2018-MAY-24
FSL version 7.6.25

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

23581 - (JSA10844) Juniper Junos OS Kernel Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-0016

Description

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

Observation

Juniper Junos is an operating system used in Juniper device.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw lies in junos kernel. Successful exploitation could allow an attacker to cause a denial of service condition or lead to remote code execution.

23599 - Google Chrome Multiple Vulnerabilities Prior To 66.0.3359.170

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

Risk Level: High

CVE: CVE-2018-6120, CVE-2018-6121, CVE-2018-6122

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to escalate privileges or cause a buffer overflow.

23600 - Google Chrome Multiple Vulnerabilities Prior To 66.0.3359.170

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-6120, CVE-2018-6121, CVE-2018-6122

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to escalate privileges or cause a buffer overflow.

23614 - (HPESBGN03732) HPE Data Protector Multiple Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2017-5807, CVE-2017-5808, CVE-2017-5809

Description

Multiple vulnerabilities are present in some versions of HP Data Protector.

Observation

HP Data Protector automates high performance backups and recovery.

Multiple vulnerabilities are present in some versions of HP Data Protector. These flaws occur due to indeterminate issues. Successful exploitation could allow an attacker to execute arbitrary code or disclose sensitive information.

23605 - (MSPT-May2018) Microsoft Excel Memory Remote Code Execution (CVE-2018-8147)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-8147

Description

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

Observation

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

The flaw lies in the Memory error. 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.

23606 - (MSPT-May2018) Microsoft Excel Memory Remote Code Execution (CVE-2018-8162)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-8162

Description

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

Observation

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

The flaw lies in the Memory error. 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.

23607 - (MSPT-May2018) Microsoft PowerPoint Remote Code Execution Vulnerability (CVE-2018-8176)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-8176

Description

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

Observation

Microsoft PowerPoint is a widely-used presentation software.

A vulnerability in some versions of Microsoft PowerPoint could lead to remote code execution. The flaw lies in how Microsoft PowerPoint handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. Exploitation requires the user to open a maliciously crafted document.

160398 - CentOS 6 CESA-2018-1414 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158, CVE-2018-5159, CVE-2018-5168, CVE-2018-5178, CVE-2018-5183

Description

The scan detected that the host is missing the following update:
CESA-2018-1414

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022832.html

CentOS 6
x86_64
firefox-52.8.0-1.el6.centos

i686
firefox-52.8.0-1.el6.centos

193714 - Fedora Linux 27 FEDORA-2018-98684f429b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15591, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-15597, CVE-2017-17044, CVE-2017-17045, CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566, CVE-2018-10981, CVE-2018-10982, CVE-2018-7540, CVE-2018-7541, CVE-2018-7542, CVE-2018-8897

Description

The scan detected that the host is missing the following update:
FEDORA-2018-98684f429b

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/2018/5/?count=200&page=3

Fedora Core 27

xen-4.9.2-3.fc27

23585 - Cisco Adaptive Security Appliance Flow Creation Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-0228

Description

A denial of service vulnerability is present in some versions of Cisco Adaptive Security Appliance Software.

Observation

Cisco Adaptive Security Appliance Software is the operating system used in Cisco ASA device.

A denial of service vulnerability is present in some versions of Cisco Adaptive Security Appliance Software. The flaw is due to improper handling of an internal software lock. Successful exploitation could allow an attacker to cause a denial of service condition.

23597 - Foxit Reader Multiple Safe Reading Mode Vulnerabilities (2017-08-22)

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

Risk Level: High

CVE: CVE-2017-10951, CVE-2017-10952

Description

Multiple vulnerabilities are present in some versions of Foxit Reader.

Observation

Foxit Reader is a free PDF viewer.

Multiple vulnerabilities are present in some versions of Foxit Reader. The flaw lies in the Safe Reading Mode feature. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

23601 - (APSB18-12) Creative Cloud Desktop Application Vulnerability

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

Risk Level: High

CVE: CVE-2018-4873, CVE-2018-4991, CVE-2018-4992

Description

Multiple vulnerabilities are present in some versions of Adobe Creative Cloud Desktop Application.

Observation

Adobe Creative Cloud Desktop Application is the desktop client used to access Adobe Creative Cloud.

Multiple vulnerabilities are present in some versions of Adobe Creative Cloud Desktop Application. The flaws lie in multiple components. Successful exploitation could allow an attacker to gain elevated privileges or bypass security restrictions to do unauthorized actions.

23602 - (APSB18-12) Creative Cloud Desktop Application Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-4873, CVE-2018-4991, CVE-2018-4992

Description

Multiple vulnerabilities are present in some versions of Adobe Creative Cloud Desktop Application.

Observation

Adobe Creative Cloud Desktop Application is the desktop client used to access Adobe Creative Cloud.

Multiple vulnerabilities are present in some versions of Adobe Creative Cloud Desktop Application. The flaws lie in multiple components. Successful exploitation could allow an attacker to gain elevated privileges or bypass security restrictions to do unauthorized actions.

23610 - (HPESBUX03706) HP-UX NTP Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311

Description

Multiple vulnerabilities are present in some versions of HP-UX.

Observation

HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP-UX. The flaws lie in ntpd. Successful exploitation could allow an attacker to bypass access restriction, make an unauthorized modification or cause a denial of service.

96053 - Red Hat Enterprise Linux RHSA-2018-1649 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1649

Observation

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

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

RHEL7D
x86_64
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-1.8.0.171-8.b10.el7_5

java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el7_5

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-zip-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el7_5

RHEL7S
noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-zip-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el7_5

x86_64
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el7_5

RHEL7WS
x86_64
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el7_5

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-zip-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el7_5

96054 - Red Hat Enterprise Linux RHSA-2018-1629 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1629

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00080.html

RHEL7D
x86_64
kernel-debug-3.10.0-862.3.2.el7
kernel-3.10.0-862.3.2.el7
python-perf-debuginfo-3.10.0-862.3.2.el7
kernel-tools-libs-devel-3.10.0-862.3.2.el7
kernel-tools-debuginfo-3.10.0-862.3.2.el7
perf-debuginfo-3.10.0-862.3.2.el7
kernel-debuginfo-common-x86_64-3.10.0-862.3.2.el7
kernel-debug-devel-3.10.0-862.3.2.el7
kernel-devel-3.10.0-862.3.2.el7
kernel-tools-libs-3.10.0-862.3.2.el7
kernel-debuginfo-3.10.0-862.3.2.el7
perf-3.10.0-862.3.2.el7
kernel-tools-3.10.0-862.3.2.el7
python-perf-3.10.0-862.3.2.el7
kernel-debug-debuginfo-3.10.0-862.3.2.el7
kernel-headers-3.10.0-862.3.2.el7

noarch
kernel-abi-whitelists-3.10.0-862.3.2.el7
kernel-doc-3.10.0-862.3.2.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-862.3.2.el7
kernel-doc-3.10.0-862.3.2.el7

x86_64
kernel-debug-3.10.0-862.3.2.el7
kernel-3.10.0-862.3.2.el7
python-perf-debuginfo-3.10.0-862.3.2.el7
kernel-tools-libs-devel-3.10.0-862.3.2.el7
kernel-tools-debuginfo-3.10.0-862.3.2.el7
perf-debuginfo-3.10.0-862.3.2.el7
kernel-debuginfo-common-x86_64-3.10.0-862.3.2.el7
kernel-debug-devel-3.10.0-862.3.2.el7
kernel-devel-3.10.0-862.3.2.el7
kernel-tools-libs-3.10.0-862.3.2.el7
kernel-debuginfo-3.10.0-862.3.2.el7
perf-3.10.0-862.3.2.el7
kernel-tools-3.10.0-862.3.2.el7
python-perf-3.10.0-862.3.2.el7

kernel-debug-debuginfo-3.10.0-862.3.2.el7
kernel-headers-3.10.0-862.3.2.el7

RHEL7WS
x86_64
kernel-debug-3.10.0-862.3.2.el7
kernel-3.10.0-862.3.2.el7
python-perf-debuginfo-3.10.0-862.3.2.el7
kernel-tools-libs-devel-3.10.0-862.3.2.el7
kernel-tools-debuginfo-3.10.0-862.3.2.el7
perf-debuginfo-3.10.0-862.3.2.el7
kernel-debuginfo-common-x86_64-3.10.0-862.3.2.el7
kernel-debug-devel-3.10.0-862.3.2.el7
kernel-devel-3.10.0-862.3.2.el7
kernel-tools-libs-3.10.0-862.3.2.el7
kernel-debuginfo-3.10.0-862.3.2.el7
perf-3.10.0-862.3.2.el7
kernel-tools-3.10.0-862.3.2.el7
python-perf-3.10.0-862.3.2.el7
kernel-debug-debuginfo-3.10.0-862.3.2.el7
kernel-headers-3.10.0-862.3.2.el7

noarch
kernel-abi-whitelists-3.10.0-862.3.2.el7
kernel-doc-3.10.0-862.3.2.el7

131110 - Debian Linux 9.0 DSA-4206-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0920, CVE-2018-8971

Description

The scan detected that the host is missing the following update:
DSA-4206-1

Observation

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

http://www.debian.org/security/2018/dsa-4206

Debian 9.0
all
gitlab_8.13.11+dfsg1-8+deb9u2

132457 - Oracle VM OVMSA-2018-0219 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0219

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-May/000855.html

OVM3.4
x86_64
qemu-img-0.12.1.2-2.503.el6_9.6

141980 - Red Hat Enterprise Linux RHSA-2018-1667 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1667

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00098.html

RHEL6_7S
i386
libvirt-0.10.2-54.el6_7.8
libvirt-devel-0.10.2-54.el6_7.8
libvirt-debuginfo-0.10.2-54.el6_7.8
libvirt-client-0.10.2-54.el6_7.8
libvirt-python-0.10.2-54.el6_7.8

x86_64
libvirt-lock-sanlock-0.10.2-54.el6_7.8
libvirt-debuginfo-0.10.2-54.el6_7.8
libvirt-devel-0.10.2-54.el6_7.8
libvirt-python-0.10.2-54.el6_7.8
libvirt-client-0.10.2-54.el6_7.8
libvirt-0.10.2-54.el6_7.8

141981 - Red Hat Enterprise Linux RHSA-2018-1647 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1647

Observation

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

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

RHEL6D
i386
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el6_9

x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el6_9

RHEL6S
i386
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el6_9

x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el6_9

RHEL6WS
x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9

i386
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9

141982 - Red Hat Enterprise Linux RHSA-2018-1656 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1656

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00096.html

RHEL6_4S
x86_64
qemu-guest-agent-win32-0.12.1.2-2.355.el6_4.11
qemu-guest-agent-0.12.1.2-2.355.el6_4.11
qemu-kvm-debuginfo-0.12.1.2-2.355.el6_4.11
qemu-kvm-0.12.1.2-2.355.el6_4.11
qemu-img-0.12.1.2-2.355.el6_4.11
qemu-kvm-tools-0.12.1.2-2.355.el6_4.11

141983 - Red Hat Enterprise Linux RHSA-2018-1636 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1636

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00103.html

RHEL7_3S
noarch
kernel-doc-3.10.0-514.48.5.el7
kernel-abi-whitelists-3.10.0-514.48.5.el7

x86_64
python-perf-3.10.0-514.48.5.el7
kernel-tools-debuginfo-3.10.0-514.48.5.el7
kernel-3.10.0-514.48.5.el7
perf-debuginfo-3.10.0-514.48.5.el7
kernel-devel-3.10.0-514.48.5.el7
python-perf-debuginfo-3.10.0-514.48.5.el7
kernel-debuginfo-common-x86_64-3.10.0-514.48.5.el7
kernel-tools-libs-3.10.0-514.48.5.el7
perf-3.10.0-514.48.5.el7
kernel-debug-3.10.0-514.48.5.el7
kernel-debug-debuginfo-3.10.0-514.48.5.el7
kernel-headers-3.10.0-514.48.5.el7
kernel-tools-libs-devel-3.10.0-514.48.5.el7
kernel-debuginfo-3.10.0-514.48.5.el7
kernel-tools-3.10.0-514.48.5.el7
kernel-debug-devel-3.10.0-514.48.5.el7

141984 - Red Hat Enterprise Linux RHSA-2018-1658 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1658

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00083.html

RHEL6_6S
x86_64
qemu-kvm-debuginfo-0.12.1.2-2.448.el6_6.6
qemu-kvm-0.12.1.2-2.448.el6_6.6
qemu-guest-agent-0.12.1.2-2.448.el6_6.6
qemu-img-0.12.1.2-2.448.el6_6.6
qemu-kvm-tools-0.12.1.2-2.448.el6_6.6

141985 - Red Hat Enterprise Linux RHSA-2018-1648 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1648

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00085.html

RHEL7D
x86_64
java-1.7.0-openjdk-headless-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-accessibility-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el7_5

noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el7_5

RHEL7S
noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el7_5

x86_64
java-1.7.0-openjdk-headless-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-accessibility-1.7.0.181-2.6.14.8.el7_5

java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el7_5

RHEL7WS
x86_64
java-1.7.0-openjdk-headless-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-accessibility-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el7_5

noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el7_5

141986 - Red Hat Enterprise Linux RHSA-2018-1664 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1664

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00099.html

RHEL6_4S
x86_64
libvirt-debuginfo-0.10.2-18.el6_4.17
libvirt-python-0.10.2-18.el6_4.17
libvirt-lock-sanlock-0.10.2-18.el6_4.17
libvirt-0.10.2-18.el6_4.17
libvirt-client-0.10.2-18.el6_4.17
libvirt-devel-0.10.2-18.el6_4.17

141987 - Red Hat Enterprise Linux RHSA-2018-1657 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1657

Observation

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

For more information see:

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

RHEL6_5S
x86_64
qemu-kvm-tools-0.12.1.2-2.415.el6_5.18
qemu-img-0.12.1.2-2.415.el6_5.18
qemu-kvm-debuginfo-0.12.1.2-2.415.el6_5.18
qemu-guest-agent-0.12.1.2-2.415.el6_5.18
qemu-kvm-0.12.1.2-2.415.el6_5.18

141988 - Red Hat Enterprise Linux RHSA-2018-1662 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1662

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00095.html

RHEL7_3S
x86_64
qemu-kvm-1.5.3-126.el7_3.14
qemu-kvm-debuginfo-1.5.3-126.el7_3.14
qemu-img-1.5.3-126.el7_3.14
qemu-kvm-common-1.5.3-126.el7_3.14
qemu-kvm-tools-1.5.3-126.el7_3.14

141989 - Red Hat Enterprise Linux RHSA-2018-1632 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1632

Observation

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

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

RHEL7D
x86_64
libvirt-daemon-driver-storage-gluster-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-iscsi-3.9.0-14.el7_5.5

libvirt-daemon-config-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-3.9.0-14.el7_5.5
libvirt-lock-sanlock-3.9.0-14.el7_5.5
libvirt-client-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-core-3.9.0-14.el7_5.5
libvirt-libs-3.9.0-14.el7_5.5
libvirt-daemon-driver-secret-3.9.0-14.el7_5.5
libvirt-login-shell-3.9.0-14.el7_5.5
libvirt-debuginfo-3.9.0-14.el7_5.5
libvirt-daemon-3.9.0-14.el7_5.5
libvirt-daemon-driver-nodedev-3.9.0-14.el7_5.5
libvirt-daemon-config-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-rbd-3.9.0-14.el7_5.5
libvirt-3.9.0-14.el7_5.5
libvirt-daemon-driver-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-logical-3.9.0-14.el7_5.5
libvirt-daemon-kvm-3.9.0-14.el7_5.5
libvirt-nss-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-disk-3.9.0-14.el7_5.5
libvirt-admin-3.9.0-14.el7_5.5
libvirt-devel-3.9.0-14.el7_5.5
libvirt-daemon-driver-qemu-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-mpath-3.9.0-14.el7_5.5
libvirt-daemon-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-scsi-3.9.0-14.el7_5.5
libvirt-daemon-driver-interface-3.9.0-14.el7_5.5
libvirt-docs-3.9.0-14.el7_5.5

RHEL7S
x86_64
libvirt-daemon-driver-storage-gluster-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-iscsi-3.9.0-14.el7_5.5
libvirt-daemon-config-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-3.9.0-14.el7_5.5
libvirt-lock-sanlock-3.9.0-14.el7_5.5
libvirt-client-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-core-3.9.0-14.el7_5.5
libvirt-libs-3.9.0-14.el7_5.5
libvirt-daemon-driver-secret-3.9.0-14.el7_5.5
libvirt-login-shell-3.9.0-14.el7_5.5
libvirt-debuginfo-3.9.0-14.el7_5.5
libvirt-daemon-3.9.0-14.el7_5.5
libvirt-daemon-driver-nodedev-3.9.0-14.el7_5.5
libvirt-daemon-config-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-rbd-3.9.0-14.el7_5.5
libvirt-3.9.0-14.el7_5.5
libvirt-daemon-driver-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-logical-3.9.0-14.el7_5.5
libvirt-daemon-kvm-3.9.0-14.el7_5.5
libvirt-nss-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-disk-3.9.0-14.el7_5.5
libvirt-admin-3.9.0-14.el7_5.5
libvirt-devel-3.9.0-14.el7_5.5
libvirt-daemon-driver-qemu-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-mpath-3.9.0-14.el7_5.5
libvirt-daemon-lxc-3.9.0-14.el7_5.5

libvirt-daemon-driver-storage-scsi-3.9.0-14.el7_5.5
libvirt-daemon-driver-interface-3.9.0-14.el7_5.5
libvirt-docs-3.9.0-14.el7_5.5

RHEL7WS
x86_64
libvirt-daemon-driver-storage-gluster-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-iscsi-3.9.0-14.el7_5.5
libvirt-daemon-config-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-3.9.0-14.el7_5.5
libvirt-lock-sanlock-3.9.0-14.el7_5.5
libvirt-client-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-core-3.9.0-14.el7_5.5
libvirt-libs-3.9.0-14.el7_5.5
libvirt-daemon-driver-secret-3.9.0-14.el7_5.5
libvirt-login-shell-3.9.0-14.el7_5.5
libvirt-debuginfo-3.9.0-14.el7_5.5
libvirt-daemon-3.9.0-14.el7_5.5
libvirt-daemon-driver-nodedev-3.9.0-14.el7_5.5
libvirt-daemon-config-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-rbd-3.9.0-14.el7_5.5
libvirt-3.9.0-14.el7_5.5
libvirt-daemon-driver-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-logical-3.9.0-14.el7_5.5
libvirt-daemon-kvm-3.9.0-14.el7_5.5
libvirt-nss-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-disk-3.9.0-14.el7_5.5
libvirt-admin-3.9.0-14.el7_5.5
libvirt-devel-3.9.0-14.el7_5.5
libvirt-daemon-driver-qemu-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-mpath-3.9.0-14.el7_5.5
libvirt-daemon-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-scsi-3.9.0-14.el7_5.5
libvirt-daemon-driver-interface-3.9.0-14.el7_5.5
libvirt-docs-3.9.0-14.el7_5.5

141990 - Red Hat Enterprise Linux RHSA-2018-1666 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1666

Observation

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

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

RHEL6_6S
x86_64
libvirt-lock-sanlock-0.10.2-46.el6_6.8
libvirt-client-0.10.2-46.el6_6.8

libvirt-python-0.10.2-46.el6_6.8
libvirt-devel-0.10.2-46.el6_6.8
libvirt-debuginfo-0.10.2-46.el6_6.8
libvirt-0.10.2-46.el6_6.8

141991 - Red Hat Enterprise Linux RHSA-2018-1651 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1651

Observation

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

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

RHEL6D
i386
kernel-debuginfo-2.6.32-696.30.1.el6
kernel-headers-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
python-perf-debuginfo-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6
kernel-debug-debuginfo-2.6.32-696.30.1.el6
perf-debuginfo-2.6.32-696.30.1.el6
kernel-debuginfo-common-i686-2.6.32-696.30.1.el6

noarch
kernel-abi-whitelists-2.6.32-696.30.1.el6
kernel-doc-2.6.32-696.30.1.el6
kernel-firmware-2.6.32-696.30.1.el6

x86_64
kernel-debuginfo-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.30.1.el6
kernel-debuginfo-common-i686-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-debuginfo-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-headers-2.6.32-696.30.1.el6
python-perf-debuginfo-2.6.32-696.30.1.el6
kernel-debug-debuginfo-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6

RHEL6S
i386

kernel-debuginfo-2.6.32-696.30.1.el6
kernel-headers-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
python-perf-debuginfo-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6
kernel-debug-debuginfo-2.6.32-696.30.1.el6
perf-debuginfo-2.6.32-696.30.1.el6
kernel-debuginfo-common-i686-2.6.32-696.30.1.el6

noarch
kernel-abi-whitelists-2.6.32-696.30.1.el6
kernel-doc-2.6.32-696.30.1.el6
kernel-firmware-2.6.32-696.30.1.el6

x86_64
kernel-debuginfo-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.30.1.el6
kernel-debuginfo-common-i686-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-debuginfo-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-headers-2.6.32-696.30.1.el6
python-perf-debuginfo-2.6.32-696.30.1.el6
kernel-debug-debuginfo-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6

RHEL6WS
i386
kernel-debuginfo-2.6.32-696.30.1.el6
kernel-headers-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
python-perf-debuginfo-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6
kernel-debug-debuginfo-2.6.32-696.30.1.el6
perf-debuginfo-2.6.32-696.30.1.el6
kernel-debuginfo-common-i686-2.6.32-696.30.1.el6

noarch
kernel-abi-whitelists-2.6.32-696.30.1.el6
kernel-doc-2.6.32-696.30.1.el6
kernel-firmware-2.6.32-696.30.1.el6

x86_64
kernel-debuginfo-2.6.32-696.30.1.el6
kernel-headers-2.6.32-696.30.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6

python-perf-debuginfo-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6
kernel-debug-debuginfo-2.6.32-696.30.1.el6
perf-debuginfo-2.6.32-696.30.1.el6
kernel-debuginfo-common-i686-2.6.32-696.30.1.el6

141992 - Red Hat Enterprise Linux RHSA-2018-1665 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1665

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00090.html

RHEL6_5S
x86_64
libvirt-0.10.2-29.el6_5.16
libvirt-devel-0.10.2-29.el6_5.16
libvirt-lock-sanlock-0.10.2-29.el6_5.16
libvirt-python-0.10.2-29.el6_5.16
libvirt-debuginfo-0.10.2-29.el6_5.16
libvirt-client-0.10.2-29.el6_5.16

141993 - Red Hat Enterprise Linux RHSA-2018-1660 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1660

Observation

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

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

RHEL6D
x86_64
qemu-img-0.12.1.2-2.503.el6_9.6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.6
qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-0.12.1.2-2.503.el6_9.6
qemu-kvm-tools-0.12.1.2-2.503.el6_9.6

i386

qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.6

RHEL6S
i386
qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.6

x86_64
qemu-img-0.12.1.2-2.503.el6_9.6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.6
qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-0.12.1.2-2.503.el6_9.6
qemu-kvm-tools-0.12.1.2-2.503.el6_9.6

RHEL6WS
x86_64
qemu-img-0.12.1.2-2.503.el6_9.6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.6
qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-0.12.1.2-2.503.el6_9.6
qemu-kvm-tools-0.12.1.2-2.503.el6_9.6

i386
qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.6

141994 - Red Hat Enterprise Linux RHSA-2018-1650 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1650

Observation

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

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

RHEL6D
i386
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

noarch

java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el6_9

x86_64
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

RHEL6S
i386
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el6_9

x86_64
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

RHEL6WS
x86_64
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9

i386
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9

141995 - Red Hat Enterprise Linux RHSA-2018-1653 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1653

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00082.html

RHEL7_3S
x86_64
libvirt-devel-2.0.0-10.el7_3.12
libvirt-daemon-config-network-2.0.0-10.el7_3.12
libvirt-lock-sanlock-2.0.0-10.el7_3.12
libvirt-daemon-driver-nwfilter-2.0.0-10.el7_3.12
libvirt-daemon-2.0.0-10.el7_3.12
libvirt-daemon-driver-network-2.0.0-10.el7_3.12
libvirt-2.0.0-10.el7_3.12
libvirt-daemon-config-nwfilter-2.0.0-10.el7_3.12
libvirt-daemon-driver-storage-2.0.0-10.el7_3.12
libvirt-daemon-driver-qemu-2.0.0-10.el7_3.12
libvirt-daemon-driver-secret-2.0.0-10.el7_3.12
libvirt-daemon-driver-lxc-2.0.0-10.el7_3.12
libvirt-debuginfo-2.0.0-10.el7_3.12
libvirt-daemon-lxc-2.0.0-10.el7_3.12
libvirt-nss-2.0.0-10.el7_3.12
libvirt-login-shell-2.0.0-10.el7_3.12
libvirt-daemon-driver-interface-2.0.0-10.el7_3.12
libvirt-daemon-kvm-2.0.0-10.el7_3.12
libvirt-daemon-driver-nodedev-2.0.0-10.el7_3.12
libvirt-client-2.0.0-10.el7_3.12
libvirt-docs-2.0.0-10.el7_3.12

141996 - Red Hat Enterprise Linux RHSA-2018-1633 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1633

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00093.html

RHEL7D
x86_64
qemu-kvm-debuginfo-1.5.3-156.el7_5.2
qemu-img-1.5.3-156.el7_5.2
qemu-kvm-common-1.5.3-156.el7_5.2
qemu-kvm-tools-1.5.3-156.el7_5.2
qemu-kvm-1.5.3-156.el7_5.2

RHEL7S
x86_64
qemu-kvm-debuginfo-1.5.3-156.el7_5.2
qemu-img-1.5.3-156.el7_5.2
qemu-kvm-common-1.5.3-156.el7_5.2
qemu-kvm-tools-1.5.3-156.el7_5.2
qemu-kvm-1.5.3-156.el7_5.2

RHEL7WS
x86_64
qemu-kvm-debuginfo-1.5.3-156.el7_5.2
qemu-img-1.5.3-156.el7_5.2
qemu-kvm-common-1.5.3-156.el7_5.2
qemu-kvm-tools-1.5.3-156.el7_5.2
qemu-kvm-1.5.3-156.el7_5.2

141997 - Red Hat Enterprise Linux RHSA-2018-1669 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1669

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00094.html

RHEL6D
x86_64
libvirt-debuginfo-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2
libvirt-lock-sanlock-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-devel-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2

i386
libvirt-devel-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2
libvirt-debuginfo-0.10.2-62.el6_9.2

RHEL6S
i386

libvirt-devel-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2
libvirt-debuginfo-0.10.2-62.el6_9.2

x86_64
libvirt-debuginfo-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2
libvirt-lock-sanlock-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-devel-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2

RHEL6WS
x86_64
libvirt-devel-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2
libvirt-debuginfo-0.10.2-62.el6_9.2

i386
libvirt-devel-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2
libvirt-debuginfo-0.10.2-62.el6_9.2

141998 - Red Hat Enterprise Linux RHSA-2018-1659 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1659

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00089.html

RHEL6_7S
i386
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.7
qemu-guest-agent-0.12.1.2-2.479.el6_7.7

x86_64
qemu-guest-agent-0.12.1.2-2.479.el6_7.7
qemu-kvm-tools-0.12.1.2-2.479.el6_7.7
qemu-kvm-0.12.1.2-2.479.el6_7.7
qemu-img-0.12.1.2-2.479.el6_7.7
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.7

146681 - SuSE SLES 11 SP4 SUSE-SU-2018:1365-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1172

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1365-1

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-May/004069.html

SuSE SLES 11 SP4
i586
squid3-3.1.23-8.16.37.6.1

x86_64
squid3-3.1.23-8.16.37.6.1

146682 - SuSE Linux 42.3 openSUSE-SU-2018:1344-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000301

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1344-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00066.html

SuSE Linux 42.3
x86_64
libcurl4-debuginfo-32bit-7.37.0-36.1
curl-debugsource-7.37.0-36.1
libcurl4-debuginfo-7.37.0-36.1
libcurl4-32bit-7.37.0-36.1
libcurl4-7.37.0-36.1
curl-debuginfo-7.37.0-36.1
curl-7.37.0-36.1
libcurl-devel-7.37.0-36.1
libcurl-devel-32bit-7.37.0-36.1

i586
curl-debugsource-7.37.0-36.1
libcurl4-debuginfo-7.37.0-36.1
libcurl4-7.37.0-36.1
curl-debuginfo-7.37.0-36.1

curl-7.37.0-36.1
libcurl-devel-7.37.0-36.1

146687 - SuSE Linux 42.3 openSUSE-SU-2018:1360-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10992

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1360-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00082.html

SuSE Linux 42.3
x86_64
lilypond-2.18.2-7.3.1
lilypond-debugsource-2.18.2-7.3.1
lilypond-debuginfo-2.18.2-7.3.1

noarch
lilypond-doc-de-2.18.2-7.3.1
lilypond-doc-it-2.18.2-7.3.1
lilypond-fonts-common-2.18.2-7.3.1
lilypond-doc-es-2.18.2-7.3.1
lilypond-doc-nl-2.18.2-7.3.1
lilypond-century-schoolbook-l-fonts-2.18.2-7.3.1
lilypond-doc-ja-2.18.2-7.3.1
lilypond-emmentaler-fonts-2.18.2-7.3.1
lilypond-doc-fr-2.18.2-7.3.1
lilypond-doc-hu-2.18.2-7.3.1
lilypond-doc-zh-2.18.2-7.3.1
lilypond-doc-2.18.2-7.3.1
lilypond-doc-cs-2.18.2-7.3.1

146689 - SuSE SLES 11 SP4 SUSE-SU-2018:1309-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5156, CVE-2016-7915, CVE-2017-0861, CVE-2017-12190, CVE-2017-13166, CVE-2017-16644, CVE-2017-16911, CVE-2017-16912, CVE-2017-16913, CVE-2017-16914, CVE-2017-18203, CVE-2017-18208, CVE-2018-10087, CVE-2018-10124, CVE-2018-6927, CVE-2018-7566, CVE-2018-7757, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1309-1

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-May/004055.html

SuSE SLES 11 SP4
x86_64
kernel-rt_trace-base-3.0.101.rt130-69.24.1
kernel-rt_trace-devel-3.0.101.rt130-69.24.1
kernel-rt-devel-3.0.101.rt130-69.24.1
kernel-rt-3.0.101.rt130-69.24.1
kernel-syms-rt-3.0.101.rt130-69.24.1
kernel-rt-base-3.0.101.rt130-69.24.1
kernel-rt_trace-3.0.101.rt130-69.24.1
kernel-source-rt-3.0.101.rt130-69.24.1

146690 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:1361-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5174, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1361-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00083.html

SuSE Linux 15.0
x86_64
MozillaThunderbird-buildsymbols-52.8-lp150.3.3.2
MozillaThunderbird-debuginfo-52.8-lp150.3.3.2
MozillaThunderbird-devel-52.8-lp150.3.3.2
MozillaThunderbird-52.8-lp150.3.3.2
MozillaThunderbird-debugsource-52.8-lp150.3.3.2
MozillaThunderbird-translations-other-52.8-lp150.3.3.2
MozillaThunderbird-translations-common-52.8-lp150.3.3.2

SuSE Linux 42.3
x86_64
MozillaThunderbird-buildsymbols-52.8-63.1
MozillaThunderbird-debuginfo-52.8-63.1
MozillaThunderbird-debugsource-52.8-63.1
MozillaThunderbird-52.8-63.1
MozillaThunderbird-devel-52.8-63.1
MozillaThunderbird-translations-common-52.8-63.1
MozillaThunderbird-translations-other-52.8-63.1

146693 - SuSE Linux 42.3 openSUSE-SU-2018:1317-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10545, CVE-2018-10546, CVE-2018-10547, CVE-2018-10548

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1317-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00052.html

SuSE Linux 42.3
i586
php5-phar-5.5.14-100.1
php5-suhosin-5.5.14-100.1
php5-soap-5.5.14-100.1
php5-opcache-5.5.14-100.1
php5-zlib-debuginfo-5.5.14-100.1
php5-gd-debuginfo-5.5.14-100.1
php5-xmlreader-debuginfo-5.5.14-100.1
php5-ldap-debuginfo-5.5.14-100.1
php5-pcntl-5.5.14-100.1
php5-dom-debuginfo-5.5.14-100.1
php5-mcrypt-5.5.14-100.1
php5-sysvmsg-5.5.14-100.1
php5-mssql-5.5.14-100.1
php5-gmp-5.5.14-100.1
php5-imap-5.5.14-100.1
php5-xmlwriter-debuginfo-5.5.14-100.1
php5-pgsql-debuginfo-5.5.14-100.1
php5-enchant-5.5.14-100.1
php5-fastcgi-5.5.14-100.1
php5-pspell-debuginfo-5.5.14-100.1
php5-devel-5.5.14-100.1
php5-firebird-5.5.14-100.1
php5-zlib-5.5.14-100.1
php5-opcache-debuginfo-5.5.14-100.1
php5-phar-debuginfo-5.5.14-100.1
php5-fileinfo-5.5.14-100.1
php5-bz2-debuginfo-5.5.14-100.1
php5-fpm-5.5.14-100.1
php5-calendar-debuginfo-5.5.14-100.1
php5-json-debuginfo-5.5.14-100.1
php5-sockets-5.5.14-100.1
php5-pcntl-debuginfo-5.5.14-100.1
php5-snmp-debuginfo-5.5.14-100.1
php5-dba-debuginfo-5.5.14-100.1
php5-bcmath-debuginfo-5.5.14-100.1
php5-bcmath-5.5.14-100.1
php5-readline-5.5.14-100.1
php5-5.5.14-100.1
php5-wddx-debuginfo-5.5.14-100.1
php5-sysvmsg-debuginfo-5.5.14-100.1
php5-odbc-debuginfo-5.5.14-100.1
php5-zip-5.5.14-100.1
php5-sqlite-5.5.14-100.1
php5-xmlwriter-5.5.14-100.1
php5-ctype-5.5.14-100.1
php5-sysvshm-debuginfo-5.5.14-100.1
php5-mbstring-5.5.14-100.1
php5-gmp-debuginfo-5.5.14-100.1
php5-tidy-debuginfo-5.5.14-100.1

php5-curl-5.5.14-100.1
php5-iconv-debuginfo-5.5.14-100.1
php5-intl-5.5.14-100.1
php5-sysvsem-debuginfo-5.5.14-100.1
php5-gettext-debuginfo-5.5.14-100.1
php5-gd-5.5.14-100.1
php5-suhosin-debuginfo-5.5.14-100.1
php5-xmlrpc-debuginfo-5.5.14-100.1
php5-xsl-debuginfo-5.5.14-100.1
php5-posix-5.5.14-100.1
php5-dba-5.5.14-100.1
php5-debugsource-5.5.14-100.1
php5-json-5.5.14-100.1
php5-tokenizer-debuginfo-5.5.14-100.1
php5-mysql-5.5.14-100.1
php5-sqlite-debuginfo-5.5.14-100.1
php5-curl-debuginfo-5.5.14-100.1
php5-mssql-debuginfo-5.5.14-100.1
php5-pgsql-5.5.14-100.1
php5-shmop-debuginfo-5.5.14-100.1
php5-bz2-5.5.14-100.1
php5-pspell-5.5.14-100.1
php5-sysvshm-5.5.14-100.1
php5-mbstring-debuginfo-5.5.14-100.1
php5-sockets-debuginfo-5.5.14-100.1
php5-openssl-5.5.14-100.1
php5-enchant-debuginfo-5.5.14-100.1
php5-xmlrpc-5.5.14-100.1
php5-debuginfo-5.5.14-100.1
php5-zip-debuginfo-5.5.14-100.1
php5-readline-debuginfo-5.5.14-100.1
php5-calendar-5.5.14-100.1
php5-fastcgi-debuginfo-5.5.14-100.1
php5-exif-debuginfo-5.5.14-100.1
php5-ctype-debuginfo-5.5.14-100.1
apache2-mod_php5-debuginfo-5.5.14-100.1
php5-xmlreader-5.5.14-100.1
php5-iconv-5.5.14-100.1
php5-tokenizer-5.5.14-100.1
php5-pdo-5.5.14-100.1
php5-dom-5.5.14-100.1
php5-firebird-debuginfo-5.5.14-100.1
php5-ftp-debuginfo-5.5.14-100.1
php5-odbc-5.5.14-100.1
php5-xsl-5.5.14-100.1
php5-posix-debuginfo-5.5.14-100.1
php5-mysql-debuginfo-5.5.14-100.1
php5-gettext-5.5.14-100.1
php5-imap-debuginfo-5.5.14-100.1
php5-fileinfo-debuginfo-5.5.14-100.1
php5-soap-debuginfo-5.5.14-100.1
php5-wddx-5.5.14-100.1
php5-exif-5.5.14-100.1
apache2-mod_php5-5.5.14-100.1
php5-sysvsem-5.5.14-100.1
php5-tidy-5.5.14-100.1
php5-intl-debuginfo-5.5.14-100.1
php5-mcrypt-debuginfo-5.5.14-100.1
php5-ftp-5.5.14-100.1
php5-openssl-debuginfo-5.5.14-100.1

php5-pdo-debuginfo-5.5.14-100.1
php5-ldap-5.5.14-100.1
php5-fpm-debuginfo-5.5.14-100.1
php5-snmp-5.5.14-100.1
php5-shmop-5.5.14-100.1

noarch
php5-pear-5.5.14-100.1

x86_64
php5-phar-5.5.14-100.1
php5-suhosin-5.5.14-100.1
php5-soap-5.5.14-100.1
php5-opcache-5.5.14-100.1
php5-zlib-debuginfo-5.5.14-100.1
php5-gd-debuginfo-5.5.14-100.1
php5-xmlreader-debuginfo-5.5.14-100.1
php5-ldap-debuginfo-5.5.14-100.1
php5-pcntl-5.5.14-100.1
php5-dom-debuginfo-5.5.14-100.1
php5-mcrypt-5.5.14-100.1
php5-sysvmsg-5.5.14-100.1
php5-mssql-5.5.14-100.1
php5-gmp-5.5.14-100.1
php5-imap-5.5.14-100.1
php5-xmlwriter-debuginfo-5.5.14-100.1
php5-pgsql-debuginfo-5.5.14-100.1
php5-enchant-5.5.14-100.1
php5-fastcgi-5.5.14-100.1
php5-pspell-debuginfo-5.5.14-100.1
php5-devel-5.5.14-100.1
php5-firebird-5.5.14-100.1
php5-zlib-5.5.14-100.1
php5-opcache-debuginfo-5.5.14-100.1
php5-phar-debuginfo-5.5.14-100.1
php5-fileinfo-5.5.14-100.1
php5-bz2-debuginfo-5.5.14-100.1
php5-fpm-5.5.14-100.1
php5-calendar-debuginfo-5.5.14-100.1
php5-json-debuginfo-5.5.14-100.1
php5-sockets-5.5.14-100.1
php5-pcntl-debuginfo-5.5.14-100.1
php5-snmp-debuginfo-5.5.14-100.1
php5-dba-debuginfo-5.5.14-100.1
php5-bcmath-debuginfo-5.5.14-100.1
php5-bcmath-5.5.14-100.1
php5-readline-5.5.14-100.1
php5-5.5.14-100.1
php5-wddx-debuginfo-5.5.14-100.1
php5-sysvmsg-debuginfo-5.5.14-100.1
php5-odbc-debuginfo-5.5.14-100.1
php5-zip-5.5.14-100.1
php5-sqlite-5.5.14-100.1
php5-xmlwriter-5.5.14-100.1
php5-ctype-5.5.14-100.1
php5-sysvshm-debuginfo-5.5.14-100.1
php5-mbstring-5.5.14-100.1
php5-gmp-debuginfo-5.5.14-100.1
php5-tidy-debuginfo-5.5.14-100.1
php5-curl-5.5.14-100.1

php5-iconv-debuginfo-5.5.14-100.1
php5-intl-5.5.14-100.1
php5-sysvsem-debuginfo-5.5.14-100.1
php5-gettext-debuginfo-5.5.14-100.1
php5-gd-5.5.14-100.1
php5-suhosin-debuginfo-5.5.14-100.1
php5-xmlrpc-debuginfo-5.5.14-100.1
php5-xsl-debuginfo-5.5.14-100.1
php5-posix-5.5.14-100.1
php5-dba-5.5.14-100.1
php5-debugsource-5.5.14-100.1
php5-json-5.5.14-100.1
php5-tokenizer-debuginfo-5.5.14-100.1
php5-mysql-5.5.14-100.1
php5-sqlite-debuginfo-5.5.14-100.1
php5-curl-debuginfo-5.5.14-100.1
php5-mssql-debuginfo-5.5.14-100.1
php5-pgsql-5.5.14-100.1
php5-shmop-debuginfo-5.5.14-100.1
php5-bz2-5.5.14-100.1
php5-pspell-5.5.14-100.1
php5-sysvshm-5.5.14-100.1
php5-mbstring-debuginfo-5.5.14-100.1
php5-sockets-debuginfo-5.5.14-100.1
php5-openssl-5.5.14-100.1
php5-enchant-debuginfo-5.5.14-100.1
php5-xmlrpc-5.5.14-100.1
php5-debuginfo-5.5.14-100.1
php5-zip-debuginfo-5.5.14-100.1
php5-readline-debuginfo-5.5.14-100.1
php5-calendar-5.5.14-100.1
php5-fastcgi-debuginfo-5.5.14-100.1
php5-exif-debuginfo-5.5.14-100.1
php5-ctype-debuginfo-5.5.14-100.1
apache2-mod_php5-debuginfo-5.5.14-100.1
php5-xmlreader-5.5.14-100.1
php5-iconv-5.5.14-100.1
php5-tokenizer-5.5.14-100.1
php5-pdo-5.5.14-100.1
php5-dom-5.5.14-100.1
php5-firebird-debuginfo-5.5.14-100.1
php5-ftp-debuginfo-5.5.14-100.1
php5-odbc-5.5.14-100.1
php5-xsl-5.5.14-100.1
php5-posix-debuginfo-5.5.14-100.1
php5-mysql-debuginfo-5.5.14-100.1
php5-gettext-5.5.14-100.1
php5-imap-debuginfo-5.5.14-100.1
php5-fileinfo-debuginfo-5.5.14-100.1
php5-soap-debuginfo-5.5.14-100.1
php5-wddx-5.5.14-100.1
php5-exif-5.5.14-100.1
apache2-mod_php5-5.5.14-100.1
php5-sysvsem-5.5.14-100.1
php5-tidy-5.5.14-100.1
php5-intl-debuginfo-5.5.14-100.1
php5-mcrypt-debuginfo-5.5.14-100.1
php5-ftp-5.5.14-100.1
php5-openssl-debuginfo-5.5.14-100.1
php5-pdo-debuginfo-5.5.14-100.1

php5-ldap-5.5.14-100.1
php5-fpm-debuginfo-5.5.14-100.1
php5-snmp-5.5.14-100.1
php5-shmop-5.5.14-100.1

146696 - SuSE Linux 42.3 openSUSE-SU-2018:1330-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17688, CVE-2017-17689

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1330-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00056.html

SuSE Linux 42.3
x86_64
enigmail-2.0.4-12.1

i586
enigmail-2.0.4-12.1

146697 - SuSE SLES 11 SP4 SUSE-SU-2018:1323-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1323-1

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-May/004059.html

SuSE SLES 11 SP4
i586
libcurl4-7.37.0-70.27.1
curl-7.37.0-70.27.1

x86_64
libcurl4-32bit-7.37.0-70.27.1
libcurl4-7.37.0-70.27.1
curl-7.37.0-70.27.1

146698 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1334-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158, CVE-2018-5159, CVE-2018-5168, CVE-2018-5174, CVE-2018-5178, CVE-2018-5183

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1334-1

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-May/004065.html

SuSE SLED 12 SP3
x86_64
MozillaFirefox-debugsource-52.8.0esr-109.31.2
MozillaFirefox-52.8.0esr-109.31.2
MozillaFirefox-translations-52.8.0esr-109.31.2
MozillaFirefox-debuginfo-52.8.0esr-109.31.2

SuSE SLES 12 SP3
x86_64
MozillaFirefox-debugsource-52.8.0esr-109.31.2
MozillaFirefox-52.8.0esr-109.31.2
MozillaFirefox-translations-52.8.0esr-109.31.2
MozillaFirefox-debuginfo-52.8.0esr-109.31.2

146699 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1327-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000301

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1327-1

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-May/004062.html

SuSE SLED 12 SP3
x86_64
libcurl4-debuginfo-7.37.0-37.23.1
curl-debuginfo-7.37.0-37.23.1
libcurl4-32bit-7.37.0-37.23.1
libcurl4-debuginfo-32bit-7.37.0-37.23.1
curl-debugsource-7.37.0-37.23.1
curl-7.37.0-37.23.1
libcurl4-7.37.0-37.23.1

SuSE SLES 12 SP3

x86_64
libcurl4-debuginfo-7.37.0-37.23.1
curl-debuginfo-7.37.0-37.23.1
libcurl4-32bit-7.37.0-37.23.1
libcurl4-debuginfo-32bit-7.37.0-37.23.1
curl-debugsource-7.37.0-37.23.1
curl-7.37.0-37.23.1
libcurl4-7.37.0-37.23.1

146700 - SuSE SLES 11 SP4 SUSE-SU-2018:1319-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158, CVE-2018-5159, CVE-2018-5168, CVE-2018-5174, CVE-2018-5178, CVE-2018-5183

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1319-1

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-May/004056.html

SuSE SLES 11 SP4
i586
MozillaFirefox-52.8.0esr-72.32.1
MozillaFirefox-translations-52.8.0esr-72.32.1

x86_64
MozillaFirefox-52.8.0esr-72.32.1
MozillaFirefox-translations-52.8.0esr-72.32.1

146701 - SuSE Linux 15.0 openSUSE-SU-2018:1340-1 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-2018:1340-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00062.html

SuSE Linux 15.0
x86_64
update-test-security-5.1-lp150.3.4.2

i586

update-test-security-5.1-lp150.3.4.2

146702 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1364-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1239, CVE-2017-171479, CVE-2017-17479, CVE-2017-17480

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1364-1

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-May/004068.html

SuSE SLED 12 SP3
x86_64
libopenjp2-7-2.1.0-4.9.1
libopenjp2-7-debuginfo-2.1.0-4.9.1
openjpeg2-debuginfo-2.1.0-4.9.1
openjpeg2-debugsource-2.1.0-4.9.1

SuSE SLES 12 SP3
x86_64
libopenjp2-7-2.1.0-4.9.1
libopenjp2-7-debuginfo-2.1.0-4.9.1
openjpeg2-debuginfo-2.1.0-4.9.1
openjpeg2-debugsource-2.1.0-4.9.1

146703 - SuSE Linux 15.0 openSUSE-SU-2018:1347-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17688, CVE-2017-17689

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1347-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00069.html

SuSE Linux 15.0
x86_64
enigmail-2.0.4-lp150.2.3.1

160393 - CentOS 7 CESA-2018-1649 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1649

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022839.html

CentOS 7
i686
java-1.8.0-openjdk-accessibility-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-zip-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el7_5

x86_64
java-1.8.0-openjdk-accessibility-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5

160394 - CentOS 7 CESA-2018-1629 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1629

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022843.html

CentOS 7
x86_64
kernel-headers-3.10.0-862.3.2.el7
kernel-debug-devel-3.10.0-862.3.2.el7
kernel-devel-3.10.0-862.3.2.el7
kernel-tools-libs-3.10.0-862.3.2.el7
python-perf-3.10.0-862.3.2.el7
perf-3.10.0-862.3.2.el7
kernel-3.10.0-862.3.2.el7
kernel-debug-3.10.0-862.3.2.el7
kernel-tools-3.10.0-862.3.2.el7
kernel-tools-libs-devel-3.10.0-862.3.2.el7

noarch
kernel-abi-whitelists-3.10.0-862.3.2.el7
kernel-doc-3.10.0-862.3.2.el7

160395 - CentOS 7 CESA-2018-1632 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1632

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022840.html

CentOS 7
x86_64
libvirt-daemon-driver-storage-gluster-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-iscsi-3.9.0-14.el7_5.5
libvirt-daemon-config-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-3.9.0-14.el7_5.5
libvirt-lock-sanlock-3.9.0-14.el7_5.5
libvirt-client-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-core-3.9.0-14.el7_5.5
libvirt-libs-3.9.0-14.el7_5.5
libvirt-daemon-driver-secret-3.9.0-14.el7_5.5
libvirt-login-shell-3.9.0-14.el7_5.5
libvirt-daemon-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-mpath-3.9.0-14.el7_5.5
libvirt-daemon-driver-nodedev-3.9.0-14.el7_5.5
libvirt-daemon-driver-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-rbd-3.9.0-14.el7_5.5

libvirt-daemon-config-network-3.9.0-14.el7_5.5
libvirt-3.9.0-14.el7_5.5
libvirt-daemon-driver-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-logical-3.9.0-14.el7_5.5
libvirt-daemon-kvm-3.9.0-14.el7_5.5
libvirt-nss-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-disk-3.9.0-14.el7_5.5
libvirt-admin-3.9.0-14.el7_5.5
libvirt-devel-3.9.0-14.el7_5.5
libvirt-daemon-driver-qemu-3.9.0-14.el7_5.5
libvirt-daemon-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-scsi-3.9.0-14.el7_5.5
libvirt-daemon-driver-interface-3.9.0-14.el7_5.5
libvirt-docs-3.9.0-14.el7_5.5

i686
libvirt-nss-3.9.0-14.el7_5.5
libvirt-libs-3.9.0-14.el7_5.5
libvirt-client-3.9.0-14.el7_5.5
libvirt-devel-3.9.0-14.el7_5.5

160396 - CentOS 6 CESA-2018-1650 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1650

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022833.html

CentOS 6
i686
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el6_9

x86_64
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9

java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

160397 - CentOS 7 CESA-2018-1648 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1648

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022838.html

CentOS 7
x86_64
java-1.7.0-openjdk-accessibility-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-headless-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el7_5

noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el7_5

160399 - CentOS 6 CESA-2018-1660 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1660

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022837.html

CentOS 6
x86_64
qemu-img-0.12.1.2-2.503.el6_9.6
qemu-kvm-tools-0.12.1.2-2.503.el6_9.6

qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-0.12.1.2-2.503.el6_9.6

i686
qemu-guest-agent-0.12.1.2-2.503.el6_9.6

160400 - CentOS 6 CESA-2018-1647 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1647

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022834.html

CentOS 6
i686
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el6_9

x86_64
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el6_9

160401 - CentOS 7 CESA-2018-1633 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1633

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022842.html

CentOS 7
x86_64

qemu-kvm-tools-1.5.3-156.el7_5.2
qemu-img-1.5.3-156.el7_5.2
qemu-kvm-common-1.5.3-156.el7_5.2
qemu-kvm-1.5.3-156.el7_5.2

160402 - CentOS 6 CESA-2018-1651 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1651

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022835.html

CentOS 6
i686
kernel-headers-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6

noarch
kernel-abi-whitelists-2.6.32-696.30.1.el6
kernel-doc-2.6.32-696.30.1.el6
kernel-firmware-2.6.32-696.30.1.el6

x86_64
kernel-headers-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6

163619 - Oracle Enterprise Linux ELSA-2018-1649 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1649

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007747.html

OEL7
x86_64
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-zip-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el7_5

163620 - Oracle Enterprise Linux ELSA-2018-1669 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1669

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007756.html

OEL6
x86_64
libvirt-devel-0.10.2-62.0.1.el6_9.2
libvirt-0.10.2-62.0.1.el6_9.2
libvirt-client-0.10.2-62.0.1.el6_9.2
libvirt-python-0.10.2-62.0.1.el6_9.2
libvirt-lock-sanlock-0.10.2-62.0.1.el6_9.2

i386
libvirt-devel-0.10.2-62.0.1.el6_9.2
libvirt-0.10.2-62.0.1.el6_9.2
libvirt-client-0.10.2-62.0.1.el6_9.2
libvirt-python-0.10.2-62.0.1.el6_9.2

163621 - Oracle Enterprise Linux ELSA-2018-1651 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1651

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007754.html

OEL6
x86_64
kernel-headers-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
kernel-doc-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-abi-whitelists-2.6.32-696.30.1.el6
kernel-firmware-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6

i386
kernel-headers-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
kernel-doc-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-abi-whitelists-2.6.32-696.30.1.el6
kernel-firmware-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6

163622 - Oracle Enterprise Linux ELSA-2018-4110 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5157, CVE-2017-0861, CVE-2017-14106, CVE-2017-15299, CVE-2017-15868, CVE-2017-16525, CVE-2017-16526, CVE-2017-16527, CVE-2017-16529, CVE-2017-16531, CVE-2017-16532, CVE-2017-16533, CVE-2017-16536, CVE-2017-16537, CVE-2017-16643, CVE-2017-16649, CVE-2017-17448, CVE-2017-17558, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-6951, CVE-2017-7482, CVE-2017-8824, CVE-2018-100199, CVE-2018-10323, CVE-2018-1068, CVE-2018-1093, CVE-2018-5332, CVE-2018-8897

Description

The scan detected that the host is missing the following update:
ELSA-2018-4110

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007738.html

OEL6
x86_64
kernel-uek-debug-2.6.39-400.299.1.el6uek
kernel-uek-firmware-2.6.39-400.299.1.el6uek
kernel-uek-doc-2.6.39-400.299.1.el6uek
kernel-uek-devel-2.6.39-400.299.1.el6uek
kernel-uek-debug-devel-2.6.39-400.299.1.el6uek
kernel-uek-2.6.39-400.299.1.el6uek

i386
kernel-uek-debug-2.6.39-400.299.1.el6uek
kernel-uek-firmware-2.6.39-400.299.1.el6uek
kernel-uek-doc-2.6.39-400.299.1.el6uek
kernel-uek-devel-2.6.39-400.299.1.el6uek
kernel-uek-debug-devel-2.6.39-400.299.1.el6uek
kernel-uek-2.6.39-400.299.1.el6uek

163623 - Oracle Enterprise Linux ELSA-2018-1647 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1647

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007753.html

OEL6
x86_64
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.0.1.el6_9
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.0.1.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.0.1.el6_9
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.0.1.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.0.1.el6_9

i386
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.0.1.el6_9
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.0.1.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.0.1.el6_9
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.0.1.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.0.1.el6_9

163624 - Oracle Enterprise Linux ELSA-2018-1648 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1648

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007748.html

OEL7
x86_64
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.0.1.el7_5
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.0.1.el7_5
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.0.1.el7_5
java-1.7.0-openjdk-accessibility-1.7.0.181-2.6.14.8.0.1.el7_5
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.0.1.el7_5
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.0.1.el7_5
java-1.7.0-openjdk-headless-1.7.0.181-2.6.14.8.0.1.el7_5

163625 - Oracle Enterprise Linux ELSA-2018-1632 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1632

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007751.html

OEL7
x86_64
libvirt-daemon-driver-storage-gluster-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-iscsi-3.9.0-14.el7_5.5
libvirt-daemon-config-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-3.9.0-14.el7_5.5
libvirt-lock-sanlock-3.9.0-14.el7_5.5
libvirt-client-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-core-3.9.0-14.el7_5.5
libvirt-libs-3.9.0-14.el7_5.5
libvirt-daemon-driver-secret-3.9.0-14.el7_5.5
libvirt-login-shell-3.9.0-14.el7_5.5
libvirt-daemon-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-mpath-3.9.0-14.el7_5.5
libvirt-daemon-driver-nodedev-3.9.0-14.el7_5.5
libvirt-daemon-driver-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-rbd-3.9.0-14.el7_5.5
libvirt-daemon-config-network-3.9.0-14.el7_5.5
libvirt-3.9.0-14.el7_5.5
libvirt-daemon-driver-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-logical-3.9.0-14.el7_5.5

libvirt-daemon-kvm-3.9.0-14.el7_5.5
libvirt-nss-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-disk-3.9.0-14.el7_5.5
libvirt-admin-3.9.0-14.el7_5.5
libvirt-devel-3.9.0-14.el7_5.5
libvirt-daemon-driver-qemu-3.9.0-14.el7_5.5
libvirt-daemon-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-scsi-3.9.0-14.el7_5.5
libvirt-daemon-driver-interface-3.9.0-14.el7_5.5
libvirt-docs-3.9.0-14.el7_5.5

163626 - Oracle Enterprise Linux ELSA-2018-1650 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1650

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007757.html

OEL6
x86_64
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

i386
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

163627 - Oracle Enterprise Linux ELSA-2018-1660 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1660

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007755.html

OEL6
x86_64
qemu-img-0.12.1.2-2.503.el6_9.6
qemu-kvm-tools-0.12.1.2-2.503.el6_9.6
qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-0.12.1.2-2.503.el6_9.6

i386
qemu-guest-agent-0.12.1.2-2.503.el6_9.6

163628 - Oracle Enterprise Linux ELSA-2018-1633 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2018-1633

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007749.html

OEL7
x86_64
qemu-kvm-tools-1.5.3-156.el7_5.2
qemu-img-1.5.3-156.el7_5.2
qemu-kvm-common-1.5.3-156.el7_5.2
qemu-kvm-1.5.3-156.el7_5.2

163629 - Oracle Enterprise Linux ELSA-2018-1629 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000199, CVE-2018-1087, CVE-2018-3639, CVE-2018-8897

Description

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

ELSA-2018-1629

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007750.html

OEL7
x86_64
kernel-headers-3.10.0-862.3.2.el7
kernel-debug-devel-3.10.0-862.3.2.el7
kernel-devel-3.10.0-862.3.2.el7
kernel-abi-whitelists-3.10.0-862.3.2.el7
python-perf-3.10.0-862.3.2.el7
perf-3.10.0-862.3.2.el7
kernel-3.10.0-862.3.2.el7
kernel-debug-3.10.0-862.3.2.el7
kernel-doc-3.10.0-862.3.2.el7
kernel-tools-3.10.0-862.3.2.el7
kernel-tools-libs-3.10.0-862.3.2.el7
kernel-tools-libs-devel-3.10.0-862.3.2.el7

175385 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL6.x i386/x86_64 (1805-23105)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.7.0-openjdk on SL6.x i386/x86_64 (1805-23105)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=23105

SL6
i386
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el6_9

x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el6_9
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el6_9

175386 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL7.x x86_64 (1805-24796)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.7.0-openjdk on SL7.x x86_64 (1805-24796)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=24796

SL7
x86_64
java-1.7.0-openjdk-headless-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-accessibility-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-debuginfo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-demo-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-devel-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-src-1.7.0.181-2.6.14.8.el7_5
java-1.7.0-openjdk-1.7.0.181-2.6.14.8.el7_5

noarch
java-1.7.0-openjdk-javadoc-1.7.0.181-2.6.14.8.el7_5

175387 - Scientific Linux Security ERRATA Important: libvirt on SL6.x i386/x86_64 (1805-23455)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libvirt on SL6.x i386/x86_64 (1805-23455)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=23455

SL6
x86_64
libvirt-debuginfo-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2
libvirt-lock-sanlock-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-devel-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2

i386
libvirt-devel-0.10.2-62.el6_9.2

libvirt-client-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2
libvirt-debuginfo-0.10.2-62.el6_9.2

175388 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1805-25141)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1805-25141)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=25141

SL7
x86_64
kernel-debug-3.10.0-862.3.2.el7
kernel-3.10.0-862.3.2.el7
python-perf-debuginfo-3.10.0-862.3.2.el7
kernel-tools-libs-devel-3.10.0-862.3.2.el7
kernel-tools-debuginfo-3.10.0-862.3.2.el7
perf-debuginfo-3.10.0-862.3.2.el7
kernel-debuginfo-common-x86_64-3.10.0-862.3.2.el7
kernel-debug-devel-3.10.0-862.3.2.el7
kernel-devel-3.10.0-862.3.2.el7
kernel-tools-libs-3.10.0-862.3.2.el7
kernel-debuginfo-3.10.0-862.3.2.el7
perf-3.10.0-862.3.2.el7
kernel-tools-3.10.0-862.3.2.el7
python-perf-3.10.0-862.3.2.el7
kernel-debug-debuginfo-3.10.0-862.3.2.el7
kernel-headers-3.10.0-862.3.2.el7

noarch
kernel-abi-whitelists-3.10.0-862.3.2.el7
kernel-doc-3.10.0-862.3.2.el7

175389 - Scientific Linux Security ERRATA Important: libvirt on SL7.x x86_64 (1805-25806)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libvirt on SL7.x x86_64 (1805-25806)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=25806

SL7
x86_64
libvirt-daemon-driver-storage-gluster-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-iscsi-3.9.0-14.el7_5.5
libvirt-daemon-config-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-nwfilter-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-3.9.0-14.el7_5.5
libvirt-lock-sanlock-3.9.0-14.el7_5.5
libvirt-client-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-core-3.9.0-14.el7_5.5
libvirt-libs-3.9.0-14.el7_5.5
libvirt-daemon-driver-secret-3.9.0-14.el7_5.5
libvirt-login-shell-3.9.0-14.el7_5.5
libvirt-debuginfo-3.9.0-14.el7_5.5
libvirt-daemon-3.9.0-14.el7_5.5
libvirt-daemon-driver-nodedev-3.9.0-14.el7_5.5
libvirt-daemon-config-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-rbd-3.9.0-14.el7_5.5
libvirt-3.9.0-14.el7_5.5
libvirt-daemon-driver-network-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-logical-3.9.0-14.el7_5.5
libvirt-daemon-kvm-3.9.0-14.el7_5.5
libvirt-nss-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-disk-3.9.0-14.el7_5.5
libvirt-admin-3.9.0-14.el7_5.5
libvirt-devel-3.9.0-14.el7_5.5
libvirt-daemon-driver-qemu-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-mpath-3.9.0-14.el7_5.5
libvirt-daemon-lxc-3.9.0-14.el7_5.5
libvirt-daemon-driver-storage-scsi-3.9.0-14.el7_5.5
libvirt-daemon-driver-interface-3.9.0-14.el7_5.5
libvirt-docs-3.9.0-14.el7_5.5

175390 - Scientific Linux Security ERRATA Important: java-1.8.0-openjdk on SL7.x x86_64 (1805-25462)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.8.0-openjdk on SL7.x x86_64 (1805-25462)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=25462

SL7
x86_64
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5

java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-accessibility-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el7_5

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-zip-1.8.0.171-8.b10.el7_5
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el7_5

175391 - Scientific Linux Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1805-24471)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1805-24471)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=24471

SL7
x86_64
qemu-kvm-debuginfo-1.5.3-156.el7_5.2
qemu-img-1.5.3-156.el7_5.2
qemu-kvm-common-1.5.3-156.el7_5.2
qemu-kvm-tools-1.5.3-156.el7_5.2
qemu-kvm-1.5.3-156.el7_5.2

175392 - Scientific Linux Security ERRATA Important: java-1.8.0-openjdk on SL6.x i386/x86_64 (1805-24121)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.8.0-openjdk on SL6.x i386/x86_64 (1805-24121)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=24121

SL6
i386
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-javadoc-1.8.0.171-8.b10.el6_9

x86_64
java-1.8.0-openjdk-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-src-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-demo-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-devel-debug-1.8.0.171-8.b10.el6_9
java-1.8.0-openjdk-debug-1.8.0.171-8.b10.el6_9

175393 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1805-23783)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1805-23783)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=23783

SL6
i386
kernel-debuginfo-2.6.32-696.30.1.el6
kernel-headers-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6

python-perf-debuginfo-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6
kernel-debug-debuginfo-2.6.32-696.30.1.el6
perf-debuginfo-2.6.32-696.30.1.el6
kernel-debuginfo-common-i686-2.6.32-696.30.1.el6

noarch
kernel-abi-whitelists-2.6.32-696.30.1.el6
kernel-doc-2.6.32-696.30.1.el6
kernel-firmware-2.6.32-696.30.1.el6

x86_64
kernel-debuginfo-2.6.32-696.30.1.el6
perf-2.6.32-696.30.1.el6
python-perf-2.6.32-696.30.1.el6
kernel-debuginfo-common-x86_64-2.6.32-696.30.1.el6
kernel-debuginfo-common-i686-2.6.32-696.30.1.el6
kernel-2.6.32-696.30.1.el6
kernel-devel-2.6.32-696.30.1.el6
perf-debuginfo-2.6.32-696.30.1.el6
kernel-debug-devel-2.6.32-696.30.1.el6
kernel-headers-2.6.32-696.30.1.el6
python-perf-debuginfo-2.6.32-696.30.1.el6
kernel-debug-debuginfo-2.6.32-696.30.1.el6
kernel-debug-2.6.32-696.30.1.el6

175394 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1805-22775)

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1805-22775)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1805&L=scientific-linux-errata&F=&S=&P=22775

SL6
x86_64
qemu-img-0.12.1.2-2.503.el6_9.6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.6
qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-0.12.1.2-2.503.el6_9.6
qemu-kvm-tools-0.12.1.2-2.503.el6_9.6

i386
qemu-guest-agent-0.12.1.2-2.503.el6_9.6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.6

186212 - Ubuntu Linux 14.04 USN-3655-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12134, CVE-2017-13220, CVE-2017-13305, CVE-2017-17449, CVE-2017-18079, CVE-2017-18203, CVE-2017-18204, CVE-2017-18208, CVE-2017-18221, CVE-2018-3639, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
USN-3655-1

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-May/004406.html

Ubuntu 14.04

linux-image-generic_3.13.0.149.159
linux-image-lowlatency_3.13.0.149.159
linux-image-powerpc64-emb_3.13.0.149.159
linux-image-3.13.0-149-powerpc64-emb_3.13.0-149.199
linux-image-3.13.0-149-powerpc64-smp_3.13.0-149.199
linux-image-powerpc-e500mc_3.13.0.149.159
linux-image-3.13.0-149-powerpc-e500_3.13.0-149.199
linux-image-powerpc-smp_3.13.0.149.159
linux-image-powerpc-e500_3.13.0.149.159
linux-image-3.13.0-149-lowlatency_3.13.0-149.199
linux-image-3.13.0-149-powerpc-e500mc_3.13.0-149.199
linux-image-generic-lpae_3.13.0.149.159
linux-image-3.13.0-149-powerpc-smp_3.13.0-149.199
linux-image-3.13.0-149-generic_3.13.0-149.199
linux-image-3.13.0-149-generic-lpae_3.13.0-149.199
linux-image-powerpc64-smp_3.13.0.149.159

186214 - Ubuntu Linux 14.04 USN-3654-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17975, CVE-2017-18193, CVE-2017-18222, CVE-2018-1065, CVE-2018-1068, CVE-2018-1130, CVE-2018-3639, CVE-2018-5803, CVE-2018-7480, CVE-2018-7757, CVE-2018-7995, CVE-2018-8781, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
USN-3654-2

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-May/004405.html

Ubuntu 14.04

linux-image-4.4.0-127-generic_4.4.0-127.153~14.04.1
linux-image-4.4.0-1022-aws_4.4.0-1022.22
linux-image-4.4.0-127-powerpc-smp_4.4.0-127.153~14.04.1
linux-image-aws_4.4.0.1022.22
linux-image-4.4.0-127-generic-lpae_4.4.0-127.153~14.04.1

linux-image-powerpc-smp-lts-xenial_4.4.0.127.107
linux-image-generic-lpae-lts-xenial_4.4.0.127.107
linux-image-4.4.0-127-lowlatency_4.4.0-127.153~14.04.1
linux-image-4.4.0-127-powerpc-e500mc_4.4.0-127.153~14.04.1
linux-image-generic-lts-xenial_4.4.0.127.107
linux-image-4.4.0-127-powerpc64-smp_4.4.0-127.153~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.127.107
linux-image-4.4.0-127-powerpc64-emb_4.4.0-127.153~14.04.1
linux-image-powerpc64-emb-lts-xenial_4.4.0.127.107
linux-image-lowlatency-lts-xenial_4.4.0.127.107
linux-image-powerpc-e500mc-lts-xenial_4.4.0.127.107

186216 - Ubuntu Linux 16.04 USN-3654-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17975, CVE-2017-18193, CVE-2017-18222, CVE-2018-1065, CVE-2018-1068, CVE-2018-1130, CVE-2018-3639, CVE-2018-5803, CVE-2018-7480, CVE-2018-7757, CVE-2018-7995, CVE-2018-8781, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
USN-3654-1

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-May/004404.html

Ubuntu 16.04

linux-image-aws_4.4.0.1060.62
linux-image-4.4.0-127-powerpc-smp_4.4.0-127.153
linux-image-kvm_4.4.0.1026.25
linux-image-4.4.0-127-powerpc64-emb_4.4.0-127.153
linux-image-powerpc64-smp_4.4.0.127.133
linux-image-powerpc-smp_4.4.0.127.133
linux-image-4.4.0-1026-kvm_4.4.0-1026.31
linux-image-4.4.0-127-powerpc64-smp_4.4.0-127.153
linux-image-generic-lpae_4.4.0.127.133
linux-image-lowlatency_4.4.0.127.133
linux-image-4.4.0-1060-aws_4.4.0-1060.69
linux-image-4.4.0-127-lowlatency_4.4.0-127.153
linux-image-4.4.0-127-generic_4.4.0-127.153
linux-image-4.4.0-127-powerpc-e500mc_4.4.0-127.153
linux-image-4.4.0-127-generic-lpae_4.4.0-127.153
linux-image-powerpc64-emb_4.4.0.127.133
linux-image-generic_4.4.0.127.133
linux-image-powerpc-e500mc_4.4.0.127.133

186217 - Ubuntu Linux 12.04 USN-3655-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12134, CVE-2017-13220, CVE-2017-13305, CVE-2017-17449, CVE-2017-18079, CVE-2017-18203, CVE-2017-18204, CVE-2017-18208, CVE-2017-18221, CVE-2018-3639, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
USN-3655-2

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-May/004407.html

Ubuntu 12.04

linux-image-generic-lpae-lts-trusty_3.13.0.149.140
linux-image-generic-lts-trusty_3.13.0.149.140
linux-image-3.13.0-149-generic_3.13.0-149.199~precise1
linux-image-3.13.0-149-generic-lpae_3.13.0-149.199~precise1

186222 - Ubuntu Linux 17.10 USN-3657-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17449, CVE-2017-17975, CVE-2017-18203, CVE-2017-18208, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
USN-3657-1

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-May/004409.html

Ubuntu 17.10

linux-image-raspi2_4.13.0.1020.18
linux-image-4.13.0-1020-raspi2_4.13.0-1020.21

186224 - Ubuntu Linux 16.04 USN-3653-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17449, CVE-2017-17975, CVE-2017-18203, CVE-2017-18208, CVE-2018-3639, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
USN-3653-2

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-May/004403.html

Ubuntu 16.04

linux-image-generic-hwe-16.04_4.13.0.43.62
linux-image-oem_4.13.0.1028.33
linux-image-lowlatency-hwe-16.04_4.13.0.43.62
linux-image-4.13.0-43-generic-lpae_4.13.0-43.48~16.04.1
linux-image-4.13.0-43-lowlatency_4.13.0-43.48~16.04.1
linux-image-gcp_4.13.0.1017.19
linux-image-4.13.0-1028-oem_4.13.0-1028.31
linux-image-4.13.0-1017-gcp_4.13.0-1017.21
linux-image-azure_4.13.0.1018.19
linux-image-4.13.0-1018-azure_4.13.0-1018.21
linux-image-gke_4.13.0.1017.19
linux-image-generic-lpae-hwe-16.04_4.13.0.43.62
linux-image-4.13.0-43-generic_4.13.0-43.48~16.04.1

186225 - Ubuntu Linux 17.10 USN-3653-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17449, CVE-2017-17975, CVE-2017-18203, CVE-2017-18208, CVE-2018-3639, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
USN-3653-1

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-May/004402.html

Ubuntu 17.10

linux-image-lowlatency_4.13.0.43.46
linux-image-4.13.0-43-lowlatency_4.13.0-43.48
linux-image-4.13.0-43-generic_4.13.0-43.48
linux-image-4.13.0-43-generic-lpae_4.13.0-43.48
linux-image-generic-lpae_4.13.0.43.46
linux-image-generic_4.13.0.43.46

186226 - Ubuntu Linux 16.04 USN-3656-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17975, CVE-2017-18193, CVE-2017-18222, CVE-2018-1065, CVE-2018-1068, CVE-2018-1130, CVE-2018-5803, CVE-2018-7480, CVE-2018-7757, CVE-2018-7995, CVE-2018-8781, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
USN-3656-1

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-May/004408.html

Ubuntu 16.04

linux-image-4.4.0-1090-raspi2_4.4.0-1090.98
linux-image-snapdragon_4.4.0.1093.85
linux-image-4.4.0-1093-snapdragon_4.4.0-1093.98
linux-image-raspi2_4.4.0.1090.90

186227 - Ubuntu Linux 14.04, 16.04, 17.10, 18.04 USN-3649-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16845, CVE-2018-7550, CVE-2018-7858

Description

The scan detected that the host is missing the following update:
USN-3649-1

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-May/004394.html

Ubuntu 16.04

qemu-system-mips_2.5+dfsg-5ubuntu10.28
qemu-system-sparc_2.5+dfsg-5ubuntu10.28
qemu-system-aarch64_2.5+dfsg-5ubuntu10.28
qemu-system-arm_2.5+dfsg-5ubuntu10.28
qemu-system_2.5+dfsg-5ubuntu10.28
qemu-system-s390x_2.5+dfsg-5ubuntu10.28
qemu-system-ppc_2.5+dfsg-5ubuntu10.28
qemu-system-x86_2.5+dfsg-5ubuntu10.28

Ubuntu 14.04

qemu-system-sparc_2.0.0+dfsg-2ubuntu1.41
qemu-system-x86_2.0.0+dfsg-2ubuntu1.41
qemu-system_2.0.0+dfsg-2ubuntu1.41
qemu-system-mips_2.0.0+dfsg-2ubuntu1.41
qemu-system-aarch64_2.0.0+dfsg-2ubuntu1.41
qemu-system-arm_2.0.0+dfsg-2ubuntu1.41
qemu-system-ppc_2.0.0+dfsg-2ubuntu1.41

Ubuntu 18.04

qemu-system_2.11+dfsg-1ubuntu7.1
qemu-system-x86_2.11+dfsg-1ubuntu7.1
qemu-system-ppc_2.11+dfsg-1ubuntu7.1
qemu-system-arm_2.11+dfsg-1ubuntu7.1
qemu-system-sparc_2.11+dfsg-1ubuntu7.1
qemu-system-s390x_2.11+dfsg-1ubuntu7.1
qemu-system-mips_2.11+dfsg-1ubuntu7.1

Ubuntu 17.10

qemu-system-ppc_2.10+dfsg-0ubuntu3.6
qemu-system-arm_2.10+dfsg-0ubuntu3.6

qemu-system-s390x_2.10+dfsg-0ubuntu3.6
qemu-system-x86_2.10+dfsg-0ubuntu3.6
qemu-system-aarch64_2.10+dfsg-0ubuntu3.6
qemu-system-mips_2.10+dfsg-0ubuntu3.6
qemu-system-sparc_2.10+dfsg-0ubuntu3.6
qemu-system_2.10+dfsg-0ubuntu3.6

193724 - Fedora Linux 28 FEDORA-2018-c6e8b5f529 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3836, CVE-2018-7440, CVE-2018-7442

Description

The scan detected that the host is missing the following update:
FEDORA-2018-c6e8b5f529

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/2018/5/?count=200&page=3

Fedora Core 28

leptonica-1.76.0-1.fc28

131109 - Debian Linux 8.0 DSA-4204-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10995, CVE-2017-11533, CVE-2017-11535, CVE-2017-11639, CVE-2017-13143, CVE-2017-17504, CVE-2017-17879, CVE-2018-5248

Description

The scan detected that the host is missing the following update:
DSA-4204-1

Observation

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

http://www.debian.org/security/2018/dsa-4204

Debian 8.0
all
imagemagick_8:6.8.9.9-5+deb8u12

131114 - Debian Linux 9.0 DSA-4203-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17670

Description

The scan detected that the host is missing the following update:
DSA-4203-1

Observation

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

http://www.debian.org/security/2018/dsa-4203

Debian 9.0
all
vlc_3.0.2-0+deb9u1

132456 - Oracle VM OVMSA-2018-0221 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17565, CVE-2017-17566, CVE-2018-10981, CVE-2018-10982, CVE-2018-8897

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0221

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-May/000857.html

OVM3.4
x86_64
xen-4.4.4-155.0.36.el6
xen-tools-4.4.4-155.0.36.el6

132458 - Oracle VM OVMSA-2018-0218 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17565, CVE-2017-17566, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-10981, CVE-2018-10982, CVE-2018-7540, CVE-2018-7541, CVE-2018-8897

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0218

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-May/000856.html

OVM3.4
x86_64
xen-4.4.4-105.0.45.el6

xen-tools-4.4.4-105.0.45.el6

146683 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1332-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10194

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1332-1

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-May/004063.html

SuSE SLED 12 SP3
x86_64
ghostscript-debugsource-9.15-23.10.2
ghostscript-9.15-23.10.2
ghostscript-x11-9.15-23.10.2
ghostscript-x11-debuginfo-9.15-23.10.2
ghostscript-debuginfo-9.15-23.10.2

SuSE SLES 12 SP3
x86_64
ghostscript-debugsource-9.15-23.10.2
ghostscript-9.15-23.10.2
ghostscript-x11-9.15-23.10.2
ghostscript-x11-debuginfo-9.15-23.10.2
ghostscript-debuginfo-9.15-23.10.2

146684 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1324-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14160, CVE-2018-10393

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1324-1

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-May/004060.html

SuSE SLED 12 SP3
x86_64
libvorbisenc2-debuginfo-1.3.3-10.11.1
libvorbisfile3-debuginfo-32bit-1.3.3-10.11.1
libvorbis-debugsource-1.3.3-10.11.1
libvorbisfile3-debuginfo-1.3.3-10.11.1

libvorbis0-debuginfo-32bit-1.3.3-10.11.1
libvorbisfile3-1.3.3-10.11.1
libvorbisenc2-debuginfo-32bit-1.3.3-10.11.1
libvorbisenc2-32bit-1.3.3-10.11.1
libvorbis0-32bit-1.3.3-10.11.1
libvorbis0-debuginfo-1.3.3-10.11.1
libvorbisfile3-32bit-1.3.3-10.11.1
libvorbisenc2-1.3.3-10.11.1
libvorbis0-1.3.3-10.11.1

SuSE SLES 12 SP3
noarch
libvorbis-doc-1.3.3-10.11.1

x86_64
libvorbisfile3-debuginfo-32bit-1.3.3-10.11.1
libvorbis-debugsource-1.3.3-10.11.1
libvorbisfile3-debuginfo-1.3.3-10.11.1
libvorbis0-debuginfo-32bit-1.3.3-10.11.1
libvorbisfile3-1.3.3-10.11.1
libvorbisenc2-debuginfo-32bit-1.3.3-10.11.1
libvorbisenc2-32bit-1.3.3-10.11.1
libvorbisenc2-debuginfo-1.3.3-10.11.1
libvorbis0-debuginfo-1.3.3-10.11.1
libvorbisfile3-32bit-1.3.3-10.11.1
libvorbisenc2-1.3.3-10.11.1
libvorbis0-1.3.3-10.11.1
libvorbis0-32bit-1.3.3-10.11.1

146686 - SuSE Linux 42.3 openSUSE-SU-2018:1348-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10194

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1348-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00070.html

SuSE Linux 42.3
x86_64
ghostscript-mini-9.15-14.6.1
ghostscript-x11-debuginfo-9.15-14.6.1
ghostscript-devel-9.15-14.6.1
ghostscript-debuginfo-9.15-14.6.1
ghostscript-x11-9.15-14.6.1
ghostscript-9.15-14.6.1
ghostscript-mini-debuginfo-9.15-14.6.1
ghostscript-mini-devel-9.15-14.6.1
ghostscript-debugsource-9.15-14.6.1
ghostscript-mini-debugsource-9.15-14.6.1

i586
ghostscript-mini-9.15-14.6.1
ghostscript-x11-debuginfo-9.15-14.6.1
ghostscript-devel-9.15-14.6.1
ghostscript-debuginfo-9.15-14.6.1
ghostscript-x11-9.15-14.6.1
ghostscript-9.15-14.6.1
ghostscript-mini-debuginfo-9.15-14.6.1
ghostscript-mini-devel-9.15-14.6.1
ghostscript-debugsource-9.15-14.6.1
ghostscript-mini-debugsource-9.15-14.6.1

146688 - SuSE Linux 42.3 openSUSE-SU-2018:1345-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14160, CVE-2018-10393

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1345-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00067.html

SuSE Linux 42.3
i586
libvorbisenc2-1.3.3-14.1
libvorbis-devel-1.3.3-14.1
libvorbisfile3-debuginfo-1.3.3-14.1
libvorbisenc2-debuginfo-1.3.3-14.1
libvorbis-debugsource-1.3.3-14.1
libvorbis0-debuginfo-1.3.3-14.1
libvorbisfile3-1.3.3-14.1
libvorbis0-1.3.3-14.1

noarch
libvorbis-doc-1.3.3-14.1

x86_64
libvorbisenc2-1.3.3-14.1
libvorbisfile3-debuginfo-1.3.3-14.1
libvorbisenc2-32bit-1.3.3-14.1
libvorbis0-1.3.3-14.1
libvorbis0-32bit-1.3.3-14.1
libvorbisenc2-debuginfo-32bit-1.3.3-14.1
libvorbisenc2-debuginfo-1.3.3-14.1
libvorbis0-debuginfo-1.3.3-14.1
libvorbis-devel-1.3.3-14.1
libvorbisfile3-32bit-1.3.3-14.1
libvorbis0-debuginfo-32bit-1.3.3-14.1
libvorbisfile3-debuginfo-32bit-1.3.3-14.1
libvorbisfile3-1.3.3-14.1
libvorbis-debugsource-1.3.3-14.1

146691 - SuSE Linux 42.3 openSUSE-SU-2018:1311-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10119, CVE-2018-10120

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1311-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00046.html

SuSE Linux 42.3
x86_64
libreofficekit-devel-6.0.4.2-21.1
libreoffice-mailmerge-6.0.4.2-21.1
libreoffice-draw-6.0.4.2-21.1
libreoffice-impress-debuginfo-6.0.4.2-21.1
libreoffice-draw-debuginfo-6.0.4.2-21.1
libreoffice-base-drivers-mysql-6.0.4.2-21.1
libreoffice-sdk-6.0.4.2-21.1
libreoffice-sdk-doc-6.0.4.2-21.1
libreoffice-filters-optional-6.0.4.2-21.1
libreoffice-debugsource-6.0.4.2-21.1
libreoffice-impress-6.0.4.2-21.1
libreoffice-math-6.0.4.2-21.1
libreoffice-pyuno-6.0.4.2-21.1
libreoffice-sdk-debuginfo-6.0.4.2-21.1
libreoffice-base-drivers-mysql-debuginfo-6.0.4.2-21.1
libreoffice-writer-debuginfo-6.0.4.2-21.1
libreoffice-pyuno-debuginfo-6.0.4.2-21.1
libreoffice-calc-6.0.4.2-21.1
libreoffice-base-drivers-postgresql-debuginfo-6.0.4.2-21.1
libreoffice-6.0.4.2-21.1
libreoffice-kde4-debuginfo-6.0.4.2-21.1
libreoffice-gtk2-debuginfo-6.0.4.2-21.1
libreoffice-calc-debuginfo-6.0.4.2-21.1
libreoffice-math-debuginfo-6.0.4.2-21.1
libreoffice-gnome-6.0.4.2-21.1
libreoffice-officebean-debuginfo-6.0.4.2-21.1
libreoffice-officebean-6.0.4.2-21.1
libreoffice-debuginfo-6.0.4.2-21.1
libreoffice-gtk3-debuginfo-6.0.4.2-21.1
libreoffice-gnome-debuginfo-6.0.4.2-21.1
libreoffice-base-debuginfo-6.0.4.2-21.1
libreoffice-writer-6.0.4.2-21.1
libreoffice-gtk3-6.0.4.2-21.1
libreoffice-writer-extensions-6.0.4.2-21.1
libreoffice-base-drivers-postgresql-6.0.4.2-21.1
libreoffice-calc-extensions-6.0.4.2-21.1
libreoffice-kde4-6.0.4.2-21.1
libreoffice-base-6.0.4.2-21.1
libreoffice-gtk2-6.0.4.2-21.1
libreofficekit-6.0.4.2-21.1

noarch
libreoffice-l10n-bg-6.0.4.2-21.1
libreoffice-l10n-mr-6.0.4.2-21.1
libreoffice-l10n-cy-6.0.4.2-21.1
libreoffice-l10n-ml-6.0.4.2-21.1
libreoffice-l10n-ru-6.0.4.2-21.1
libreoffice-l10n-et-6.0.4.2-21.1
libreoffice-l10n-or-6.0.4.2-21.1
libreoffice-l10n-ar-6.0.4.2-21.1
libreoffice-l10n-ve-6.0.4.2-21.1
libreoffice-l10n-de-6.0.4.2-21.1
libreoffice-l10n-nb-6.0.4.2-21.1
libreoffice-l10n-eo-6.0.4.2-21.1
libreoffice-l10n-el-6.0.4.2-21.1
libreoffice-l10n-fi-6.0.4.2-21.1
libreoffice-gdb-pretty-printers-6.0.4.2-21.1
libreoffice-l10n-zu-6.0.4.2-21.1
libreoffice-l10n-ts-6.0.4.2-21.1
libreoffice-l10n-ca-6.0.4.2-21.1
libreoffice-icon-themes-6.0.4.2-21.1
libreoffice-glade-6.0.4.2-21.1
libreoffice-l10n-en-6.0.4.2-21.1
libreoffice-l10n-it-6.0.4.2-21.1
libreoffice-l10n-sr-6.0.4.2-21.1
libreoffice-l10n-xh-6.0.4.2-21.1
libreoffice-l10n-zh_CN-6.0.4.2-21.1
libreoffice-l10n-ga-6.0.4.2-21.1
libreoffice-l10n-pt_PT-6.0.4.2-21.1
libreoffice-l10n-hr-6.0.4.2-21.1
libreoffice-branding-upstream-6.0.4.2-21.1
libreoffice-l10n-kn-6.0.4.2-21.1
libreoffice-l10n-lv-6.0.4.2-21.1
libreoffice-l10n-st-6.0.4.2-21.1
libreoffice-l10n-he-6.0.4.2-21.1
libreoffice-l10n-gl-6.0.4.2-21.1
libreoffice-l10n-nr-6.0.4.2-21.1
libreoffice-l10n-ja-6.0.4.2-21.1
libreoffice-l10n-fa-6.0.4.2-21.1
libreoffice-l10n-th-6.0.4.2-21.1
libreoffice-l10n-sl-6.0.4.2-21.1
libreoffice-l10n-br-6.0.4.2-21.1
libreoffice-l10n-eu-6.0.4.2-21.1
libreoffice-l10n-ro-6.0.4.2-21.1
libreoffice-l10n-as-6.0.4.2-21.1
libreoffice-l10n-kk-6.0.4.2-21.1
libreoffice-l10n-fr-6.0.4.2-21.1
libreoffice-l10n-cs-6.0.4.2-21.1
libreoffice-l10n-es-6.0.4.2-21.1
libreoffice-l10n-sv-6.0.4.2-21.1
libreoffice-l10n-mai-6.0.4.2-21.1
libreoffice-l10n-pl-6.0.4.2-21.1
libreoffice-l10n-lt-6.0.4.2-21.1
libreoffice-l10n-da-6.0.4.2-21.1
libreoffice-l10n-pt_BR-6.0.4.2-21.1
libreoffice-l10n-nl-6.0.4.2-21.1
libreoffice-l10n-pa-6.0.4.2-21.1
libreoffice-l10n-af-6.0.4.2-21.1
libreoffice-l10n-hu-6.0.4.2-21.1
libreoffice-l10n-tr-6.0.4.2-21.1
libreoffice-l10n-dz-6.0.4.2-21.1

libreoffice-l10n-zh_TW-6.0.4.2-21.1
libreoffice-l10n-ss-6.0.4.2-21.1
libreoffice-l10n-nso-6.0.4.2-21.1
libreoffice-l10n-ta-6.0.4.2-21.1
libreoffice-l10n-nn-6.0.4.2-21.1
libreoffice-l10n-si-6.0.4.2-21.1
libreoffice-l10n-tn-6.0.4.2-21.1
libreoffice-l10n-ko-6.0.4.2-21.1
libreoffice-l10n-gu-6.0.4.2-21.1
libreoffice-l10n-te-6.0.4.2-21.1
libreoffice-l10n-hi-6.0.4.2-21.1
libreoffice-l10n-bn-6.0.4.2-21.1
libreoffice-l10n-sk-6.0.4.2-21.1
libreoffice-l10n-uk-6.0.4.2-21.1

146695 - SuSE SLES 11 SP4 SUSE-SU-2018:1321-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14160, CVE-2018-10393

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1321-1

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-May/004057.html

SuSE SLES 11 SP4
i586
libvorbis-1.2.0-79.20.11.1
libvorbis-doc-1.2.0-79.20.11.1

x86_64
libvorbis-32bit-1.2.0-79.20.11.1
libvorbis-doc-1.2.0-79.20.11.1
libvorbis-1.2.0-79.20.11.1

193716 - Fedora Linux 26 FEDORA-2018-742a69ccc3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13735, CVE-2017-14348, CVE-2018-10528, CVE-2018-10529

Description

The scan detected that the host is missing the following update:
FEDORA-2018-742a69ccc3

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/2018/5/?count=200&page=2

Fedora Core 26

LibRaw-0.18.11-1.fc26

193719 - Fedora Linux 26 FEDORA-2018-d955395c08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3265, CVE-2017-3308, CVE-2017-3309, CVE-2017-3313, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2018-2755, CVE-2018-2761, CVE-2018-2766, CVE-2018-2771, CVE-2018-2773, CVE-2018-2781, CVE-2018-2782, CVE-2018-2784, CVE-2018-2787, CVE-2018-2813, CVE-2018-2817, CVE-2018-2818, CVE-2018-2819

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d955395c08

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/2018/5/?count=200&page=1

Fedora Core 26

mariadb-10.1.33-1.fc26

23592 - (APSB18-18) Vulnerability In Adobe Connect

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

Risk Level: Medium

CVE: CVE-2018-4994

Description

A vulnerability is present in some versions of Adobe Connect.

Observation

Adobe Connect is a network meeting solution.

A vulnerability is present in some versions of Adobe Connect. The flaw lies in authentication mechanism. Successful exploitation could allow an attacker to cause disclosure of information.

23595 - LibreOffice MSWord Customizations Parsing Heap Buffer Overflow Vulnerability

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

Risk Level: Medium

CVE: CVE-2018-10120

Description

A vulnerability is present in some versions of LibreOffice.

Observation

LibreOffice is an open source office suite.

A vulnerability is present in some versions of LibreOffice. The flaw lies in the SwCTBWrapper Read function. Successful exploitation by an attacker could result in a denial-of-service condition.

23596 - LibreOffice MSWord Customizations Parsing Heap Buffer Overflow Vulnerability

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

Risk Level: Medium

CVE: CVE-2018-10120

Description

A vulnerability is present in some versions of LibreOffice.

Observation

LibreOffice is an open source office suite.

A vulnerability is present in some versions of LibreOffice. The flaw lies in the SwCTBWrapper Read function. Successful exploitation by an attacker could result in a denial-of-service condition.

23598 - (K04912972) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2018-7185

Description

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

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

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

23612 - (K23520761) F5 BIG-IP BIG-IP ASM and BIG-IP Analytics Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2018-5505

Description

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

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in ASM and AVR modules. Successful exploitation could allow remote attackers to cause a denial of service.

23613 - (K54562183) F5 BIG-IP BIG-IP PEM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2018-5503

Description

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

Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in PEM policy content insertion actions. Successful exploitation could allow remote attackers to cause a denial of service.

178630 - Gentoo Linux GLSA-201805-07 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-201805-07

Observation

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

https://security.gentoo.org/glsa/201805-07

Affected packages:
net-fs/samba < 4.5.16

178631 - Gentoo Linux GLSA-201805-09 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-201805-09

Observation

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

https://security.gentoo.org/glsa/201805-09

Affected packages:
sys-apps/shadow < 4.6

178632 - Gentoo Linux GLSA-201805-06 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-201805-06

Observation

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

https://security.gentoo.org/glsa/201805-06

Affected packages:
www-client/chromium < 66.0.3359.170
www-client/google-chrome < 66.0.3359.170

178633 - Gentoo Linux GLSA-201805-08 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-201805-08

Observation

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

https://security.gentoo.org/glsa/201805-08

Affected packages:
app-emulation/virtualbox < 5.1.36
app-emulation/virtualbox-bin < 5.1.36.122089

193723 - Fedora Linux 28 FEDORA-2018-54c29139b3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17723, CVE-2017-17725, CVE-2017-5772, CVE-2018-5772

Description

The scan detected that the host is missing the following update:
FEDORA-2018-54c29139b3

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/2018/5/?count=200&page=2

Fedora Core 28

exiv2-0.26-10.fc28

193727 - Fedora Linux 28 FEDORA-2018-9b965c4eed Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1002101

Description

The scan detected that the host is missing the following update:
FEDORA-2018-9b965c4eed

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/2018/5/?count=200&page=3

Fedora Core 28

kubernetes-1.10.1-0.fc28

193728 - Fedora Linux 27 FEDORA-2018-fc9c5969b4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17723, CVE-2017-17725, CVE-2017-5772, CVE-2018-5772

Description

The scan detected that the host is missing the following update:
FEDORA-2018-fc9c5969b4

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/2018/5/?count=200&page=2

Fedora Core 27

exiv2-0.26-10.fc27

88944 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-136-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10546, CVE-2018-10547, CVE-2018-10548, CVE-2018-10549, CVE-2018-5712

Description

The scan detected that the host is missing the following update:
SSA:2018-136-02

Observation

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

For more information see:

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2018&m=slackware-security.411881

Slackware 14.0
x86_64
php-5.6.36-x86_64-1

Slackware 14.2
x86_64
php-5.6.36-x86_64-1

i586
php-5.6.36-i586-1

Slackware 14.1
x86_64
php-5.6.36-x86_64-1

146685 - SuSE SLES 11 SP4 SUSE-SU-2018:1333-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2755, CVE-2018-2761, CVE-2018-2771, CVE-2018-2773, CVE-2018-2781, CVE-2018-2813, CVE-2018-2817, CVE-2018-2818, CVE-2018-2819

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1333-1

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-May/004064.html

SuSE SLES 11 SP4
i586
libmysql55client_r18-5.5.60-0.39.12.1
mysql-5.5.60-0.39.12.1
mysql-tools-5.5.60-0.39.12.1
libmysql55client18-5.5.60-0.39.12.1
mysql-client-5.5.60-0.39.12.1

x86_64
libmysql55client_r18-5.5.60-0.39.12.1
mysql-5.5.60-0.39.12.1
libmysql55client18-32bit-5.5.60-0.39.12.1
libmysql55client18-5.5.60-0.39.12.1
mysql-tools-5.5.60-0.39.12.1
libmysql55client_r18-32bit-5.5.60-0.39.12.1
mysql-client-5.5.60-0.39.12.1

146692 - SuSE Linux 42.3 openSUSE-SU-2018:1310-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000041

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1310-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00045.html

SuSE Linux 42.3
i586
typelib-1_0-Rsvg-2_0-2.40.20-15.1
gdk-pixbuf-loader-rsvg-2.40.20-15.1
rsvg-view-2.40.20-15.1
librsvg-2-2-debuginfo-2.40.20-15.1
rsvg-view-debuginfo-2.40.20-15.1
librsvg-debugsource-2.40.20-15.1
gdk-pixbuf-loader-rsvg-debuginfo-2.40.20-15.1
librsvg-2-2-2.40.20-15.1
librsvg-devel-2.40.20-15.1

noarch
rsvg-thumbnailer-2.40.20-15.1

x86_64
librsvg-debugsource-2.40.20-15.1
librsvg-2-2-2.40.20-15.1
librsvg-2-2-32bit-2.40.20-15.1
gdk-pixbuf-loader-rsvg-debuginfo-32bit-2.40.20-15.1
gdk-pixbuf-loader-rsvg-2.40.20-15.1
librsvg-2-2-debuginfo-2.40.20-15.1
librsvg-devel-2.40.20-15.1
gdk-pixbuf-loader-rsvg-32bit-2.40.20-15.1
librsvg-2-2-debuginfo-32bit-2.40.20-15.1
gdk-pixbuf-loader-rsvg-debuginfo-2.40.20-15.1
typelib-1_0-Rsvg-2_0-2.40.20-15.1
rsvg-view-2.40.20-15.1
rsvg-view-debuginfo-2.40.20-15.1

88945 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-136-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000300, CVE-2018-1000301

Description

The scan detected that the host is missing the following update:
SSA:2018-136-01

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.422028

Slackware 14.0
x86_64
curl-7.60.0-x86_64-1

Slackware 14.2
x86_64
curl-7.60.0-x86_64-1

i586
curl-7.60.0-i586-1

Slackware 14.1
x86_64
curl-7.60.0-x86_64-1

131111 - Debian Linux 9.0 DSA-4207-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1106

Description

The scan detected that the host is missing the following update:
DSA-4207-1

Observation

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

http://www.debian.org/security/2018/dsa-4207

Debian 9.0
all
packagekit_1.1.5-2+deb9u1

131112 - Debian Linux 9.0 DSA-4201-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10471, CVE-2018-10472, CVE-2018-10981, CVE-2018-10982, CVE-2018-8897

Description

The scan detected that the host is missing the following update:
DSA-4201-1

Observation

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

http://www.debian.org/security/2018/dsa-4201

Debian 9.0
all
xen-hypervisor-4.8-arm64_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
xen-system-arm64_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6

xen-hypervisor-4.8-armhf_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
xen-utils-4.8_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
xen-hypervisor-4.8-amd64_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
xen-utils-common_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
libxenstore3.0_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
xenstore-utils_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
libxen-4.8_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
xen-system-armhf_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
xen-system-amd64_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6
libxen-dev_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u6

131113 - Debian Linux 8.0, 9.0 DSA-4202-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000301

Description

The scan detected that the host is missing the following update:
DSA-4202-1

Observation

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

http://www.debian.org/security/2018/dsa-4202

Debian 8.0
all
curl_7.38.0-4+deb8u11

Debian 9.0
all
curl_7.52.1-5+deb9u6

146694 - SuSE SLES 11 SP4 SUSE-SU-2018:1322-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12613

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1322-1

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-May/004058.html

SuSE SLES 11 SP4
i586
libapr1-1.3.3-11.18.19.13.2

x86_64

libapr1-1.3.3-11.18.19.13.2

182698 - FreeBSD BIND Multiple Vulnerabilities (94599fe0-5ca3-11e8-8be1-d05099c0ae8c)

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

Risk Level: Low

CVE: CVE-2018-5736, CVE-2018-5737

Description

The scan detected that the host is missing the following update:
BIND -- multiple vulnerabilities (94599fe0-5ca3-11e8-8be1-d05099c0ae8c)

Observation

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

http://www.vuxml.org/freebsd/94599fe0-5ca3-11e8-8be1-d05099c0ae8c.html

Affected packages:
bind912 < 9.12.1P2

182699 - FreeBSD cURL Multiple Vulnerabilities (04fe6c8d-2a34-4009-a81e-e7a7e759b5d2)

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

Risk Level: Low

CVE: CVE-2018-1000300, CVE-2018-1000301

Description

The scan detected that the host is missing the following update:
cURL -- multiple vulnerabilities (04fe6c8d-2a34-4009-a81e-e7a7e759b5d2)

Observation

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

http://www.vuxml.org/freebsd/04fe6c8d-2a34-4009-a81e-e7a7e759b5d2.html

Affected packages:
curl < 7.60.0

186213 - Ubuntu Linux 14.04, 16.04, 17.10, 18.04 USN-3648-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000300, CVE-2018-1000301, CVE-2018-1000303

Description

The scan detected that the host is missing the following update:
USN-3648-1

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-May/004395.html

Ubuntu 16.04

libcurl3-nss_7.47.0-1ubuntu2.8
libcurl3_7.47.0-1ubuntu2.8
libcurl3-gnutls_7.47.0-1ubuntu2.8
curl_7.47.0-1ubuntu2.8

Ubuntu 14.04

libcurl3_7.35.0-1ubuntu2.16
libcurl3-gnutls_7.35.0-1ubuntu2.16
libcurl3-nss_7.35.0-1ubuntu2.16
curl_7.35.0-1ubuntu2.16

Ubuntu 18.04

curl_7.58.0-2ubuntu3.1
libcurl3-gnutls_7.58.0-2ubuntu3.1
libcurl3-nss_7.58.0-2ubuntu3.1
libcurl4_7.58.0-2ubuntu3.1

Ubuntu 17.10

libcurl3_7.55.1-1ubuntu2.5
libcurl3-nss_7.55.1-1ubuntu2.5
curl_7.55.1-1ubuntu2.5
libcurl3-gnutls_7.55.1-1ubuntu2.5

186218 - Ubuntu Linux 14.04, 16.04, 17.10, 18.04 USN-3645-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5150, CVE-2018-5151, CVE-2018-5152, CVE-2018-5153, CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158, CVE-2018-5159, CVE-2018-5160, CVE-2018-5163, CVE-2018-5164, CVE-2018-5166, CVE-2018-5167, CVE-2018-5168, CVE-2018-5169, CVE-2018-5172, CVE-2018-5173, CVE-2018-5175, CVE-2018-5176, CVE-2018-5177, CVE-2018-5180, CVE-2018-5181, CVE-2018-5182

Description

The scan detected that the host is missing the following update:
USN-3645-2

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-May/004398.html

Ubuntu 16.04

firefox_60.0.1+build2-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_60.0.1+build2-0ubuntu0.14.04.1

Ubuntu 18.04

firefox_60.0.1+build2-0ubuntu0.18.04.1

Ubuntu 17.10

firefox_60.0.1+build2-0ubuntu0.17.10.1

186220 - Ubuntu Linux 17.10 USN-3642-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1059

Description

The scan detected that the host is missing the following update:
USN-3642-2

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-May/004396.html

Ubuntu 17.10

dpdk_17.05.2-0ubuntu1.1

186221 - Ubuntu Linux 18.04 USN-3652-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
USN-3652-1

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-May/004401.html

Ubuntu 18.04

linux-image-oem_4.15.0.1006.8
linux-image-4.15.0-1008-gcp_4.15.0-1008.8
linux-image-4.15.0-1010-kvm_4.15.0-1010.10
linux-image-kvm_4.15.0.1010.10
linux-image-generic-lpae_4.15.0.22.23
linux-image-4.15.0-22-generic_4.15.0-22.24
linux-image-gcp_4.15.0.1008.10
linux-image-azure_4.15.0.1012.12
linux-image-azure-edge_4.15.0.1012.12
linux-image-gke_4.15.0.1008.10
linux-image-lowlatency_4.15.0.22.23

linux-image-4.15.0-22-lowlatency_4.15.0-22.24
linux-image-4.15.0-22-generic-lpae_4.15.0-22.24
linux-image-generic_4.15.0.22.23
linux-image-4.15.0-1009-aws_4.15.0-1009.9
linux-image-aws_4.15.0.1009.9

193708 - Fedora Linux 27 FEDORA-2018-937c789f2a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15097, CVE-2018-1115

Description

The scan detected that the host is missing the following update:
FEDORA-2018-937c789f2a

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/2018/5/?count=200&page=1

Fedora Core 27

postgresql-9.6.9-1.fc27

193709 - Fedora Linux 28 FEDORA-2018-d3b44e5574 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10528, CVE-2018-10529

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d3b44e5574

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/2018/5/?count=200&page=3

Fedora Core 28

mingw-LibRaw-0.18.10-1.fc28

193710 - Fedora Linux 27 FEDORA-2018-0e6e400e7a 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-2018-0e6e400e7a

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/2018/5/?count=200&page=3

Fedora Core 27

seamonkey-2.49.3-1.fc27

193711 - Fedora Linux 28 FEDORA-2018-264d881a62 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-2018-264d881a62

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/2018/5/?count=200&page=1

Fedora Core 28

glibc-2.27-14.fc28

193712 - Fedora Linux 27 FEDORA-2018-e4c2507720 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10237

Description

The scan detected that the host is missing the following update:
FEDORA-2018-e4c2507720

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/2018/5/?count=200&page=2

Fedora Core 27

guava-18.0-12.fc27

193713 - Fedora Linux 28 FEDORA-2018-bba8fed5ab Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1124, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
FEDORA-2018-bba8fed5ab

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/2018/5/?count=200&page=1

Fedora Core 28

procps-ng-3.3.12-2.fc28

193715 - Fedora Linux 27 FEDORA-2018-46f3f13c68 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10733, CVE-2018-10767

Description

The scan detected that the host is missing the following update:
FEDORA-2018-46f3f13c68

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/2018/5/?count=200&page=3

Fedora Core 27

libgxps-0.3.0-4.fc27

193717 - Fedora Linux 26 FEDORA-2018-5392896132 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1111

Description

The scan detected that the host is missing the following update:
FEDORA-2018-5392896132

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/2018/5/?count=200&page=3

Fedora Core 26

dhcp-4.3.5-11.fc26

193718 - Fedora Linux 28 FEDORA-2018-630ecbb116 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-2018-630ecbb116

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/2018/5/?count=200&page=2

Fedora Core 28

love-0.10.2-12.fc28

193720 - Fedora Linux 26 FEDORA-2018-bd6f9237b5 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15097, CVE-2018-1115

Description

The scan detected that the host is missing the following update:
FEDORA-2018-bd6f9237b5

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/2018/5/?count=200&page=1

Fedora Core 26

postgresql-9.6.9-1.fc26

193721 - Fedora Linux 27 FEDORA-2018-ccb2cc96be Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10528, CVE-2018-10529

Description

The scan detected that the host is missing the following update:
FEDORA-2018-ccb2cc96be

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/2018/5/?count=200&page=3

Fedora Core 27

mingw-LibRaw-0.18.10-1.fc27

193722 - Fedora Linux 28 FEDORA-2018-fa01002d7e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000300, CVE-2018-1000301

Description

The scan detected that the host is missing the following update:
FEDORA-2018-fa01002d7e

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/2018/5/?count=200&page=1

Fedora Core 28

curl-7.59.0-3.fc28

193725 - Fedora Linux 28 FEDORA-2018-efd98d9a58 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-18266

Description

The scan detected that the host is missing the following update:
FEDORA-2018-efd98d9a58

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/2018/5/?count=200&page=2

Fedora Core 28

xdg-utils-1.1.3-1.fc28

193726 - Fedora Linux 26 FEDORA-2018-6a9fea1b3a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-4200

Description

The scan detected that the host is missing the following update:
FEDORA-2018-6a9fea1b3a

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/2018/5/?count=200&page=1

Fedora Core 26

webkitgtk4-2.20.2-1.fc26

193729 - Fedora Linux 27 FEDORA-2018-b753813bf0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-18266

Description

The scan detected that the host is missing the following update:
FEDORA-2018-b753813bf0

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/2018/5/?count=200&page=2

Fedora Core 27

xdg-utils-1.1.3-1.fc27

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.

146238 - SuSE Linux 42.3 openSUSE-SU-2018:0060-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0359

Update Details

Risk is updated

182290 - FreeBSD diffoscope Arbitrary File Write (077bbadf-f2f4-11e6-92a7-902b34361349)

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

Risk Level: High

CVE: CVE-2017-0359

Update Details

Risk is updated

191769 - Fedora Linux 25 FEDORA-2017-101722eb25 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0359

Update Details

Risk is updated

191770 - Fedora Linux 24 FEDORA-2017-33cb46c6b0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0359

Update Details

Risk is updated

23589 - (APSB18-09) Vulnerabilities In Adobe Acrobat And Reader

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

Risk Level: High

CVE: CVE-2018-4947, CVE-2018-4948, CVE-2018-4949, CVE-2018-4950, CVE-2018-4951, CVE-2018-4952, CVE-2018-4953, CVE-2018-4954, CVE-2018-4955, CVE-2018-4956, CVE-2018-4957, CVE-2018-4958, CVE-2018-4959, CVE-2018-4960, CVE-2018-4961, CVE-2018-4962, CVE-2018-4963, CVE-2018-4964, CVE-2018-4965, CVE-2018-4966, CVE-2018-4967, CVE-2018-4968, CVE-2018-4969, CVE-2018-4970, CVE-2018-4971, CVE-2018-4972, CVE-2018-4973, CVE-2018-4974, CVE-2018-4975, CVE-2018-4976, CVE-2018-4977, CVE-2018-4978, CVE-2018-4979, CVE-2018-4980, CVE-2018-4981, CVE-2018-4982, CVE-2018-4983, CVE-2018-4984, CVE-2018-4985, CVE-2018-4986, CVE-2018-4987, CVE-2018-4988, CVE-2018-4989, CVE-2018-4990, CVE-2018-4993

Update Details

CVE is updated

32097 - Oracle Solaris 125358-27 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0689, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620, CVE-2013-1739, CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1490, CVE-2014-1491, CVE-2014-1492

Update Details

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

32098 - Oracle Solaris 125359-27 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0689, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620, CVE-2013-1739, CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1490, CVE-2014-1491, CVE-2014-1492

Update Details

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

33207 - Oracle Solaris 119213-37 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0689, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620, CVE-2013-1739, CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1490, CVE-2014-1491, CVE-2014-1492

Update Details

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

33218 - Oracle Solaris 119214-37 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0689, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620, CVE-2013-1739, CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1490, CVE-2014-1491, CVE-2014-1492

Update Details

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

32575 - Oracle Solaris 143506-13 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-1634, CVE-2010-3492, CVE-2011-3389, CVE-2012-0845, CVE-2012-0876, CVE-2012-1150, CVE-2013-4238, CVE-2014-1912, CVE-2014-7185

Update Details

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

32576 - Oracle Solaris 143507-13 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-1634, CVE-2010-3492, CVE-2011-3389, CVE-2012-0845, CVE-2012-0876, CVE-2012-1150, CVE-2013-4238, CVE-2014-1912, CVE-2014-7185

Update Details

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

130694 - Debian Linux 8.0 DSA-3780-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0358

Update Details

Risk is updated

131078 - Debian Linux 8.0, 9.0 DSA-4172-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-6797, CVE-2018-6798, CVE-2018-6913

Update Details
Risk is updated

131082 - Debian Linux 9.0 DSA-4174-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-1084

Update Details
Risk is updated

141945 - Red Hat Enterprise Linux RHSA-2018-1192 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-6797, CVE-2018-6798

Update Details
Risk is updated

178409 - Gentoo Linux GLSA-201702-10 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: High
CVE: CVE-2017-0358

Update Details
Risk is updated

182297 - FreeBSD ikiwiki Authentication Bypass Vulnerability (7b35a77a-0151-11e7-ae1b-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-0356

Update Details
Risk is updated

182363 - FreeBSD FreeBSD Ipfilter (4) fragment handling panic (51d1282d-420e-11e7-82c5-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-1081

Update Details

Risk is updated

182677 - FreeBSD perl Multiple Vulnerabilities (41c96ffd-29a6-4dcc-9a88-65f5038fa6eb)

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

Risk Level: High

CVE: CVE-2018-6797, CVE-2018-6798, CVE-2018-6913

Update Details

Risk is updated

185568 - Ubuntu Linux 16.04, 16.10 USN-3186-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0357

Update Details

Risk is updated

185571 - Ubuntu Linux 16.04, 16.10 USN-3182-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0358

Update Details

Risk is updated

192116 - Fedora Linux 25 FEDORA-2017-2643ef1cad Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0372

Update Details

Risk is updated

193522 - Fedora Linux 28 FEDORA-2018-c40addbe0d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1002150

Update Details

Risk is updated

193549 - Fedora Linux 27 FEDORA-2018-f61d8bdd42 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2018-1002150

Update Details
Risk is updated

193576 - Fedora Linux 28 FEDORA-2018-12da088117 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-1084

Update Details
Risk is updated

193577 - Fedora Linux 26 FEDORA-2018-81d3af3f36 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-1002150

Update Details
Risk is updated

193587 - Fedora Linux 27 FEDORA-2018-b0253649be Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-1084

Update Details
Risk is updated

193588 - Fedora Linux 27 FEDORA-2018-1c8b49fbc7 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-6797, CVE-2018-6798, CVE-2018-6913

Update Details
Risk is updated

193597 - Fedora Linux 26 FEDORA-2018-d87e29047d Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-1084

Update Details
Risk is updated

193624 - Fedora Linux 26 FEDORA-2018-0050f7c0d1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-6797, CVE-2018-6798, CVE-2018-6913

Update Details
Risk is updated

193698 - Fedora Linux 28 FEDORA-2018-d1ba58394e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-6797, CVE-2018-6798, CVE-2018-6913

Update Details
Risk is updated

131063 - Debian Linux 9.0 DSA-4159-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-0493

Update Details
Risk is updated

131085 - Debian Linux 8.0, 9.0 DSA-4178-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-10119, CVE-2018-10120

Update Details
Risk is updated

146614 - SuSE Linux 42.3 openSUSE-SU-2018:1058-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-10188

Update Details
Risk is updated

146620 - SuSE Linux 42.3 openSUSE-SU-2018:1038-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-3848, CVE-2018-3849

Update Details

Risk is updated

146677 - SuSE SLED 12 SP3 SUSE-SU-2018:1296-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10119, CVE-2018-10120

Update Details

Risk is updated

170783 - Amazon Linux AMI ALAS-2017-806 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9586

Update Details

Risk is updated

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

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

Risk Level: Medium

CVE: CVE-2016-9586

Update Details

Risk is updated

182479 - FreeBSD xorg-server Multiple Issues (ab881a74-c016-4e6d-9f7d-68c8e7cedafb)

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

Risk Level: Medium

CVE: CVE-2017-10971, CVE-2017-10972

Update Details

FASLScript is updated

182662 - FreeBSD moodle Multiple Vulnerabilities (cdb4d962-34f9-11e8-92db-080027907385)

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

Risk Level: Medium

CVE: CVE-2018-1081, CVE-2018-1082

Update Details

Risk is updated

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

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

Risk Level: Medium
CVE: CVE-2016-9586

Update Details
Risk is updated

191568 - Fedora Linux 24 FEDORA-2016-86d2b5aefb Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9586

Update Details
Risk is updated

193603 - Fedora Linux 27 FEDORA-2018-3247413570 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-10194

Update Details
Risk is updated

193608 - Fedora Linux 28 FEDORA-2018-e048a4ef13 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1088

Update Details
Risk is updated

193623 - Fedora Linux 28 FEDORA-2018-b4ef545db5 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-9918

Update Details
Risk is updated

193625 - Fedora Linux 27 FEDORA-2018-6dc9145693 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1088

Update Details
Risk is updated

193626 - Fedora Linux 28 FEDORA-2018-8359498f3c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10194

Update Details

Risk is updated

193627 - Fedora Linux 26 FEDORA-2018-226dac231f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10194

Update Details

Risk is updated

193652 - Fedora Linux 26 FEDORA-2018-f9e0f1caf7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1088

Update Details

Risk is updated

22135 - (SYM17-005) Symantec Management Console XSS/XXE Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-6322, CVE-2017-6323

Update Details

Risk is updated

131080 - Debian Linux 9.0 DSA-4169-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1086

Update Details

Risk is updated

131094 - Debian Linux 8.0 DSA-4186-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000164

Update Details

Risk is updated

131102 - Debian Linux 8.0, 9.0 DSA-4193-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10100, CVE-2018-10101, CVE-2018-10102

Update Details

Risk is updated

146596 - SuSE Linux 42.3 openSUSE-SU-2018:0965-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000164

Update Details

Risk is updated

193570 - Fedora Linux 28 FEDORA-2018-bbfb0f5bc9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1079, CVE-2018-1086

Update Details

Risk is updated

193584 - Fedora Linux 26 FEDORA-2018-ce5d7106d8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1079, CVE-2018-1086

Update Details

Risk is updated

193600 - Fedora Linux 27 FEDORA-2018-57bbe74c6c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1079, CVE-2018-1086

Update Details

Risk is updated

131062 - Debian Linux 8.0, 9.0 DSA-4163-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2018-0492

Update Details
Risk is updated

170960 - Amazon Linux AMI ALAS-2018-1000 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-0737

Update Details
Risk is updated

182671 - FreeBSD OpenSSL Cache Timing Vulnerability (8f353420-4197-11e8-8777-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-0737

Update Details
Risk is updated

187539 - Fedora Linux 19 FEDORA-2014-0508 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-1398, CVE-2014-1399, CVE-2014-1400

Update Details
Risk is updated

187544 - Fedora Linux 20 FEDORA-2014-0509 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-1398, CVE-2014-1399, CVE-2014-1400

Update Details
Risk is updated

182014 - FreeBSD tiff Buffer Overflow (0ab66088-4aa5-11e6-a7bd-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-5314, CVE-2016-5320, CVE-2016-5875

Update Details
CVE is updated

146647 - SuSE SLES 11 SP4 SUSE-SU-2018:1171-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10124, CVE-2018-1087, CVE-2018-8897

Update Details

Risk is updated

70014 - netbios-helpers.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70019 - version.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70046 - macosx.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70087 - hp.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.