observation

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

http://www.vuxml.org/freebsd/8e89a89a-fd15-11e7-bdf6-00e04c1ea73d.html

Affected packages:
phpbb3 < 3.2.2

182579 - FreeBSD gitlab Remote Code Execution On Project Import (65fab89f-2231-46db-8541-978f4e87f32a)

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

Risk Level: Low

CVE: CVE-2017-0915, CVE-2018-3710

Description

The scan detected that the host is missing the following update:
gitlab -- Remote code execution on project import (65fab89f-2231-46db-8541-978f4e87f32a)

Observation

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

http://www.vuxml.org/freebsd/65fab89f-2231-46db-8541-978f4e87f32a.html

Affected packages:
gitlab < 10.1.6

182580 - FreeBSD chromium Out Of Bounds Read (82894193-ffd4-11e7-8b91-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-15428

Description

The scan detected that the host is missing the following update:
chromium -- out of bounds read (82894193-ffd4-11e7-8b91-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/82894193-ffd4-11e7-8b91-e8e0b747a45a.html

Affected packages:
chromium < 62.0.3202.94

182581 - FreeBSD chromium Multiple Vulnerabilities (1d951e85-ffdb-11e7-8b91-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427, CVE-2017-15430

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (1d951e85-ffdb-11e7-8b91-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/1d951e85-ffdb-11e7-8b91-e8e0b747a45a.html

Affected packages:
chromium < 63.0.3239.84

182582 - FreeBSD mozilla Multiple Vulnerabilities (a891c5b4-3d7a-4de9-9c71-eef3fd698c77)

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

Risk Level: Low

CVE: CVE-2018-5089, CVE-2018-5090, CVE-2018-5091, CVE-2018-5092, CVE-2018-5093, CVE-2018-5094, CVE-2018-5095, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5100, CVE-2018-5101, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5105, CVE-2018-5106, CVE-2018-5107, CVE-2018-5108, CVE-2018-5109, CVE-2018-5110, CVE-2018-5111, CVE-2018-5112, CVE-2018-5113, CVE-2018-5114, CVE-2018-5115, CVE-2018-5116, CVE-2018-5117, CVE-2018-5118, CVE-2018-5119, CVE-2018-5121, CVE-2018-5122

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (a891c5b4-3d7a-4de9-9c71-eef3fd698c77)

Observation

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

http://www.vuxml.org/freebsd/a891c5b4-3d7a-4de9-9c71-eef3fd698c77.html

Affected packages:
firefox < 58.0_1,1
waterfox < 56.0.3_4
seamonkey < 2.49.2
linux-seamonkey < 2.49.2
firefox-esr < 52.6.0_1,1
linux-firefox < 52.6.0,2
libxul < 52.6.0
thunderbird < 52.6.0
linux-thunderbird < 52.6.0

186056 - Ubuntu Linux 12.04 USN-3536-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000001

Description

The scan detected that the host is missing the following update:
USN-3536-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004232.html

Ubuntu 12.04

libc6_2.15-0ubuntu10.21

186065 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3535-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
USN-3535-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004230.html

Ubuntu 16.04

bind9_9.10.3.dfsg.P4-8ubuntu1.10

Ubuntu 14.04

bind9_9.9.5.dfsg-3ubuntu0.17

Ubuntu 17.10

bind9_9.10.3.dfsg.P4-12.6ubuntu1.1

193191 - Fedora Linux 26 FEDORA-2018-8dc60a4feb Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5332, CVE-2018-5333, CVE-2018-5344

Description

The scan detected that the host is missing the following update:
FEDORA-2018-8dc60a4feb

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/2018/1/?count=200&page=2

Fedora Core 26

kernel-4.14.14-200.fc26

193192 - Fedora Linux 27 FEDORA-2018-2299cfb708 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15111, CVE-2017-15112

Description

The scan detected that the host is missing the following update:
FEDORA-2018-2299cfb708

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/2018/1/?count=200&page=3

Fedora Core 27

keycloak-httpd-client-install-0.8-1.fc27

193199 - Fedora Linux 27 FEDORA-2018-d2b135d345 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-2018-d2b135d345

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/2018/1/?count=200&page=3

Fedora Core 27

rootsh-1.5.3-17.fc27

193200 - Fedora Linux 26 FEDORA-2018-e1539d9bc6 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-2018-e1539d9bc6

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/2018/1/?count=200&page=3

Fedora Core 26

icecat-52.5.3-2.fc26

193202 - Fedora Linux 26 FEDORA-2018-0d6a80f496 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15365

Description

The scan detected that the host is missing the following update:
FEDORA-2018-0d6a80f496

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/2018/1/?count=200&page=2

Fedora Core 26

mariadb-10.1.30-1.fc26

193203 - Fedora Linux 27 FEDORA-2018-97bdb9ba32 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3145

Description

The scan detected that the host is missing the following update:
FEDORA-2018-97bdb9ba32

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/2018/1/?count=200&page=1

Fedora Core 27

bind-9.11.2-1.P1.fc27
dnsperf-2.1.0.0-11.fc27

bind-dyndb-ldap-11.1-8.fc27

193204 - Fedora Linux 26 FEDORA-2018-94665e91e0 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-2018-94665e91e0

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/2018/1/?count=200&page=3

Fedora Core 26

rootsh-1.5.3-17.fc26

193205 - Fedora Linux 27 FEDORA-2018-da4263f065 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6003

Description

The scan detected that the host is missing the following update:
FEDORA-2018-da4263f065

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/2018/1/?count=200&page=1

Fedora Core 27

libtasn1-4.13-1.fc27

193206 - Fedora Linux 27 FEDORA-2018-d1e263e68e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5702

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d1e263e68e

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/2018/1/?count=200&page=3

Fedora Core 27

transmission-2.92-11.fc27

193207 - Fedora Linux 27 FEDORA-2018-6349371aa1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13194

Description

The scan detected that the host is missing the following update:
FEDORA-2018-6349371aa1

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/2018/1/?count=200&page=1

Fedora Core 27

libvpx-1.6.1-5.fc27

193208 - Fedora Linux 27 FEDORA-2018-16a76da6cc 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-2018-16a76da6cc

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/2018/1/?count=200&page=3

Fedora Core 27

icecat-52.5.3-2.fc27

193210 - Fedora Linux 27 FEDORA-2018-262eb7c289 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5332, CVE-2018-5333, CVE-2018-5344

Description

The scan detected that the host is missing the following update:
FEDORA-2018-262eb7c289

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/2018/1/?count=200&page=1

Fedora Core 27

kernel-4.14.14-300.fc27

22976 - (VMSA-2018-0003) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: Low

CVE: CVE-2017-4945, CVE-2017-4948

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components.
Successful exploitation could allow an attacker to disclose sensitive information or may cause a Denial of Service.

135191 - Oracle Solaris 11.3.27.4.0 Update Is Not Installed (CVE-2018-2560)

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

Risk Level: Low

CVE: CVE-2018-2560

Description

The scan detected that the host is missing the following update:
SRU 11.3.27.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2336753.1&_adf.ctrl-state=m6bdfs8xc_4&_afrLoop=335357878787577

135192 - Oracle Solaris 11.3.27.4.0 Update Is Not Installed (CVE-2018-2577)

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

Risk Level: Low

CVE: CVE-2018-2577

Description

The scan detected that the host is missing the following update:
SRU 11.3.27.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2336753.1&_adf.ctrl-state=m6bdfs8xc_4&_afrLoop=335357878787577

135193 - Oracle Solaris 11.3.27.4.0 Update Is Not Installed (CVE-2018-2578)

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

Risk Level: Low

CVE: CVE-2018-2578

Description

The scan detected that the host is missing the following update:
SRU 11.3.27.4.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2336753.1&_adf.ctrl-state=m6bdfs8xc_4&_afrLoop=335357878787577

135194 - Oracle Solaris 11.1.12.5.0 Update Is Not Installed (CVE-2018-2710)

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

Risk Level: Low

CVE: CVE-2018-2710

Description

The scan detected that the host is missing the following update:
SRU 11.1.12.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2336753.1&_adf.ctrl-state=m6bdfs8xc_4&_afrLoop=335357878787577

135195 - Oracle Solaris 11.1.12.5.0 Update Is Not Installed (CVE-2018-2717)

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

Risk Level: Low

CVE: CVE-2018-2717

Description

The scan detected that the host is missing the following update:
SRU 11.1.12.5.0

Observation

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

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2336753.1&_adf.ctrl-state=m6bdfs8xc_4&_afrLoop=335357878787577

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.

22952 - (MSPT-Jan2018) Microsoft Office Email Parsing Remote Code Execution (CVE-2018-0793)

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

Risk Level: High

CVE: CVE-2018-0793

Update Details

Recommendation is updated

88907 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-008-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5205, CVE-2018-5206, CVE-2018-5207, CVE-2018-5208

Update Details

Risk is updated

93358 - Mandriva Linux MBS1 MDVSA-2014-145 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4914

Update Details

Risk is updated

130977 - Debian Linux 8.0, 9.0 DSA-4070-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17843, CVE-2017-17844, CVE-2017-17845, CVE-2017-17846, CVE-2017-17847, CVE-2017-17848

Update Details

Risk is updated

130991 - Debian Linux 8.0, 9.0 DSA-4084-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000421

Update Details

Risk is updated

139063 - Oracle Solaris 11.3.15.4.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2015-8325, CVE-2016-0762, CVE-2016-3739, CVE-2016-5018, CVE-2016-5290, CVE-2016-5291, CVE-2016-5296, CVE-2016-5297, CVE-2016-5384, CVE-2016-5407, CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-6210, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797, CVE-2016-7076, CVE-2016-7167, CVE-2016-7942, CVE-2016-7943, CVE-2016-7944, CVE-2016-7945, CVE-2016-7946, CVE-2016-7947, CVE-2016-7948, CVE-2016-7949, CVE-2016-7950, CVE-2016-7951, CVE-2016-7952, CVE-2016-7953, CVE-2016-8330, CVE-2016-8858, CVE-2016-8864, CVE-2016-9064, CVE-2016-9066, CVE-2016-9074, CVE-2016-9189, CVE-2016-9190, CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633, CVE-2017-3276, CVE-2018-2717

Update Details

CVE is updated

170362 - Amazon Linux AMI ALAS-2014-394 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4914

Update Details

Risk is updated

182567 - FreeBSD irssi Multiple Vulnerabilities (a3764767-f31e-11e7-95f2-005056925db4)

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

Risk Level: High

CVE: CVE-2018-5205, CVE-2018-5206, CVE-2018-5207, CVE-2018-5208

Update Details

Risk is updated

182568 - FreeBSD awstats Remote Code Execution (4055aee5-f4c6-11e7-95f2-005056925db4)

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

Risk Level: High

CVE: CVE-2017-1000501

Update Details

Risk is updated

186031 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3518-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000501

Update Details

Risk is updated

186043 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3527-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5205, CVE-2018-5206, CVE-2018-5207, CVE-2018-5208

Update Details

Risk is updated

188080 - Fedora Linux 19 FEDORA-2014-8309 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4914

Update Details

Risk is updated

188087 - Fedora Linux 20 FEDORA-2014-8308 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4914

Update Details

Risk is updated

193177 - Fedora Linux 26 FEDORA-2018-6cd2e0e292 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000421

Update Details

Risk is updated

22894 - (VMSA-2017-0021) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4933, CVE-2017-4941

Update Details

Risk is updated

22904 - (VMSA-2017-0021) VMware ESXi Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4933, CVE-2017-4940, CVE-2017-4941

Update Details

Risk is updated

22905 - (VMSA-2017-0021) VMware ESXi Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4933, CVE-2017-4940, CVE-2017-4941

Update Details

Risk is updated

22977 - (VMSA-2017-0021) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4933, CVE-2017-4941

Update Details

Risk is updated

22978 - (VMSA-2017-0021) VMware Workstation Player Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4933, CVE-2017-4941

Update Details

Risk is updated

33145 - Oracle Solaris 150401-59 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5544, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122, CVE-2018-2710, CVE-2018-2717

Update Details

CVE is updated

130978 - Debian Linux 8.0, 9.0 DSA-4069-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17476

Update Details

Risk is updated

130997 - Debian Linux 8.0, 9.0 DSA-4088-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000422

Update Details

Risk is updated

182275 - FreeBSD chromium Multiple Vulnerabilities (4b9ca994-e3d9-11e6-813d-e8e0b747a45a)

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

Risk Level: Medium

CVE: CVE-2017-5006, CVE-2017-5007, CVE-2017-5008, CVE-2017-5009, CVE-2017-5010, CVE-2017-5011, CVE-2017-5012, CVE-2017-5013, CVE-2017-5014, CVE-2017-5015, CVE-2017-5016, CVE-2017-5017, CVE-2017-5018, CVE-2017-5019

Update Details

CVE is updated

193156 - Fedora Linux 27 FEDORA-2017-4c30d86843 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17866

Update Details

Risk is updated

193183 - Fedora Linux 26 FEDORA-2017-d1213cef30 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17866

Update Details

Risk is updated

12824 - HTTP Server Prone To Slow Denial Of Service Attack

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

Risk Level: Medium

CVE: CVE-2007-6750, CVE-2012-5568

Update Details

FASLScript is updated

139025 - Oracle Solaris 11.1.12.5.0 Update Is Not Installed (Third Party Components)

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

Risk Level: Medium

CVE: CVE-2011-2391, CVE-2013-4124, CVE-2013-4238, CVE-2013-5861, CVE-2013-5866, CVE-2018-2710

Update Details

CVE is updated

143868 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1249-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8119

Update Details

Risk is updated

144237 - SuSE SLES 11 SP3, 11 SP4, SLED 11 SP3, 11 SP4 SUSE-SU-2015:1792-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8119

Update Details

Risk is updated

146182 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3421-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11424

Update Details

Risk is updated CVE is updated

182561 - FreeBSD asterisk Crash In PJSIP Resource When Missing A Contact Header (2a3bc6ac-e7c6-11e7-a90b-001999f8d30b)

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

Risk Level: Medium

CVE: CVE-2017-17850

Update Details

Risk is updated

189290 - Fedora Linux 22 FEDORA-2015-5885 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8119

Update Details

Risk is updated

189326 - Fedora Linux 20 FEDORA-2015-5910 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8119

Update Details

Risk is updated

189327 - Fedora Linux 21 FEDORA-2015-5872 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8119

Update Details

Risk is updated

193145 - Fedora Linux 27 FEDORA-2017-41242dfe10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17850

Update Details

Risk is updated

33162 - Oracle Solaris 150400-59 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122, CVE-2018-2710, CVE-2018-2717

Update Details

CVE is updated

193041 - Fedora Linux 27 FEDORA-2017-97b730736f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16818

Update Details

Risk is updated

193154 - Fedora Linux 26 FEDORA-2018-20ba39cba9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000456

Update Details

Risk is updated

193159 - Fedora Linux 27 FEDORA-2018-048468d7a8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000456

Update Details

Risk is updated

182506 - FreeBSD chromium Stack Overflow In V8 (3cd46257-bbc5-11e7-a3bc-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-15396, CVE-2017-15406

Update Details

CVE is updated FASLScript is updated

22975 - (VMSA-2018-0003) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: Low

CVE: CVE-2017-4945, CVE-2017-4948

Update Details

Risk is updated

182549 - FreeBSD rubygem-passenger Arbitrary File Read Vulnerability (8cf25a29-e063-11e7-9b2c-001e672571bc)

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

Risk Level: Low

CVE: CVE-2017-16355

Update Details

Risk is updated

70088 - ibm.fasl3.inc

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

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.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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

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

Copyright 2018 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates