2018-JAN-05
FSL version 7.5.991

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

163516 - Oracle Enterprise Linux ELSA-2018-0008 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11176, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7542, CVE-2017-9074

Description

The scan detected that the host is missing the following update:
ELSA-2018-0008

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007436.html

OEL6
x86_64
kernel-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-doc-2.6.32-696.18.7.el6
kernel-devel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-firmware-2.6.32-696.18.7.el6
kernel-abi-whitelists-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6

i386
kernel-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-doc-2.6.32-696.18.7.el6
kernel-devel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-firmware-2.6.32-696.18.7.el6
kernel-abi-whitelists-2.6.32-696.18.7.el6

170916 - Amazon Linux AMI ALAS-2018-939 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
ALAS-2018-939

Observation

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

https://alas.aws.amazon.com/ALAS-2018-939.html

Amazon Linux AMI
i686
kernel-headers-4.9.70-25.242.amzn1

noarch
kernel-doc-4.9.70-25.242.amzn1

x86_64
kernel-4.9.70-25.242.amzn1
kernel-debuginfo-common-x86_64-4.9.70-25.242.amzn1
kernel-tools-devel-4.9.70-25.242.amzn1
kernel-devel-4.9.70-25.242.amzn1
kernel-debuginfo-4.9.70-25.242.amzn1
kernel-tools-debuginfo-4.9.70-25.242.amzn1
kernel-headers-4.9.70-25.242.amzn1
kernel-tools-4.9.70-25.242.amzn1
perf-4.9.70-25.242.amzn1
perf-debuginfo-4.9.70-25.242.amzn1

132422 - Oracle VM OVMSA-2018-0002 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16525, CVE-2017-16526, CVE-2017-16529, CVE-2017-16530, CVE-2017-16531, CVE-2017-16533, CVE-2017-16535, CVE-2017-16536

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0002

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000811.html

OVM3.4
x86_64
kernel-uek-4.1.12-112.14.2.el6uek
kernel-uek-firmware-4.1.12-112.14.2.el6uek

141811 - Red Hat Enterprise Linux RHSA-2018-0011 Update Is Not Installed

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

Risk Level: High

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

Description

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

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00006.html

RHEL6_7S
i386
kernel-debug-2.6.32-573.49.3.el6
python-perf-2.6.32-573.49.3.el6
perf-debuginfo-2.6.32-573.49.3.el6
kernel-debuginfo-common-i686-2.6.32-573.49.3.el6
kernel-devel-2.6.32-573.49.3.el6
kernel-2.6.32-573.49.3.el6
kernel-debug-devel-2.6.32-573.49.3.el6
perf-2.6.32-573.49.3.el6
kernel-headers-2.6.32-573.49.3.el6
python-perf-debuginfo-2.6.32-573.49.3.el6
kernel-debuginfo-2.6.32-573.49.3.el6
kernel-debug-debuginfo-2.6.32-573.49.3.el6

noarch
kernel-abi-whitelists-2.6.32-573.49.3.el6
kernel-firmware-2.6.32-573.49.3.el6
kernel-doc-2.6.32-573.49.3.el6

x86_64
kernel-headers-2.6.32-573.49.3.el6
python-perf-2.6.32-573.49.3.el6
kernel-debuginfo-common-i686-2.6.32-573.49.3.el6
kernel-debuginfo-2.6.32-573.49.3.el6
kernel-debug-2.6.32-573.49.3.el6
kernel-2.6.32-573.49.3.el6
kernel-debuginfo-common-x86_64-2.6.32-573.49.3.el6
kernel-devel-2.6.32-573.49.3.el6
perf-2.6.32-573.49.3.el6
perf-debuginfo-2.6.32-573.49.3.el6
kernel-debug-devel-2.6.32-573.49.3.el6
kernel-debug-debuginfo-2.6.32-573.49.3.el6
python-perf-debuginfo-2.6.32-573.49.3.el6

141812 - Red Hat Enterprise Linux RHSA-2018-0020 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0020

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00016.html

RHEL6_2S
x86_64
kernel-debug-debuginfo-2.6.32-220.76.2.el6
kernel-debug-devel-2.6.32-220.76.2.el6
kernel-devel-2.6.32-220.76.2.el6
kernel-debuginfo-2.6.32-220.76.2.el6
python-perf-debuginfo-2.6.32-220.76.2.el6
perf-2.6.32-220.76.2.el6
kernel-debuginfo-common-x86_64-2.6.32-220.76.2.el6
kernel-2.6.32-220.76.2.el6
kernel-headers-2.6.32-220.76.2.el6
kernel-debug-2.6.32-220.76.2.el6
python-perf-2.6.32-220.76.2.el6
perf-debuginfo-2.6.32-220.76.2.el6

noarch
kernel-firmware-2.6.32-220.76.2.el6
kernel-doc-2.6.32-220.76.2.el6

141813 - Red Hat Enterprise Linux RHSA-2018-0027 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0027

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00021.html

RHEL7_3S
x86_64
qemu-kvm-1.5.3-126.el7_3.13
qemu-img-1.5.3-126.el7_3.13
qemu-kvm-common-1.5.3-126.el7_3.13
qemu-kvm-debuginfo-1.5.3-126.el7_3.13
qemu-kvm-tools-1.5.3-126.el7_3.13

141814 - Red Hat Enterprise Linux RHSA-2018-0037 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0037

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00032.html

RHEL6_6S
x86_64
microcode_ctl-1.17-19.1.el6_6
microcode_ctl-debuginfo-1.17-19.1.el6_6

141815 - Red Hat Enterprise Linux RHSA-2018-0007 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0007

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00008.html

RHEL7D
x86_64
kernel-debuginfo-3.10.0-693.11.6.el7
perf-debuginfo-3.10.0-693.11.6.el7
kernel-tools-libs-devel-3.10.0-693.11.6.el7
kernel-3.10.0-693.11.6.el7
python-perf-debuginfo-3.10.0-693.11.6.el7
python-perf-3.10.0-693.11.6.el7
kernel-headers-3.10.0-693.11.6.el7
kernel-tools-libs-3.10.0-693.11.6.el7
kernel-debuginfo-common-x86_64-3.10.0-693.11.6.el7
kernel-devel-3.10.0-693.11.6.el7
kernel-tools-debuginfo-3.10.0-693.11.6.el7
kernel-tools-3.10.0-693.11.6.el7
kernel-debug-3.10.0-693.11.6.el7
kernel-debug-debuginfo-3.10.0-693.11.6.el7
kernel-debug-devel-3.10.0-693.11.6.el7
perf-3.10.0-693.11.6.el7

noarch
kernel-abi-whitelists-3.10.0-693.11.6.el7
kernel-doc-3.10.0-693.11.6.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-693.11.6.el7
kernel-doc-3.10.0-693.11.6.el7

x86_64
kernel-debuginfo-3.10.0-693.11.6.el7
perf-debuginfo-3.10.0-693.11.6.el7
kernel-tools-libs-devel-3.10.0-693.11.6.el7
kernel-3.10.0-693.11.6.el7
python-perf-debuginfo-3.10.0-693.11.6.el7
python-perf-3.10.0-693.11.6.el7
kernel-headers-3.10.0-693.11.6.el7
kernel-tools-libs-3.10.0-693.11.6.el7
kernel-debuginfo-common-x86_64-3.10.0-693.11.6.el7
kernel-devel-3.10.0-693.11.6.el7
kernel-tools-debuginfo-3.10.0-693.11.6.el7
kernel-tools-3.10.0-693.11.6.el7
kernel-debug-3.10.0-693.11.6.el7
kernel-debug-debuginfo-3.10.0-693.11.6.el7
kernel-debug-devel-3.10.0-693.11.6.el7
perf-3.10.0-693.11.6.el7

RHEL7WS
x86_64
kernel-debuginfo-3.10.0-693.11.6.el7
perf-debuginfo-3.10.0-693.11.6.el7
kernel-tools-libs-devel-3.10.0-693.11.6.el7
kernel-3.10.0-693.11.6.el7
python-perf-debuginfo-3.10.0-693.11.6.el7
python-perf-3.10.0-693.11.6.el7
kernel-headers-3.10.0-693.11.6.el7
kernel-tools-libs-3.10.0-693.11.6.el7
kernel-debuginfo-common-x86_64-3.10.0-693.11.6.el7
kernel-devel-3.10.0-693.11.6.el7
kernel-tools-debuginfo-3.10.0-693.11.6.el7
kernel-tools-3.10.0-693.11.6.el7
kernel-debug-3.10.0-693.11.6.el7
kernel-debug-debuginfo-3.10.0-693.11.6.el7
kernel-debug-devel-3.10.0-693.11.6.el7
perf-3.10.0-693.11.6.el7

noarch
kernel-abi-whitelists-3.10.0-693.11.6.el7
kernel-doc-3.10.0-693.11.6.el7

141816 - Red Hat Enterprise Linux RHSA-2018-0017 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0017

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00014.html

RHEL6_6S

x86_64
kernel-debug-debuginfo-2.6.32-504.64.4.el6
python-perf-debuginfo-2.6.32-504.64.4.el6
kernel-debuginfo-common-x86_64-2.6.32-504.64.4.el6
kernel-debuginfo-2.6.32-504.64.4.el6
kernel-headers-2.6.32-504.64.4.el6
python-perf-2.6.32-504.64.4.el6
kernel-debug-devel-2.6.32-504.64.4.el6
perf-2.6.32-504.64.4.el6
kernel-debug-2.6.32-504.64.4.el6
kernel-devel-2.6.32-504.64.4.el6
perf-debuginfo-2.6.32-504.64.4.el6
kernel-2.6.32-504.64.4.el6

noarch
kernel-abi-whitelists-2.6.32-504.64.4.el6
kernel-firmware-2.6.32-504.64.4.el6
kernel-doc-2.6.32-504.64.4.el6

141817 - Red Hat Enterprise Linux RHSA-2018-0008 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0008

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00007.html

RHEL6D
i386
kernel-devel-2.6.32-696.18.7.el6
perf-debuginfo-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6
kernel-debuginfo-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
python-perf-debuginfo-2.6.32-696.18.7.el6
kernel-debug-debuginfo-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-debuginfo-common-i686-2.6.32-696.18.7.el6

noarch
kernel-doc-2.6.32-696.18.7.el6
kernel-firmware-2.6.32-696.18.7.el6
kernel-abi-whitelists-2.6.32-696.18.7.el6

x86_64
kernel-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6

kernel-debug-2.6.32-696.18.7.el6
python-perf-debuginfo-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
perf-debuginfo-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6
kernel-debuginfo-2.6.32-696.18.7.el6
kernel-debug-debuginfo-2.6.32-696.18.7.el6
kernel-debuginfo-common-i686-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-devel-2.6.32-696.18.7.el6
kernel-debuginfo-common-x86_64-2.6.32-696.18.7.el6

RHEL6S
i386
kernel-devel-2.6.32-696.18.7.el6
perf-debuginfo-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6
kernel-debuginfo-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
python-perf-debuginfo-2.6.32-696.18.7.el6
kernel-debug-debuginfo-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-debuginfo-common-i686-2.6.32-696.18.7.el6

noarch
kernel-doc-2.6.32-696.18.7.el6
kernel-firmware-2.6.32-696.18.7.el6
kernel-abi-whitelists-2.6.32-696.18.7.el6

x86_64
kernel-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
python-perf-debuginfo-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
perf-debuginfo-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6
kernel-debuginfo-2.6.32-696.18.7.el6
kernel-debug-debuginfo-2.6.32-696.18.7.el6
kernel-debuginfo-common-i686-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-devel-2.6.32-696.18.7.el6
kernel-debuginfo-common-x86_64-2.6.32-696.18.7.el6

RHEL6WS
i386
kernel-devel-2.6.32-696.18.7.el6
perf-debuginfo-2.6.32-696.18.7.el6
kernel-debuginfo-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
python-perf-debuginfo-2.6.32-696.18.7.el6
kernel-debug-debuginfo-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-debuginfo-common-i686-2.6.32-696.18.7.el6

noarch
kernel-doc-2.6.32-696.18.7.el6
kernel-firmware-2.6.32-696.18.7.el6
kernel-abi-whitelists-2.6.32-696.18.7.el6

x86_64
kernel-devel-2.6.32-696.18.7.el6
perf-debuginfo-2.6.32-696.18.7.el6
kernel-debuginfo-2.6.32-696.18.7.el6
kernel-debuginfo-common-x86_64-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
python-perf-debuginfo-2.6.32-696.18.7.el6
kernel-debug-debuginfo-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-debuginfo-common-i686-2.6.32-696.18.7.el6

141818 - Red Hat Enterprise Linux RHSA-2018-0023 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0023

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00023.html

RHEL7D
x86_64
qemu-kvm-common-1.5.3-141.el7_4.6
qemu-kvm-tools-1.5.3-141.el7_4.6
qemu-img-1.5.3-141.el7_4.6
qemu-kvm-1.5.3-141.el7_4.6
qemu-kvm-debuginfo-1.5.3-141.el7_4.6

RHEL7S
x86_64
qemu-kvm-common-1.5.3-141.el7_4.6
qemu-kvm-tools-1.5.3-141.el7_4.6
qemu-img-1.5.3-141.el7_4.6
qemu-kvm-1.5.3-141.el7_4.6
qemu-kvm-debuginfo-1.5.3-141.el7_4.6

RHEL7WS
x86_64
qemu-kvm-common-1.5.3-141.el7_4.6
qemu-kvm-tools-1.5.3-141.el7_4.6
qemu-img-1.5.3-141.el7_4.6
qemu-kvm-1.5.3-141.el7_4.6
qemu-kvm-debuginfo-1.5.3-141.el7_4.6

141819 - Red Hat Enterprise Linux RHSA-2018-0012 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

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

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00010.html

RHEL7D
x86_64
microcode_ctl-debuginfo-2.1-22.2.el7
microcode_ctl-2.1-22.2.el7

RHEL7S
x86_64
microcode_ctl-debuginfo-2.1-22.2.el7
microcode_ctl-2.1-22.2.el7

RHEL7WS
x86_64
microcode_ctl-debuginfo-2.1-22.2.el7
microcode_ctl-2.1-22.2.el7

141820 - Red Hat Enterprise Linux RHSA-2018-0013 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

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

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00009.html

RHEL6D
x86_64
microcode_ctl-1.17-25.2.el6_9
microcode_ctl-debuginfo-1.17-25.2.el6_9

i386
microcode_ctl-1.17-25.2.el6_9
microcode_ctl-debuginfo-1.17-25.2.el6_9

RHEL6S
x86_64
microcode_ctl-1.17-25.2.el6_9
microcode_ctl-debuginfo-1.17-25.2.el6_9

i386
microcode_ctl-1.17-25.2.el6_9
microcode_ctl-debuginfo-1.17-25.2.el6_9

RHEL6WS
x86_64
microcode_ctl-1.17-25.2.el6_9
microcode_ctl-debuginfo-1.17-25.2.el6_9

i386
microcode_ctl-1.17-25.2.el6_9
microcode_ctl-debuginfo-1.17-25.2.el6_9

141821 - Red Hat Enterprise Linux RHSA-2018-0015 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0015

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00011.html

RHEL7_3S
noarch
iwl7260-firmware-22.0.7.0-50.el7_3
iwl6000g2a-firmware-17.168.5.3-50.el7_3
iwl4965-firmware-228.61.2.24-50.el7_3
iwl3160-firmware-22.0.7.0-50.el7_3
iwl6050-firmware-41.28.5.1-50.el7_3
iwl105-firmware-18.168.6.1-50.el7_3
linux-firmware-20160830-50.git7534e19.el7_3
iwl7265-firmware-22.0.7.0-50.el7_3
iwl2030-firmware-18.168.6.1-50.el7_3
iwl2000-firmware-18.168.6.1-50.el7_3
iwl3945-firmware-15.32.2.9-50.el7_3
iwl135-firmware-18.168.6.1-50.el7_3
iwl100-firmware-39.31.5.1-50.el7_3
iwl6000g2b-firmware-17.168.5.2-50.el7_3
iwl6000-firmware-9.221.4.1-50.el7_3
iwl5150-firmware-8.24.2.2-50.el7_3
iwl5000-firmware-8.83.5.1_1-50.el7_3
iwl1000-firmware-39.31.5.1-50.el7_3

141822 - Red Hat Enterprise Linux RHSA-2018-0029 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0029

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00034.html

RHEL7D
x86_64
libvirt-daemon-driver-storage-iscsi-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-rbd-3.2.0-14.el7_4.7
libvirt-lock-sanlock-3.2.0-14.el7_4.7
libvirt-daemon-config-nwfilter-3.2.0-14.el7_4.7
libvirt-docs-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-gluster-3.2.0-14.el7_4.7
libvirt-daemon-driver-secret-3.2.0-14.el7_4.7
libvirt-daemon-driver-nwfilter-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-core-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-scsi-3.2.0-14.el7_4.7
libvirt-daemon-config-network-3.2.0-14.el7_4.7
libvirt-daemon-driver-qemu-3.2.0-14.el7_4.7
libvirt-daemon-driver-interface-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-disk-3.2.0-14.el7_4.7
libvirt-daemon-driver-network-3.2.0-14.el7_4.7
libvirt-nss-3.2.0-14.el7_4.7
libvirt-debuginfo-3.2.0-14.el7_4.7
libvirt-libs-3.2.0-14.el7_4.7
libvirt-daemon-driver-lxc-3.2.0-14.el7_4.7
libvirt-admin-3.2.0-14.el7_4.7
libvirt-login-shell-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-mpath-3.2.0-14.el7_4.7
libvirt-devel-3.2.0-14.el7_4.7
libvirt-client-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-logical-3.2.0-14.el7_4.7
libvirt-daemon-driver-nodedev-3.2.0-14.el7_4.7
libvirt-daemon-3.2.0-14.el7_4.7
libvirt-daemon-lxc-3.2.0-14.el7_4.7
libvirt-daemon-kvm-3.2.0-14.el7_4.7
libvirt-3.2.0-14.el7_4.7

RHEL7S
x86_64
libvirt-daemon-driver-storage-iscsi-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-rbd-3.2.0-14.el7_4.7
libvirt-lock-sanlock-3.2.0-14.el7_4.7
libvirt-daemon-config-nwfilter-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-gluster-3.2.0-14.el7_4.7
libvirt-daemon-driver-secret-3.2.0-14.el7_4.7
libvirt-daemon-driver-nwfilter-3.2.0-14.el7_4.7
libvirt-docs-3.2.0-14.el7_4.7

libvirt-daemon-driver-storage-scsi-3.2.0-14.el7_4.7
libvirt-daemon-config-network-3.2.0-14.el7_4.7
libvirt-daemon-driver-qemu-3.2.0-14.el7_4.7
libvirt-daemon-driver-interface-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-disk-3.2.0-14.el7_4.7
libvirt-daemon-driver-network-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-core-3.2.0-14.el7_4.7
libvirt-nss-3.2.0-14.el7_4.7
libvirt-debuginfo-3.2.0-14.el7_4.7
libvirt-libs-3.2.0-14.el7_4.7
libvirt-daemon-driver-lxc-3.2.0-14.el7_4.7
libvirt-admin-3.2.0-14.el7_4.7
libvirt-login-shell-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-mpath-3.2.0-14.el7_4.7
libvirt-devel-3.2.0-14.el7_4.7
libvirt-client-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-logical-3.2.0-14.el7_4.7
libvirt-daemon-driver-nodedev-3.2.0-14.el7_4.7
libvirt-daemon-3.2.0-14.el7_4.7
libvirt-daemon-lxc-3.2.0-14.el7_4.7
libvirt-daemon-kvm-3.2.0-14.el7_4.7
libvirt-3.2.0-14.el7_4.7

RHEL7WS
x86_64
libvirt-daemon-driver-storage-iscsi-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-rbd-3.2.0-14.el7_4.7
libvirt-lock-sanlock-3.2.0-14.el7_4.7
libvirt-daemon-config-nwfilter-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-gluster-3.2.0-14.el7_4.7
libvirt-daemon-driver-secret-3.2.0-14.el7_4.7
libvirt-daemon-driver-nwfilter-3.2.0-14.el7_4.7
libvirt-docs-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-scsi-3.2.0-14.el7_4.7
libvirt-daemon-config-network-3.2.0-14.el7_4.7
libvirt-daemon-driver-qemu-3.2.0-14.el7_4.7
libvirt-daemon-driver-interface-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-disk-3.2.0-14.el7_4.7
libvirt-daemon-driver-network-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-core-3.2.0-14.el7_4.7
libvirt-nss-3.2.0-14.el7_4.7
libvirt-debuginfo-3.2.0-14.el7_4.7
libvirt-libs-3.2.0-14.el7_4.7
libvirt-daemon-driver-lxc-3.2.0-14.el7_4.7
libvirt-admin-3.2.0-14.el7_4.7
libvirt-login-shell-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-mpath-3.2.0-14.el7_4.7
libvirt-devel-3.2.0-14.el7_4.7
libvirt-client-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-logical-3.2.0-14.el7_4.7
libvirt-daemon-driver-nodedev-3.2.0-14.el7_4.7
libvirt-daemon-3.2.0-14.el7_4.7
libvirt-daemon-lxc-3.2.0-14.el7_4.7
libvirt-daemon-kvm-3.2.0-14.el7_4.7
libvirt-3.2.0-14.el7_4.7

141823 - Red Hat Enterprise Linux RHSA-2018-0039 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0039

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00029.html

RHEL6_2S
x86_64
microcode_ctl-1.17-9.1.el6_2
microcode_ctl-debuginfo-1.17-9.1.el6_2

141824 - Red Hat Enterprise Linux RHSA-2018-0036 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0036

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00033.html

RHEL6_7S
x86_64
microcode_ctl-debuginfo-1.17-20.1.el6_7
microcode_ctl-1.17-20.1.el6_7

i386
microcode_ctl-debuginfo-1.17-20.1.el6_7
microcode_ctl-1.17-20.1.el6_7

141825 - Red Hat Enterprise Linux RHSA-2018-0024 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0024

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00024.html

RHEL6D
x86_64
qemu-guest-agent-0.12.1.2-2.503.el6_9.4
qemu-kvm-tools-0.12.1.2-2.503.el6_9.4
qemu-img-0.12.1.2-2.503.el6_9.4
qemu-kvm-0.12.1.2-2.503.el6_9.4
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.4

i386
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.4
qemu-guest-agent-0.12.1.2-2.503.el6_9.4

RHEL6S
i386
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.4
qemu-guest-agent-0.12.1.2-2.503.el6_9.4

x86_64
qemu-guest-agent-0.12.1.2-2.503.el6_9.4
qemu-kvm-tools-0.12.1.2-2.503.el6_9.4
qemu-img-0.12.1.2-2.503.el6_9.4
qemu-kvm-0.12.1.2-2.503.el6_9.4
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.4

RHEL6WS
x86_64
qemu-guest-agent-0.12.1.2-2.503.el6_9.4
qemu-kvm-tools-0.12.1.2-2.503.el6_9.4
qemu-img-0.12.1.2-2.503.el6_9.4
qemu-kvm-0.12.1.2-2.503.el6_9.4
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.4

i386
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.4
qemu-guest-agent-0.12.1.2-2.503.el6_9.4

141826 - Red Hat Enterprise Linux RHSA-2018-0034 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0034

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00031.html

RHEL7_3S

x86_64
microcode_ctl-debuginfo-2.1-16.4.el7_3
microcode_ctl-2.1-16.4.el7_3

141827 - Red Hat Enterprise Linux RHSA-2018-0009 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0009

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00005.html

RHEL7_3S
noarch
kernel-abi-whitelists-3.10.0-514.36.5.el7
kernel-doc-3.10.0-514.36.5.el7

x86_64
kernel-tools-libs-3.10.0-514.36.5.el7
python-perf-debuginfo-3.10.0-514.36.5.el7
kernel-tools-debuginfo-3.10.0-514.36.5.el7
kernel-debuginfo-common-x86_64-3.10.0-514.36.5.el7
perf-debuginfo-3.10.0-514.36.5.el7
perf-3.10.0-514.36.5.el7
kernel-headers-3.10.0-514.36.5.el7
kernel-debug-devel-3.10.0-514.36.5.el7
kernel-debuginfo-3.10.0-514.36.5.el7
kernel-debug-debuginfo-3.10.0-514.36.5.el7
kernel-devel-3.10.0-514.36.5.el7
kernel-debug-3.10.0-514.36.5.el7
kernel-tools-3.10.0-514.36.5.el7
kernel-3.10.0-514.36.5.el7
python-perf-3.10.0-514.36.5.el7
kernel-tools-libs-devel-3.10.0-514.36.5.el7

141828 - Red Hat Enterprise Linux RHSA-2018-0014 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

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

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00012.html

RHEL7D
noarch
iwl100-firmware-39.31.5.1-57.el7_4
linux-firmware-20170606-57.gitc990aae.el7_4
iwl7260-firmware-22.0.7.0-57.el7_4
iwl2030-firmware-18.168.6.1-57.el7_4
iwl1000-firmware-39.31.5.1-57.el7_4
iwl105-firmware-18.168.6.1-57.el7_4
iwl135-firmware-18.168.6.1-57.el7_4
iwl6050-firmware-41.28.5.1-57.el7_4
iwl4965-firmware-228.61.2.24-57.el7_4
iwl6000-firmware-9.221.4.1-57.el7_4
iwl3160-firmware-22.0.7.0-57.el7_4
iwl5000-firmware-8.83.5.1_1-57.el7_4
iwl5150-firmware-8.24.2.2-57.el7_4
iwl7265-firmware-22.0.7.0-57.el7_4
iwl2000-firmware-18.168.6.1-57.el7_4
iwl6000g2a-firmware-17.168.5.3-57.el7_4
iwl6000g2b-firmware-17.168.5.2-57.el7_4
iwl3945-firmware-15.32.2.9-57.el7_4

RHEL7S
noarch
iwl100-firmware-39.31.5.1-57.el7_4
linux-firmware-20170606-57.gitc990aae.el7_4
iwl7260-firmware-22.0.7.0-57.el7_4
iwl2030-firmware-18.168.6.1-57.el7_4
iwl1000-firmware-39.31.5.1-57.el7_4
iwl105-firmware-18.168.6.1-57.el7_4
iwl135-firmware-18.168.6.1-57.el7_4
iwl6050-firmware-41.28.5.1-57.el7_4
iwl4965-firmware-228.61.2.24-57.el7_4
iwl6000-firmware-9.221.4.1-57.el7_4
iwl3160-firmware-22.0.7.0-57.el7_4
iwl5000-firmware-8.83.5.1_1-57.el7_4
iwl5150-firmware-8.24.2.2-57.el7_4
iwl7265-firmware-22.0.7.0-57.el7_4
iwl2000-firmware-18.168.6.1-57.el7_4
iwl6000g2a-firmware-17.168.5.3-57.el7_4
iwl6000g2b-firmware-17.168.5.2-57.el7_4
iwl3945-firmware-15.32.2.9-57.el7_4

RHEL7WS
noarch
iwl100-firmware-39.31.5.1-57.el7_4
linux-firmware-20170606-57.gitc990aae.el7_4
iwl7260-firmware-22.0.7.0-57.el7_4
iwl2030-firmware-18.168.6.1-57.el7_4
iwl1000-firmware-39.31.5.1-57.el7_4
iwl105-firmware-18.168.6.1-57.el7_4
iwl135-firmware-18.168.6.1-57.el7_4
iwl6050-firmware-41.28.5.1-57.el7_4
iwl4965-firmware-228.61.2.24-57.el7_4
iwl6000-firmware-9.221.4.1-57.el7_4
iwl3160-firmware-22.0.7.0-57.el7_4
iwl5000-firmware-8.83.5.1_1-57.el7_4
iwl5150-firmware-8.24.2.2-57.el7_4
iwl7265-firmware-22.0.7.0-57.el7_4

iwl2000-firmware-18.168.6.1-57.el7_4
iwl6000g2a-firmware-17.168.5.3-57.el7_4
iwl6000g2b-firmware-17.168.5.2-57.el7_4
iwl3945-firmware-15.32.2.9-57.el7_4

141829 - Red Hat Enterprise Linux RHSA-2018-0030 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0030

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00026.html

RHEL6D
x86_64
libvirt-lock-sanlock-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-debuginfo-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1
libvirt-client-0.10.2-62.el6_9.1

i386
libvirt-client-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1
libvirt-debuginfo-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1

RHEL6S
i386
libvirt-client-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1
libvirt-debuginfo-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1

x86_64
libvirt-lock-sanlock-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-debuginfo-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1
libvirt-client-0.10.2-62.el6_9.1

RHEL6WS
x86_64
libvirt-client-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1
libvirt-debuginfo-0.10.2-62.el6_9.1

libvirt-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1

i386
libvirt-client-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1
libvirt-debuginfo-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1

141830 - Red Hat Enterprise Linux RHSA-2018-0040 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0040

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00035.html

RHEL6_5S
x86_64
microcode_ctl-debuginfo-1.17-17.el6_5.2
microcode_ctl-1.17-17.el6_5.2

141831 - Red Hat Enterprise Linux RHSA-2018-0038 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0038

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00030.html

RHEL6_4S
x86_64
microcode_ctl-debuginfo-1.17-16.1.el6_4
microcode_ctl-1.17-16.1.el6_4

141832 - Red Hat Enterprise Linux RHSA-2018-0031 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
RHSA-2018-0031

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00027.html

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

141833 - Red Hat Enterprise Linux RHSA-2018-0018 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0018

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00015.html

RHEL6_4S
x86_64
perf-2.6.32-358.84.2.el6
kernel-devel-2.6.32-358.84.2.el6

kernel-headers-2.6.32-358.84.2.el6
python-perf-debuginfo-2.6.32-358.84.2.el6
kernel-debug-devel-2.6.32-358.84.2.el6
python-perf-2.6.32-358.84.2.el6
kernel-debug-2.6.32-358.84.2.el6
perf-debuginfo-2.6.32-358.84.2.el6
kernel-debuginfo-common-x86_64-2.6.32-358.84.2.el6
kernel-debug-debuginfo-2.6.32-358.84.2.el6
kernel-debuginfo-2.6.32-358.84.2.el6
kernel-2.6.32-358.84.2.el6

noarch
kernel-doc-2.6.32-358.84.2.el6
kernel-firmware-2.6.32-358.84.2.el6

141834 - Red Hat Enterprise Linux RHSA-2018-0022 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0022

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00022.html

RHEL6_5S
x86_64
kernel-2.6.32-431.85.2.el6
kernel-debug-2.6.32-431.85.2.el6
python-perf-2.6.32-431.85.2.el6
kernel-devel-2.6.32-431.85.2.el6
perf-debuginfo-2.6.32-431.85.2.el6
kernel-headers-2.6.32-431.85.2.el6
kernel-debuginfo-2.6.32-431.85.2.el6
python-perf-debuginfo-2.6.32-431.85.2.el6
kernel-debug-devel-2.6.32-431.85.2.el6
kernel-debug-debuginfo-2.6.32-431.85.2.el6
perf-2.6.32-431.85.2.el6
kernel-debuginfo-common-x86_64-2.6.32-431.85.2.el6

noarch
kernel-abi-whitelists-2.6.32-431.85.2.el6
kernel-doc-2.6.32-431.85.2.el6
kernel-firmware-2.6.32-431.85.2.el6

146196 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0008-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0008-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003562.html

SuSE SLES 12 SP2
noarch
kernel-firmware-20170530-21.16.1
ucode-amd-20170530-21.16.1

SuSE SLED 12 SP3
noarch
kernel-firmware-20170530-21.16.1
ucode-amd-20170530-21.16.1

SuSE SLED 12 SP2
noarch
kernel-firmware-20170530-21.16.1
ucode-amd-20170530-21.16.1

SuSE SLES 12 SP3
noarch
kernel-firmware-20170530-21.16.1
ucode-amd-20170530-21.16.1

146197 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0010-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17805, CVE-2017-17806, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0010-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003564.html

SuSE SLED 12 SP3
x86_64
kernel-default-extra-debuginfo-4.4.103-6.38.1
kernel-syms-4.4.103-6.38.1
kernel-default-extra-4.4.103-6.38.1
kernel-default-debuginfo-4.4.103-6.38.1
kernel-default-devel-4.4.103-6.38.1
kernel-default-debugsource-4.4.103-6.38.1
kernel-default-4.4.103-6.38.1

noarch

kernel-devel-4.4.103-6.38.1
kernel-source-4.4.103-6.38.1
kernel-macros-4.4.103-6.38.1

SuSE SLES 12 SP3
noarch
kernel-devel-4.4.103-6.38.1
kernel-source-4.4.103-6.38.1
kernel-macros-4.4.103-6.38.1

x86_64
kernel-syms-4.4.103-6.38.1
kernel-default-base-debuginfo-4.4.103-6.38.1
kernel-default-base-4.4.103-6.38.1
kernel-default-debuginfo-4.4.103-6.38.1
kernel-default-devel-4.4.103-6.38.1
kernel-default-debugsource-4.4.103-6.38.1
kernel-default-4.4.103-6.38.1

146198 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0012-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17805, CVE-2017-17806, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0012-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003566.html

SuSE SLED 12 SP2
x86_64
kernel-default-debugsource-4.4.103-92.56.1
kernel-default-4.4.103-92.56.1
kernel-default-extra-debuginfo-4.4.103-92.56.1
kernel-default-debuginfo-4.4.103-92.56.1
kernel-default-extra-4.4.103-92.56.1
kernel-default-devel-4.4.103-92.56.1
kernel-syms-4.4.103-92.56.1

noarch
kernel-macros-4.4.103-92.56.1
kernel-devel-4.4.103-92.56.1
kernel-source-4.4.103-92.56.1

SuSE SLES 12 SP2
noarch
kernel-macros-4.4.103-92.56.1
kernel-devel-4.4.103-92.56.1
kernel-source-4.4.103-92.56.1

x86_64
kernel-default-base-debuginfo-4.4.103-92.56.1

kernel-default-4.4.103-92.56.1
kernel-syms-4.4.103-92.56.1
kernel-default-debugsource-4.4.103-92.56.1
kernel-default-devel-4.4.103-92.56.1
kernel-default-debuginfo-4.4.103-92.56.1
kernel-default-base-4.4.103-92.56.1

146199 - SuSE SLES 11 SP4 SUSE-SU-2018:0019-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2633, CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0019-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003571.html

SuSE SLES 11 SP4
i586
kvm-1.4.2-60.6.1

x86_64
kvm-1.4.2-60.6.1

146200 - SuSE Linux 42.3 openSUSE-SU-2018:0013-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0013-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00000.html

SuSE Linux 42.3
noarch
ucode-amd-20170530-14.1
kernel-firmware-20170530-14.1

146201 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0015-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14632, CVE-2017-14633

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0015-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003567.html

SuSE SLES 12 SP2
noarch
libvorbis-doc-1.3.3-10.3.1

x86_64
libvorbisenc2-32bit-1.3.3-10.3.1
libvorbisfile3-debuginfo-32bit-1.3.3-10.3.1
libvorbis0-debuginfo-32bit-1.3.3-10.3.1
libvorbisfile3-debuginfo-1.3.3-10.3.1
libvorbisfile3-1.3.3-10.3.1
libvorbis0-1.3.3-10.3.1
libvorbisenc2-debuginfo-1.3.3-10.3.1
libvorbisenc2-debuginfo-32bit-1.3.3-10.3.1
libvorbisfile3-32bit-1.3.3-10.3.1
libvorbis-debugsource-1.3.3-10.3.1
libvorbisenc2-1.3.3-10.3.1
libvorbis0-debuginfo-1.3.3-10.3.1
libvorbis0-32bit-1.3.3-10.3.1

SuSE SLED 12 SP3
x86_64
libvorbisfile3-debuginfo-32bit-1.3.3-10.3.1
libvorbis0-debuginfo-32bit-1.3.3-10.3.1
libvorbisfile3-debuginfo-1.3.3-10.3.1
libvorbisfile3-1.3.3-10.3.1
libvorbis0-1.3.3-10.3.1
libvorbisenc2-debuginfo-1.3.3-10.3.1
libvorbisenc2-debuginfo-32bit-1.3.3-10.3.1
libvorbisfile3-32bit-1.3.3-10.3.1
libvorbisenc2-1.3.3-10.3.1
libvorbis-debugsource-1.3.3-10.3.1
libvorbisenc2-32bit-1.3.3-10.3.1
libvorbis0-debuginfo-1.3.3-10.3.1
libvorbis0-32bit-1.3.3-10.3.1

SuSE SLED 12 SP2
x86_64
libvorbisfile3-debuginfo-32bit-1.3.3-10.3.1
libvorbis0-debuginfo-32bit-1.3.3-10.3.1
libvorbisfile3-debuginfo-1.3.3-10.3.1
libvorbisfile3-1.3.3-10.3.1
libvorbis0-1.3.3-10.3.1
libvorbisenc2-debuginfo-1.3.3-10.3.1
libvorbisenc2-debuginfo-32bit-1.3.3-10.3.1
libvorbisfile3-32bit-1.3.3-10.3.1
libvorbisenc2-1.3.3-10.3.1
libvorbis-debugsource-1.3.3-10.3.1

libvorbisenc2-32bit-1.3.3-10.3.1
libvorbis0-debuginfo-1.3.3-10.3.1
libvorbis0-32bit-1.3.3-10.3.1

SuSE SLES 12 SP3
noarch
libvorbis-doc-1.3.3-10.3.1

x86_64
libvorbisenc2-32bit-1.3.3-10.3.1
libvorbisfile3-debuginfo-32bit-1.3.3-10.3.1
libvorbis0-debuginfo-32bit-1.3.3-10.3.1
libvorbisfile3-debuginfo-1.3.3-10.3.1
libvorbisfile3-1.3.3-10.3.1
libvorbis0-1.3.3-10.3.1
libvorbisenc2-debuginfo-1.3.3-10.3.1
libvorbisenc2-debuginfo-32bit-1.3.3-10.3.1
libvorbisfile3-32bit-1.3.3-10.3.1
libvorbis-debugsource-1.3.3-10.3.1
libvorbisenc2-1.3.3-10.3.1
libvorbis0-debuginfo-1.3.3-10.3.1
libvorbis0-32bit-1.3.3-10.3.1

146202 - SuSE SLES 11 SP4 SUSE-SU-2018:0011-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11600, CVE-2017-13167, CVE-2017-14106, CVE-2017-15115, CVE-2017-15868, CVE-2017-16534, CVE-2017-16538, CVE-2017-16939, CVE-2017-17450, CVE-2017-17558, CVE-2017-17805, CVE-2017-17806, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7472, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0011-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003565.html

SuSE SLES 11 SP4
i586
kernel-xen-3.0.101-108.21.1
kernel-ec2-devel-3.0.101-108.21.1
kernel-trace-devel-3.0.101-108.21.1
kernel-syms-3.0.101-108.21.1
kernel-xen-base-3.0.101-108.21.1
kernel-pae-3.0.101-108.21.1
kernel-trace-3.0.101-108.21.1
kernel-trace-base-3.0.101-108.21.1
kernel-ec2-3.0.101-108.21.1
kernel-default-devel-3.0.101-108.21.1
kernel-source-3.0.101-108.21.1
kernel-pae-devel-3.0.101-108.21.1
kernel-default-3.0.101-108.21.1
kernel-ec2-base-3.0.101-108.21.1
kernel-xen-devel-3.0.101-108.21.1

kernel-pae-base-3.0.101-108.21.1
kernel-default-base-3.0.101-108.21.1

x86_64
kernel-xen-3.0.101-108.21.1
kernel-ec2-devel-3.0.101-108.21.1
kernel-trace-devel-3.0.101-108.21.1
kernel-syms-3.0.101-108.21.1
kernel-xen-base-3.0.101-108.21.1
kernel-trace-3.0.101-108.21.1
kernel-trace-base-3.0.101-108.21.1
kernel-ec2-3.0.101-108.21.1
kernel-default-devel-3.0.101-108.21.1
kernel-source-3.0.101-108.21.1
kernel-default-3.0.101-108.21.1
kernel-ec2-base-3.0.101-108.21.1
kernel-xen-devel-3.0.101-108.21.1
kernel-default-base-3.0.101-108.21.1

146203 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0017-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12563, CVE-2017-12691, CVE-2017-13061, CVE-2017-13062, CVE-2017-14042, CVE-2017-14174, CVE-2017-14343, CVE-2017-15277, CVE-2017-15281

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0017-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003569.html

SuSE SLED 12 SP2
x86_64
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.20.1
libMagickWand-6_Q16-1-6.8.8.1-71.20.1
ImageMagick-debugsource-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.20.1
libMagick++-6_Q16-3-6.8.8.1-71.20.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.20.1
ImageMagick-debuginfo-6.8.8.1-71.20.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.20.1
ImageMagick-6.8.8.1-71.20.1

SuSE SLES 12 SP3
x86_64
ImageMagick-debugsource-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-6.8.8.1-71.20.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.20.1
ImageMagick-debuginfo-6.8.8.1-71.20.1
libMagickWand-6_Q16-1-6.8.8.1-71.20.1

SuSE SLES 12 SP2
x86_64
ImageMagick-debugsource-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-6.8.8.1-71.20.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.20.1
ImageMagick-debuginfo-6.8.8.1-71.20.1
libMagickWand-6_Q16-1-6.8.8.1-71.20.1

SuSE SLED 12 SP3
x86_64
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.20.1
libMagickWand-6_Q16-1-6.8.8.1-71.20.1
ImageMagick-debugsource-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.20.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.20.1
libMagick++-6_Q16-3-6.8.8.1-71.20.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.20.1
ImageMagick-debuginfo-6.8.8.1-71.20.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.20.1
ImageMagick-6.8.8.1-71.20.1

146204 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0007-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0007-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003561.html

SuSE SLED 12 SP3
x86_64
qemu-tools-2.9.1-6.9.2
qemu-tools-debuginfo-2.9.1-6.9.2
qemu-2.9.1-6.9.2
qemu-x86-2.9.1-6.9.2
qemu-kvm-2.9.1-6.9.2
qemu-block-curl-2.9.1-6.9.2
qemu-debugsource-2.9.1-6.9.2
qemu-block-curl-debuginfo-2.9.1-6.9.2

noarch
qemu-vgabios-1.10.2-6.9.2
qemu-sgabios-8-6.9.2
qemu-ipxe-1.0.0-6.9.2
qemu-seabios-1.10.2-6.9.2

SuSE SLES 12 SP3
noarch

qemu-vgabios-1.10.2-6.9.2
qemu-sgabios-8-6.9.2
qemu-ipxe-1.0.0-6.9.2
qemu-seabios-1.10.2-6.9.2

x86_64
qemu-tools-2.9.1-6.9.2
qemu-block-rbd-debuginfo-2.9.1-6.9.2
qemu-debugsource-2.9.1-6.9.2
qemu-block-curl-debuginfo-2.9.1-6.9.2
qemu-x86-2.9.1-6.9.2
qemu-block-ssh-2.9.1-6.9.2
qemu-guest-agent-2.9.1-6.9.2
qemu-guest-agent-debuginfo-2.9.1-6.9.2
qemu-lang-2.9.1-6.9.2
qemu-2.9.1-6.9.2
qemu-block-rbd-2.9.1-6.9.2
qemu-tools-debuginfo-2.9.1-6.9.2
qemu-block-iscsi-debuginfo-2.9.1-6.9.2
qemu-block-ssh-debuginfo-2.9.1-6.9.2
qemu-kvm-2.9.1-6.9.2
qemu-block-iscsi-2.9.1-6.9.2
qemu-block-curl-2.9.1-6.9.2

146205 - SuSE SLES 11 SP4 SUSE-SU-2018:0016-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14632, CVE-2017-14633

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0016-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003568.html

SuSE SLES 11 SP4
i586
libvorbis-doc-1.2.0-79.20.3.1
libvorbis-1.2.0-79.20.3.1

x86_64
libvorbis-doc-1.2.0-79.20.3.1
libvorbis-1.2.0-79.20.3.1
libvorbis-32bit-1.2.0-79.20.3.1

146206 - SuSE SLES 11 SP4 SUSE-SU-2018:0009-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0009-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003563.html

SuSE SLES 11 SP4
x86_64
microcode_ctl-1.17-102.83.6.1

i586
microcode_ctl-1.17-102.83.6.1

146207 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0006-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0006-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003560.html

SuSE SLES 12 SP2
x86_64
ucode-intel-20170707-13.8.1
ucode-intel-debuginfo-20170707-13.8.1
ucode-intel-debugsource-20170707-13.8.1

SuSE SLED 12 SP3
x86_64
ucode-intel-20170707-13.8.1
ucode-intel-debuginfo-20170707-13.8.1
ucode-intel-debugsource-20170707-13.8.1

SuSE SLED 12 SP2
x86_64
ucode-intel-20170707-13.8.1
ucode-intel-debuginfo-20170707-13.8.1
ucode-intel-debugsource-20170707-13.8.1

SuSE SLES 12 SP3
x86_64
ucode-intel-20170707-13.8.1
ucode-intel-debuginfo-20170707-13.8.1
ucode-intel-debugsource-20170707-13.8.1

160338 - CentOS 7 CESA-2018-0007 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2018-0007

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022696.html

CentOS 7
x86_64
kernel-devel-3.10.0-693.11.6.el7
kernel-tools-libs-devel-3.10.0-693.11.6.el7
kernel-debug-devel-3.10.0-693.11.6.el7
kernel-headers-3.10.0-693.11.6.el7
python-perf-3.10.0-693.11.6.el7
kernel-tools-libs-3.10.0-693.11.6.el7
kernel-debug-3.10.0-693.11.6.el7
perf-3.10.0-693.11.6.el7
kernel-tools-3.10.0-693.11.6.el7
kernel-3.10.0-693.11.6.el7

noarch
kernel-abi-whitelists-3.10.0-693.11.6.el7
kernel-doc-3.10.0-693.11.6.el7

160339 - CentOS 6 CESA-2018-0030 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2018-0030

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022703.html

CentOS 6
x86_64
libvirt-client-0.10.2-62.el6_9.1
libvirt-lock-sanlock-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1

i686
libvirt-client-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1

160340 - CentOS 6 CESA-2018-0008 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2018-0008

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022701.html

CentOS 6
i686
kernel-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-devel-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6

noarch
kernel-doc-2.6.32-696.18.7.el6
kernel-firmware-2.6.32-696.18.7.el6
kernel-abi-whitelists-2.6.32-696.18.7.el6

x86_64
kernel-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-devel-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6

160341 - CentOS 7 CESA-2018-0029 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2018-0029

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022704.html

CentOS 7
x86_64
libvirt-daemon-driver-storage-iscsi-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-rbd-3.2.0-14.el7_4.7
libvirt-lock-sanlock-3.2.0-14.el7_4.7
libvirt-daemon-config-nwfilter-3.2.0-14.el7_4.7
libvirt-docs-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-gluster-3.2.0-14.el7_4.7
libvirt-daemon-driver-secret-3.2.0-14.el7_4.7
libvirt-daemon-driver-nwfilter-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-core-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-scsi-3.2.0-14.el7_4.7
libvirt-daemon-config-network-3.2.0-14.el7_4.7
libvirt-daemon-driver-qemu-3.2.0-14.el7_4.7
libvirt-daemon-driver-interface-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-disk-3.2.0-14.el7_4.7
libvirt-daemon-driver-network-3.2.0-14.el7_4.7
libvirt-nss-3.2.0-14.el7_4.7
libvirt-libs-3.2.0-14.el7_4.7
libvirt-daemon-driver-lxc-3.2.0-14.el7_4.7
libvirt-admin-3.2.0-14.el7_4.7
libvirt-login-shell-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-mpath-3.2.0-14.el7_4.7
libvirt-devel-3.2.0-14.el7_4.7
libvirt-client-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-logical-3.2.0-14.el7_4.7
libvirt-daemon-driver-nodedev-3.2.0-14.el7_4.7
libvirt-daemon-3.2.0-14.el7_4.7
libvirt-daemon-lxc-3.2.0-14.el7_4.7
libvirt-daemon-kvm-3.2.0-14.el7_4.7
libvirt-3.2.0-14.el7_4.7

i686
libvirt-devel-3.2.0-14.el7_4.7
libvirt-client-3.2.0-14.el7_4.7
libvirt-nss-3.2.0-14.el7_4.7
libvirt-libs-3.2.0-14.el7_4.7

160342 - CentOS 7 CESA-2018-0023 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2018-0023

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022705.html

CentOS 7
x86_64
qemu-kvm-common-1.5.3-141.el7_4.6
qemu-img-1.5.3-141.el7_4.6
qemu-kvm-1.5.3-141.el7_4.6
qemu-kvm-tools-1.5.3-141.el7_4.6

160343 - CentOS 6 CESA-2018-0013 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022700.html

CentOS 6
x86_64
microcode_ctl-1.17-25.2.el6_9

i686
microcode_ctl-1.17-25.2.el6_9

160344 - CentOS 7 CESA-2018-0012 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022697.html

CentOS 7
x86_64
microcode_ctl-2.1-22.2.el7

160345 - CentOS 7 CESA-2018-0014 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022698.html

CentOS 7
noarch
iwl2030-firmware-18.168.6.1-57.el7
iwl7260-firmware-22.0.7.0-57.el7
iwl3160-firmware-22.0.7.0-57.el7
iwl100-firmware-39.31.5.1-57.el7
iwl6050-firmware-41.28.5.1-57.el7
iwl2000-firmware-18.168.6.1-57.el7
iwl6000-firmware-9.221.4.1-57.el7
iwl6000g2b-firmware-17.168.5.2-57.el7
iwl105-firmware-18.168.6.1-57.el7
iwl5000-firmware-8.83.5.1_1-57.el7
iwl4965-firmware-228.61.2.24-57.el7
iwl6000g2a-firmware-17.168.5.3-57.el7
iwl135-firmware-18.168.6.1-57.el7
iwl1000-firmware-39.31.5.1-57.el7
linux-firmware-20170606-57.gitc990aae.el7
iwl3945-firmware-15.32.2.9-57.el7
iwl5150-firmware-8.24.2.2-57.el7
iwl7265-firmware-22.0.7.0-57.el7

163515 - Oracle Enterprise Linux ELSA-2018-4001 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16525, CVE-2017-16526, CVE-2017-16529, CVE-2017-16530, CVE-2017-16531, CVE-2017-16533, CVE-2017-16535, CVE-2017-16536

Description

The scan detected that the host is missing the following update:
ELSA-2018-4001

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007430.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007429.html

OEL7
x86_64
kernel-uek-debug-4.1.12-112.14.2.el7uek
kernel-uek-firmware-4.1.12-112.14.2.el7uek

kernel-uek-debug-devel-4.1.12-112.14.2.el7uek
kernel-uek-4.1.12-112.14.2.el7uek
kernel-uek-devel-4.1.12-112.14.2.el7uek
kernel-uek-doc-4.1.12-112.14.2.el7uek

OEL6
x86_64
kernel-uek-debug-devel-4.1.12-112.14.2.el6uek
kernel-uek-4.1.12-112.14.2.el6uek
kernel-uek-devel-4.1.12-112.14.2.el6uek
kernel-uek-debug-4.1.12-112.14.2.el6uek
kernel-uek-doc-4.1.12-112.14.2.el6uek
kernel-uek-firmware-4.1.12-112.14.2.el6uek

163517 - Oracle Enterprise Linux ELSA-2018-0012 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

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

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007433.html

OEL7
x86_64
microcode_ctl-2.1-22.2.el7

163518 - Oracle Enterprise Linux ELSA-2018-0007 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2018-0007

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007434.html

OEL7
x86_64
kernel-devel-3.10.0-693.11.6.el7
kernel-tools-libs-devel-3.10.0-693.11.6.el7
kernel-debug-devel-3.10.0-693.11.6.el7
kernel-doc-3.10.0-693.11.6.el7

python-perf-3.10.0-693.11.6.el7
kernel-abi-whitelists-3.10.0-693.11.6.el7
kernel-debug-3.10.0-693.11.6.el7
perf-3.10.0-693.11.6.el7
kernel-headers-3.10.0-693.11.6.el7
kernel-tools-3.10.0-693.11.6.el7
kernel-tools-libs-3.10.0-693.11.6.el7
kernel-3.10.0-693.11.6.el7

163519 - Oracle Enterprise Linux ELSA-2018-0013 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5715

Description

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

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007435.html

OEL6
x86_64
microcode_ctl-1.17-25.2.el6_9

i386
microcode_ctl-1.17-25.2.el6_9

170915 - Amazon Linux AMI ALAS-2018-938 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ALAS-2018-938

Observation

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

https://alas.aws.amazon.com/ALAS-2018-938.html

Amazon Linux AMI
x86_64
curl-7.53.1-13.80.amzn1
libcurl-devel-7.53.1-13.80.amzn1
curl-debuginfo-7.53.1-13.80.amzn1
libcurl-7.53.1-13.80.amzn1

i686

curl-7.53.1-13.80.amzn1
libcurl-devel-7.53.1-13.80.amzn1
curl-debuginfo-7.53.1-13.80.amzn1
libcurl-7.53.1-13.80.amzn1

175302 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1801-769)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1801-769)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=769

SL6
i386
kernel-devel-2.6.32-696.18.7.el6
perf-debuginfo-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6
kernel-debuginfo-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
python-perf-debuginfo-2.6.32-696.18.7.el6
kernel-debug-debuginfo-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
kernel-debuginfo-common-i686-2.6.32-696.18.7.el6

noarch
kernel-doc-2.6.32-696.18.7.el6
kernel-firmware-2.6.32-696.18.7.el6
kernel-abi-whitelists-2.6.32-696.18.7.el6

x86_64
kernel-2.6.32-696.18.7.el6
perf-2.6.32-696.18.7.el6
kernel-debug-2.6.32-696.18.7.el6
python-perf-debuginfo-2.6.32-696.18.7.el6
kernel-debug-devel-2.6.32-696.18.7.el6
perf-debuginfo-2.6.32-696.18.7.el6
python-perf-2.6.32-696.18.7.el6
kernel-debuginfo-2.6.32-696.18.7.el6
kernel-debug-debuginfo-2.6.32-696.18.7.el6
kernel-debuginfo-common-i686-2.6.32-696.18.7.el6
kernel-headers-2.6.32-696.18.7.el6
kernel-devel-2.6.32-696.18.7.el6
kernel-debuginfo-common-x86_64-2.6.32-696.18.7.el6

175303 - Scientific Linux Security ERRATA Important: libvirt on SL7.x x86_64 (1801-2808)

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libvirt on SL7.x x86_64 (1801-2808)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=2808

SL7
x86_64
libvirt-daemon-driver-storage-iscsi-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-rbd-3.2.0-14.el7_4.7
libvirt-lock-sanlock-3.2.0-14.el7_4.7
libvirt-daemon-config-nwfilter-3.2.0-14.el7_4.7
libvirt-docs-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-gluster-3.2.0-14.el7_4.7
libvirt-daemon-driver-secret-3.2.0-14.el7_4.7
libvirt-daemon-driver-nwfilter-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-core-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-scsi-3.2.0-14.el7_4.7
libvirt-daemon-config-network-3.2.0-14.el7_4.7
libvirt-daemon-driver-qemu-3.2.0-14.el7_4.7
libvirt-daemon-driver-interface-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-disk-3.2.0-14.el7_4.7
libvirt-daemon-driver-network-3.2.0-14.el7_4.7
libvirt-nss-3.2.0-14.el7_4.7
libvirt-debuginfo-3.2.0-14.el7_4.7
libvirt-libs-3.2.0-14.el7_4.7
libvirt-daemon-driver-lxc-3.2.0-14.el7_4.7
libvirt-admin-3.2.0-14.el7_4.7
libvirt-login-shell-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-mpath-3.2.0-14.el7_4.7
libvirt-devel-3.2.0-14.el7_4.7
libvirt-client-3.2.0-14.el7_4.7
libvirt-daemon-driver-storage-logical-3.2.0-14.el7_4.7
libvirt-daemon-driver-nodedev-3.2.0-14.el7_4.7
libvirt-daemon-3.2.0-14.el7_4.7
libvirt-daemon-lxc-3.2.0-14.el7_4.7
libvirt-daemon-kvm-3.2.0-14.el7_4.7
libvirt-3.2.0-14.el7_4.7

175304 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1801-78)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1801-78)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=78

SL7
x86_64
kernel-debuginfo-3.10.0-693.11.6.el7
perf-debuginfo-3.10.0-693.11.6.el7
kernel-tools-libs-devel-3.10.0-693.11.6.el7
kernel-3.10.0-693.11.6.el7
python-perf-debuginfo-3.10.0-693.11.6.el7
python-perf-3.10.0-693.11.6.el7
kernel-headers-3.10.0-693.11.6.el7
kernel-tools-libs-3.10.0-693.11.6.el7
kernel-debuginfo-common-x86_64-3.10.0-693.11.6.el7
kernel-devel-3.10.0-693.11.6.el7
kernel-tools-debuginfo-3.10.0-693.11.6.el7
kernel-tools-3.10.0-693.11.6.el7
kernel-debug-3.10.0-693.11.6.el7
kernel-debug-debuginfo-3.10.0-693.11.6.el7
kernel-debug-devel-3.10.0-693.11.6.el7
perf-3.10.0-693.11.6.el7

noarch
kernel-abi-whitelists-3.10.0-693.11.6.el7
kernel-doc-3.10.0-693.11.6.el7

175305 - Scientific Linux Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1801-2480)

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1801-2480)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=2480

SL7
x86_64
qemu-kvm-common-1.5.3-141.el7_4.6
qemu-kvm-tools-1.5.3-141.el7_4.6
qemu-img-1.5.3-141.el7_4.6
qemu-kvm-1.5.3-141.el7_4.6
qemu-kvm-debuginfo-1.5.3-141.el7_4.6

175306 - Scientific Linux Security ERRATA Important: microcode_ctl on SL6.x i386/x86_64 (1801-1133)

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: microcode_ctl on SL6.x i386/x86_64 (1801-1133)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=1133

SL6
x86_64
microcode_ctl-1.17-25.2.el6_9
microcode_ctl-debuginfo-1.17-25.2.el6_9

i386
microcode_ctl-1.17-25.2.el6_9
microcode_ctl-debuginfo-1.17-25.2.el6_9

175307 - Scientific Linux Security ERRATA Important: linux-firmware on SL7.x (noarch) (1801-1476)

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: linux-firmware on SL7.x (noarch) (1801-1476)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=1476

SL7
noarch
iwl100-firmware-39.31.5.1-57.el7_4
linux-firmware-20170606-57.gitc990aae.el7_4
iwl7260-firmware-22.0.7.0-57.el7_4
iwl2030-firmware-18.168.6.1-57.el7_4
iwl1000-firmware-39.31.5.1-57.el7_4
iwl105-firmware-18.168.6.1-57.el7_4
iwl135-firmware-18.168.6.1-57.el7_4
iwl6050-firmware-41.28.5.1-57.el7_4
iwl4965-firmware-228.61.2.24-57.el7_4
iwl6000-firmware-9.221.4.1-57.el7_4
iwl3160-firmware-22.0.7.0-57.el7_4
iwl5000-firmware-8.83.5.1_1-57.el7_4
iwl5150-firmware-8.24.2.2-57.el7_4
iwl7265-firmware-22.0.7.0-57.el7_4
iwl2000-firmware-18.168.6.1-57.el7_4
iwl6000g2a-firmware-17.168.5.3-57.el7_4
iwl6000g2b-firmware-17.168.5.2-57.el7_4

iwl3945-firmware-15.32.2.9-57.el7_4

175308 - Scientific Linux Security ERRATA Important: libvirt on SL6.x i386/x86_64 (1801-1816)

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libvirt on SL6.x i386/x86_64 (1801-1816)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=1816

SL6
x86_64
libvirt-lock-sanlock-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-debuginfo-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1
libvirt-client-0.10.2-62.el6_9.1

i386
libvirt-client-0.10.2-62.el6_9.1
libvirt-devel-0.10.2-62.el6_9.1
libvirt-debuginfo-0.10.2-62.el6_9.1
libvirt-0.10.2-62.el6_9.1
libvirt-python-0.10.2-62.el6_9.1

175309 - Scientific Linux Security ERRATA Important: microcode_ctl on SL7.x x86_64 (1801-433)

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: microcode_ctl on SL7.x x86_64 (1801-433)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=433

SL7
x86_64
microcode_ctl-debuginfo-2.1-22.2.el7
microcode_ctl-2.1-22.2.el7

175310 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1801-2147)

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

Risk Level: High

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1801-2147)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=2147

SL6
x86_64
qemu-guest-agent-0.12.1.2-2.503.el6_9.4
qemu-kvm-tools-0.12.1.2-2.503.el6_9.4
qemu-img-0.12.1.2-2.503.el6_9.4
qemu-kvm-0.12.1.2-2.503.el6_9.4
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.4

i386
qemu-kvm-debuginfo-0.12.1.2-2.503.el6_9.4
qemu-guest-agent-0.12.1.2-2.503.el6_9.4

193139 - Fedora Linux 26 FEDORA-2017-7fe2c4bc0e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7fe2c4bc0e

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=1

Fedora Core 26

python33-3.3.7-2.fc26

186028 - Ubuntu Linux 16.04, 17.04, 17.10 USN-3514-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13856, CVE-2017-13866, CVE-2017-13870, CVE-2017-7156

Description

The scan detected that the host is missing the following update:
USN-3514-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004200.html

Ubuntu 16.04

libjavascriptcoregtk-4.0-18_2.18.4-0ubuntu0.16.04.1
libwebkit2gtk-4.0-37_2.18.4-0ubuntu0.16.04.1

Ubuntu 17.04

libwebkit2gtk-4.0-37_2.18.4-0ubuntu0.17.04.1
libjavascriptcoregtk-4.0-18_2.18.4-0ubuntu0.17.04.1

Ubuntu 17.10

libwebkit2gtk-4.0-37_2.18.4-0ubuntu0.17.10.1
libjavascriptcoregtk-4.0-18_2.18.4-0ubuntu0.17.10.1

193140 - Fedora Linux 26 FEDORA-2017-b5cdad4163 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000256

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b5cdad4163

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=1

Fedora Core 26

libvirt-3.2.1-7.fc26

146208 - SuSE SLES 11 SP4 SUSE-SU-2018:0018-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15275

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0018-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003570.html

SuSE SLES 11 SP4
noarch
samba-doc-3.6.3-94.8.1

i586
ldapsmb-1.34b-94.8.1
libtdb1-3.6.3-94.8.1
libtalloc2-3.6.3-94.8.1
samba-3.6.3-94.8.1
libldb1-3.6.3-94.8.1
libwbclient0-3.6.3-94.8.1
samba-client-3.6.3-94.8.1
libsmbclient0-3.6.3-94.8.1
samba-winbind-3.6.3-94.8.1
samba-krb-printing-3.6.3-94.8.1
libtevent0-3.6.3-94.8.1

x86_64
libwbclient0-3.6.3-94.8.1
libtdb1-3.6.3-94.8.1
libtdb1-32bit-3.6.3-94.8.1
samba-krb-printing-3.6.3-94.8.1
samba-winbind-32bit-3.6.3-94.8.1
ldapsmb-1.34b-94.8.1
samba-client-32bit-3.6.3-94.8.1
libwbclient0-32bit-3.6.3-94.8.1
libsmbclient0-32bit-3.6.3-94.8.1
samba-32bit-3.6.3-94.8.1
libtevent0-32bit-3.6.3-94.8.1
libtalloc2-32bit-3.6.3-94.8.1
samba-3.6.3-94.8.1
libldb1-3.6.3-94.8.1
samba-winbind-3.6.3-94.8.1
libtevent0-3.6.3-94.8.1
samba-client-3.6.3-94.8.1
libtalloc2-3.6.3-94.8.1
libsmbclient0-3.6.3-94.8.1

186027 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3477-4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7826, CVE-2017-7827, CVE-2017-7828, CVE-2017-7830, CVE-2017-7831, CVE-2017-7832, CVE-2017-7833, CVE-2017-7834, CVE-2017-7835, CVE-2017-7837, CVE-2017-7838, CVE-2017-7839, CVE-2017-7840, CVE-2017-7842

Description

The scan detected that the host is missing the following update:
USN-3477-4

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004199.html

Ubuntu 16.04

firefox_57.0.3+build1-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_57.0.3+build1-0ubuntu0.14.04.1

Ubuntu 17.04

firefox_57.0.3+build1-0ubuntu0.17.04.1

Ubuntu 17.10

firefox_57.0.3+build1-0ubuntu0.17.10.1

193137 - Fedora Linux 26 FEDORA-2018-8ed5eff2c0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17852, CVE-2017-17853, CVE-2017-17854, CVE-2017-17855, CVE-2017-17856, CVE-2017-17857, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864

Description

The scan detected that the host is missing the following update:
FEDORA-2018-8ed5eff2c0

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=1

Fedora Core 26

kernel-4.14.11-200.fc26

193138 - Fedora Linux 27 FEDORA-2017-8a9862f4b7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8a9862f4b7

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=1

Fedora Core 27

php-symfony4-4.0.1-1.fc27

193141 - Fedora Linux 27 FEDORA-2018-22d5fa8a90 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17852, CVE-2017-17853, CVE-2017-17854, CVE-2017-17855, CVE-2017-17856, CVE-2017-17857, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864

Description

The scan detected that the host is missing the following update:
FEDORA-2018-22d5fa8a90

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=1

Fedora Core 27

kernel-4.14.11-300.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.

130982 - Debian Linux 8.0, 9.0 DSA-4077-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17784, CVE-2017-17785, CVE-2017-17786, CVE-2017-17787, CVE-2017-17788, CVE-2017-17789

Update Details

Risk is updated

182499 - FreeBSD h2o DoS In Workers (10c0fabc-b5da-11e7-816e-00bd5d1fff09)

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

Risk Level: Medium

CVE: CVE-2017-10868, CVE-2017-10869

Update Details

Risk is updated

HOW TO UPDATE

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

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting

"FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

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

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.