

MCAFFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

132444 - Oracle VM OVMSA-2018-0031 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-0444, CVE-2018-5146

Description

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

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2018-April/000841.html>

OVM3.3
x86_64
libvorbis-1.2.3-5.el6_9.1

132445 - Oracle VM OVMSA-2018-0030 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-0444, CVE-2018-5146

Description

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

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2018-April/000840.html>

OVM3.4
x86_64
libvorbis-1.2.3-5.el6_9.1

141921 - Red Hat Enterprise Linux RHSA-2018-1062 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3672, CVE-2016-7913, CVE-2016-8633, CVE-2017-1000252, CVE-2017-1000407, CVE-2017-1000410, CVE-2017-12154, CVE-2017-12190, CVE-2017-13166, CVE-2017-14140, CVE-2017-15116, CVE-2017-15121, CVE-2017-15126, CVE-2017-15127, CVE-2017-15129, CVE-2017-15265, CVE-2017-17448, CVE-2017-17449, CVE-2017-17558, CVE-2017-18017, CVE-2017-18203, CVE-2017-5754, CVE-2017-7294, CVE-2017-8824, CVE-2017-9725, CVE-2018-1000004, CVE-2018-5750, CVE-2018-6927

Description

The scan detected that the host is missing the following update:
RHSA-2018-1062

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00023.html>

RHEL7D

x86_64
kernel-tools-debuginfo-3.10.0-862.el7
kernel-tools-libs-devel-3.10.0-862.el7
python-perf-3.10.0-862.el7
kernel-3.10.0-862.el7
perf-3.10.0-862.el7
kernel-tools-3.10.0-862.el7
kernel-debug-3.10.0-862.el7
kernel-debug-debuginfo-3.10.0-862.el7
kernel-headers-3.10.0-862.el7
python-perf-debuginfo-3.10.0-862.el7
kernel-debug-devel-3.10.0-862.el7
kernel-tools-libs-3.10.0-862.el7
kernel-debuginfo-3.10.0-862.el7
kernel-devel-3.10.0-862.el7
kernel-debuginfo-common-x86_64-3.10.0-862.el7
perf-debuginfo-3.10.0-862.el7

noarch

kernel-doc-3.10.0-862.el7
kernel-abi-whitelists-3.10.0-862.el7

RHEL7S

noarch
kernel-doc-3.10.0-862.el7
kernel-abi-whitelists-3.10.0-862.el7

x86_64

kernel-tools-debuginfo-3.10.0-862.el7
kernel-tools-libs-devel-3.10.0-862.el7
python-perf-3.10.0-862.el7
kernel-3.10.0-862.el7
perf-3.10.0-862.el7
kernel-tools-3.10.0-862.el7
kernel-debug-3.10.0-862.el7
kernel-debug-debuginfo-3.10.0-862.el7
kernel-headers-3.10.0-862.el7
python-perf-debuginfo-3.10.0-862.el7
kernel-debug-devel-3.10.0-862.el7
kernel-tools-libs-3.10.0-862.el7
kernel-debuginfo-3.10.0-862.el7
kernel-devel-3.10.0-862.el7

kernel-debuginfo-common-x86_64-3.10.0-862.el7
perf-debuginfo-3.10.0-862.el7

RHEL7WS

x86_64
kernel-tools-debuginfo-3.10.0-862.el7
kernel-tools-libs-devel-3.10.0-862.el7
python-perf-3.10.0-862.el7
kernel-3.10.0-862.el7
perf-3.10.0-862.el7
kernel-tools-3.10.0-862.el7
kernel-debug-3.10.0-862.el7
kernel-debug-debuginfo-3.10.0-862.el7
kernel-headers-3.10.0-862.el7
python-perf-debuginfo-3.10.0-862.el7
kernel-debug-devel-3.10.0-862.el7
kernel-tools-libs-3.10.0-862.el7
kernel-debuginfo-3.10.0-862.el7
kernel-devel-3.10.0-862.el7
kernel-debuginfo-common-x86_64-3.10.0-862.el7
perf-debuginfo-3.10.0-862.el7

noarch
kernel-doc-3.10.0-862.el7
kernel-abi-whitelists-3.10.0-862.el7

163569 - Oracle Enterprise Linux ELSA-2018-0649 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-0444, CVE-2018-5146

Description

The scan detected that the host is missing the following update:
ELSA-2018-0649

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2018-April/007601.html>

OEL6
x86_64
libvorbis-devel-docs-1.2.3-5.el6_9.1
libvorbis-1.2.3-5.el6_9.1
libvorbis-devel-1.2.3-5.el6_9.1

i386
libvorbis-devel-docs-1.2.3-5.el6_9.1
libvorbis-1.2.3-5.el6_9.1
libvorbis-devel-1.2.3-5.el6_9.1

186165 - Ubuntu Linux 14.04 USN-3620-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11089, CVE-2017-12762, CVE-2017-17448, CVE-2017-17741, CVE-2017-17805, CVE-2017-17807, CVE-2018-1000026, CVE-2018-5332

Description

The scan detected that the host is missing the following update:
USN-3620-1

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-April/004347.html>

Ubuntu 14.04

linux-image-3.13.0-144-powerpc64-emb_3.13.0-144.193
linux-image-3.13.0-144-powerpc-e500_3.13.0-144.193
linux-image-3.13.0-144-lowlatency_3.13.0-144.193
linux-image-3.13.0-144-powerpc64-smp_3.13.0-144.193
linux-image-3.13.0-144-powerpc-e500mc_3.13.0-144.193
linux-image-powerpc-smp_3.13.0.144.154
linux-image-3.13.0-144-generic_3.13.0-144.193
linux-image-generic-lpae_3.13.0.144.154
linux-image-lowlatency_3.13.0.144.154
linux-image-powerpc-e500mc_3.13.0.144.154
linux-image-3.13.0-144-powerpc-smp_3.13.0-144.193
linux-image-generic_3.13.0.144.154
linux-image-powerpc-e500_3.13.0.144.154
linux-image-powerpc64-emb_3.13.0.144.154
linux-image-powerpc64-smp_3.13.0.144.154
linux-image-3.13.0-144-generic-lpae_3.13.0-144.193

186170 - Ubuntu Linux 12.04 USN-3620-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11089, CVE-2017-12762, CVE-2017-17448, CVE-2017-17741, CVE-2017-17805, CVE-2017-17807, CVE-2017-5715, CVE-2018-1000026, CVE-2018-5332

Description

The scan detected that the host is missing the following update:
USN-3620-2

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-April/004348.html>

Ubuntu 12.04

linux-image-3.13.0-144-generic-lpae_3.13.0-144.193~precise1
linux-image-3.13.0-144-generic_3.13.0-144.193~precise1
linux-image-generic-lts-trusty_3.13.0.144.135
linux-image-generic-lpae-lts-trusty_3.13.0.144.135

170955 - Amazon Linux AMI ALAS-2018-981 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5146

Description

The scan detected that the host is missing the following update:
ALAS-2018-981

Observation

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

<https://alas.aws.amazon.com/ALAS-2018-981.html>

Amazon Linux AMI

i686

libvorbis-1.3.3-8.7.amzn1

libvorbis-devel-1.3.3-8.7.amzn1

libvorbis-debuginfo-1.3.3-8.7.amzn1

noarch

libvorbis-devel-docs-1.3.3-8.7.amzn1

x86_64

libvorbis-1.3.3-8.7.amzn1

libvorbis-devel-1.3.3-8.7.amzn1

libvorbis-debuginfo-1.3.3-8.7.amzn1

170957 - Amazon Linux AMI ALAS-2018-989 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7750

Description

The scan detected that the host is missing the following update:
ALAS-2018-989

Observation

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

<https://alas.aws.amazon.com/ALAS-2018-989.html>

Amazon Linux AMI

noarch

python26-paramiko-1.15.1-2.6.amzn1

python27-paramiko-1.15.1-2.6.amzn1

131073 - Debian Linux 9.0 DSA-4170-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16872, CVE-2017-16875, CVE-2018-1000098, CVE-2018-1000099

Description

The scan detected that the host is missing the following update:
DSA-4170-1

Observation

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

<http://www.debian.org/security/2018/dsa-4170>

Debian 9.0

all

python-pjproject_2.5.5~dfsg-6+deb9u1

libpj2_2.5.5~dfsg-6+deb9u1

libpjsip-simple2_2.5.5~dfsg-6+deb9u1

libpjsip2_2.5.5~dfsg-6+deb9u1

libpjsua2-2v5_2.5.5~dfsg-6+deb9u1

libpjsip-ua2_2.5.5~dfsg-6+deb9u1

libpjmedia-codec2_2.5.5~dfsg-6+deb9u1

libpjproject-dev_2.5.5~dfsg-6+deb9u1

libpjmedia-audiodev2_2.5.5~dfsg-6+deb9u1

libpjmedia-videodev2_2.5.5~dfsg-6+deb9u1

libpjmedia2_2.5.5~dfsg-6+deb9u1

libpjlib-util2_2.5.5~dfsg-6+deb9u1

libpjnath2_2.5.5~dfsg-6+deb9u1

libpjsua2_2.5.5~dfsg-6+deb9u1

141915 - Red Hat Enterprise Linux RHSA-2018-0648 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146

Description

The scan detected that the host is missing the following update:
RHSA-2018-0648

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00006.html>

RHEL7D

x86_64

thunderbird-debuginfo-52.7.0-1.el7_4

thunderbird-52.7.0-1.el7_4

RHEL7S

x86_64

thunderbird-debuginfo-52.7.0-1.el7_4

thunderbird-52.7.0-1.el7_4

RHEL7WS

x86_64

thunderbird-debuginfo-52.7.0-1.el7_4
thunderbird-52.7.0-1.el7_4

141917 - Red Hat Enterprise Linux RHSA-2018-1098 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5148

Description

The scan detected that the host is missing the following update:
RHSA-2018-1098

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00027.html>

RHEL6D
x86_64
firefox-debuginfo-52.7.3-1.el6_9
firefox-52.7.3-1.el6_9

i386
firefox-debuginfo-52.7.3-1.el6_9
firefox-52.7.3-1.el6_9

RHEL6S
i386
firefox-debuginfo-52.7.3-1.el6_9
firefox-52.7.3-1.el6_9

x86_64
firefox-debuginfo-52.7.3-1.el6_9
firefox-52.7.3-1.el6_9

RHEL6WS
x86_64
firefox-debuginfo-52.7.3-1.el6_9
firefox-52.7.3-1.el6_9

i386
firefox-debuginfo-52.7.3-1.el6_9
firefox-52.7.3-1.el6_9

141918 - Red Hat Enterprise Linux RHSA-2018-0805 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9402, CVE-2015-5180, CVE-2017-1000366, CVE-2017-12132, CVE-2017-15670, CVE-2017-15804, CVE-2018-1000001

Description

The scan detected that the host is missing the following update:
RHSA-2018-0805

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00017.html>

RHEL7D

x86_64
glibc-static-2.17-222.el7
glibc-debuginfo-2.17-222.el7
glibc-2.17-222.el7
nscd-2.17-222.el7
glibc-headers-2.17-222.el7
glibc-devel-2.17-222.el7
glibc-common-2.17-222.el7
glibc-utils-2.17-222.el7
glibc-debuginfo-common-2.17-222.el7

RHEL7S

x86_64
glibc-static-2.17-222.el7
glibc-debuginfo-2.17-222.el7
glibc-2.17-222.el7
nscd-2.17-222.el7
glibc-headers-2.17-222.el7
glibc-devel-2.17-222.el7
glibc-common-2.17-222.el7
glibc-utils-2.17-222.el7
glibc-debuginfo-common-2.17-222.el7

RHEL7WS

x86_64
glibc-static-2.17-222.el7
glibc-debuginfo-2.17-222.el7
glibc-2.17-222.el7
nscd-2.17-222.el7
glibc-headers-2.17-222.el7
glibc-devel-2.17-222.el7
glibc-common-2.17-222.el7
glibc-utils-2.17-222.el7
glibc-debuginfo-common-2.17-222.el7

141919 - Red Hat Enterprise Linux RHSA-2018-1058 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5146

Description

The scan detected that the host is missing the following update:
RHSA-2018-1058

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00022.html>

RHEL7D
x86_64
libvorbis-debuginfo-1.3.3-8.el7.1
libvorbis-1.3.3-8.el7.1
libvorbis-devel-1.3.3-8.el7.1

noarch
libvorbis-devel-docs-1.3.3-8.el7.1

RHEL7S
noarch
libvorbis-devel-docs-1.3.3-8.el7.1

x86_64
libvorbis-debuginfo-1.3.3-8.el7.1
libvorbis-1.3.3-8.el7.1
libvorbis-devel-1.3.3-8.el7.1

RHEL7WS
x86_64
libvorbis-debuginfo-1.3.3-8.el7.1
libvorbis-1.3.3-8.el7.1
libvorbis-devel-1.3.3-8.el7.1

noarch
libvorbis-devel-docs-1.3.3-8.el7.1

141922 - Red Hat Enterprise Linux RHSA-2018-0649 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5146

Description

The scan detected that the host is missing the following update:
RHSA-2018-0649

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00005.html>

RHEL6D
i386
libvorbis-debuginfo-1.2.3-5.el6_9.1
libvorbis-1.2.3-5.el6_9.1
libvorbis-devel-1.2.3-5.el6_9.1

noarch
libvorbis-devel-docs-1.2.3-5.el6_9.1

x86_64
libvorbis-debuginfo-1.2.3-5.el6_9.1
libvorbis-1.2.3-5.el6_9.1
libvorbis-devel-1.2.3-5.el6_9.1

RHEL6S

i386
libvorbis-debuginfo-1.2.3-5.el6_9.1
libvorbis-1.2.3-5.el6_9.1
libvorbis-devel-1.2.3-5.el6_9.1

noarch
libvorbis-devel-docs-1.2.3-5.el6_9.1

x86_64
libvorbis-debuginfo-1.2.3-5.el6_9.1
libvorbis-1.2.3-5.el6_9.1
libvorbis-devel-1.2.3-5.el6_9.1

RHEL6WS
x86_64
libvorbis-1.2.3-5.el6_9.1
libvorbis-debuginfo-1.2.3-5.el6_9.1

i386
libvorbis-1.2.3-5.el6_9.1
libvorbis-debuginfo-1.2.3-5.el6_9.1

141923 - Red Hat Enterprise Linux RHSA-2018-0647 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146

Description

The scan detected that the host is missing the following update:
RHSA-2018-0647

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00007.html>

RHEL6S
i386
thunderbird-52.7.0-1.el6_9
thunderbird-debuginfo-52.7.0-1.el6_9

x86_64
thunderbird-52.7.0-1.el6_9
thunderbird-debuginfo-52.7.0-1.el6_9

RHEL6D
x86_64
thunderbird-52.7.0-1.el6_9
thunderbird-debuginfo-52.7.0-1.el6_9

i386
thunderbird-52.7.0-1.el6_9
thunderbird-debuginfo-52.7.0-1.el6_9

RHEL6WS
x86_64

thunderbird-52.7.0-1.el6_9
thunderbird-debuginfo-52.7.0-1.el6_9

i386
thunderbird-52.7.0-1.el6_9
thunderbird-debuginfo-52.7.0-1.el6_9

141925 - Red Hat Enterprise Linux RHSA-2018-0878 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15041, CVE-2017-15042, CVE-2018-6574

Description

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

RHSA-2018-0878

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00010.html>

RHEL7S
noarch
golang-docs-1.9.4-1.el7
golang-misc-1.9.4-1.el7
golang-tests-1.9.4-1.el7
golang-src-1.9.4-1.el7

x86_64
golang-1.9.4-1.el7
golang-bin-1.9.4-1.el7

141926 - Red Hat Enterprise Linux RHSA-2018-1099 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5148

Description

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

RHSA-2018-1099

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00026.html>

RHEL7D
x86_64
firefox-debuginfo-52.7.3-1.el7_5
firefox-52.7.3-1.el7_5

RHEL7S

x86_64
firefox-debuginfo-52.7.3-1.el7_5
firefox-52.7.3-1.el7_5

RHEL7WS
x86_64
firefox-debuginfo-52.7.3-1.el7_5
firefox-52.7.3-1.el7_5

141927 - Red Hat Enterprise Linux RHSA-2018-0816 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13672, CVE-2017-13711, CVE-2017-15124, CVE-2017-15268, CVE-2018-5683

Description

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

RHSA-2018-0816

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00009.html>

RHEL7D
x86_64
qemu-kvm-1.5.3-156.el7
qemu-kvm-debuginfo-1.5.3-156.el7
qemu-kvm-common-1.5.3-156.el7
qemu-kvm-tools-1.5.3-156.el7
qemu-img-1.5.3-156.el7

RHEL7S
x86_64
qemu-kvm-1.5.3-156.el7
qemu-kvm-debuginfo-1.5.3-156.el7
qemu-kvm-common-1.5.3-156.el7
qemu-kvm-tools-1.5.3-156.el7
qemu-img-1.5.3-156.el7

RHEL7WS
x86_64
qemu-kvm-1.5.3-156.el7
qemu-kvm-debuginfo-1.5.3-156.el7
qemu-kvm-common-1.5.3-156.el7
qemu-kvm-tools-1.5.3-156.el7
qemu-img-1.5.3-156.el7

141929 - Red Hat Enterprise Linux RHSA-2018-1055 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7225

Description

The scan detected that the host is missing the following update:
RHSA-2018-1055

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00020.html>

RHEL7D
x86_64
libvncserver-0.9.9-12.el7_5
libvncserver-debuginfo-0.9.9-12.el7_5
libvncserver-devel-0.9.9-12.el7_5

RHEL7S
x86_64
libvncserver-0.9.9-12.el7_5
libvncserver-debuginfo-0.9.9-12.el7_5
libvncserver-devel-0.9.9-12.el7_5

RHEL7WS
x86_64
libvncserver-0.9.9-12.el7_5
libvncserver-debuginfo-0.9.9-12.el7_5
libvncserver-devel-0.9.9-12.el7_5

146573 - SuSE Linux 42.3 openSUSE-SU-2018:0899-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-9256, CVE-2018-9259, CVE-2018-9260, CVE-2018-9261, CVE-2018-9262, CVE-2018-9263, CVE-2018-9264, CVE-2018-9265, CVE-2018-9266, CVE-2018-9267, CVE-2018-9268, CVE-2018-9269, CVE-2018-9270, CVE-2018-9271, CVE-2018-9272, CVE-2018-9273, CVE-2018-9274

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0899-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00015.html>

SuSE Linux 42.3
x86_64
wireshark-ui-qt-debuginfo-2.2.14-38.1
wireshark-ui-gtk-2.2.14-38.1
wireshark-debuginfo-2.2.14-38.1
wireshark-ui-qt-2.2.14-38.1
wireshark-ui-gtk-debuginfo-2.2.14-38.1
wireshark-devel-2.2.14-38.1
wireshark-debugsource-2.2.14-38.1
wireshark-2.2.14-38.1

146576 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0877-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12194

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0877-1

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-April/003873.html>

SuSE SLED 12 SP3

x86_64

libspice-client-glib-2_0-8-debuginfo-0.33-3.3.2

libspice-client-glib-2_0-8-0.33-3.3.2

libspice-client-gtk-3_0-5-0.33-3.3.2

typelib-1_0-SpiceClientGtk-3_0-0.33-3.3.2

spice-gtk-debugsource-0.33-3.3.2

spice-gtk-debuginfo-0.33-3.3.2

libspice-client-glib-helper-debuginfo-0.33-3.3.2

libspice-client-glib-helper-0.33-3.3.2

libspice-client-gtk-3_0-5-debuginfo-0.33-3.3.2

typelib-1_0-SpiceClientGlib-2_0-0.33-3.3.2

libspice-controller0-0.33-3.3.2

libspice-controller0-debuginfo-0.33-3.3.2

SuSE SLES 12 SP3

x86_64

libspice-client-glib-2_0-8-debuginfo-0.33-3.3.2

libspice-client-glib-2_0-8-0.33-3.3.2

libspice-client-gtk-3_0-5-0.33-3.3.2

typelib-1_0-SpiceClientGtk-3_0-0.33-3.3.2

spice-gtk-debugsource-0.33-3.3.2

spice-gtk-debuginfo-0.33-3.3.2

libspice-client-glib-helper-debuginfo-0.33-3.3.2

libspice-client-glib-helper-0.33-3.3.2

libspice-client-gtk-3_0-5-debuginfo-0.33-3.3.2

typelib-1_0-SpiceClientGlib-2_0-0.33-3.3.2

libspice-controller0-0.33-3.3.2

libspice-controller0-debuginfo-0.33-3.3.2

146579 - SuSE SLES 11 SP4 SUSE-SU-2018:0875-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7225

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0875-1

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-April/003871.html>

SuSE SLES 11 SP4
i586
LibVNCServer-0.9.1-160.3.1

x86_64
LibVNCServer-0.9.1-160.3.1

146580 - SuSE Linux 42.3 openSUSE-SU-2018:0892-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12194

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0892-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00011.html>

SuSE Linux 42.3
x86_64
libspice-controller0-0.33-2.3.1
libspice-client-glib-2_0-8-0.33-2.3.1
spice-gtk-debugsource-0.33-2.3.1
typelib-1_0-SpiceClientGtk-3_0-0.33-2.3.1
spice-gtk-debuginfo-0.33-2.3.1
libspice-client-gtk-3_0-5-0.33-2.3.1
spice-gtk-devel-0.33-2.3.1
libspice-client-gtk-3_0-5-debuginfo-0.33-2.3.1
libspice-controller0-debuginfo-0.33-2.3.1
libspice-client-glib-2_0-8-debuginfo-0.33-2.3.1
typelib-1_0-SpiceClientGlib-2_0-0.33-2.3.1
libspice-client-glib-helper-0.33-2.3.1
libspice-client-glib-helper-debuginfo-0.33-2.3.1
spice-gtk-0.33-2.3.1

noarch
spice-gtk-lang-0.33-2.3.1

146581 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0878-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14062

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0878-1

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-April/003874.html>

SuSE SLED 12 SP3

x86_64

libidn11-debuginfo-1.28-5.3.1

libidn11-1.28-5.3.1

libidn-debugsource-1.28-5.3.1

libidn11-32bit-1.28-5.3.1

libidn11-debuginfo-32bit-1.28-5.3.1

SuSE SLES 12 SP3

x86_64

libidn-tools-debuginfo-1.28-5.3.1

libidn11-debuginfo-32bit-1.28-5.3.1

libidn-tools-1.28-5.3.1

libidn11-32bit-1.28-5.3.1

libidn-debugsource-1.28-5.3.1

libidn11-1.28-5.3.1

libidn11-debuginfo-1.28-5.3.1

146583 - SuSE SLES 11 SP4 SUSE-SU-2018:0903-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14062

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0903-1

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-April/003879.html>

SuSE SLES 11 SP4

i586

libidn-1.10-7.3.1

x86_64

libidn-1.10-7.3.1

libidn-32bit-1.10-7.3.1

146584 - SuSE SLES 11 SP4 SUSE-SU-2018:0907-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5130, CVE-2018-5131, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146, CVE-2018-5147, CVE-2018-5148

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0907-1

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-April/003882.html>

SuSE SLES 11 SP4

i586

MozillaFirefox-52.7.3esr-72.27.2

MozillaFirefox-translations-52.7.3esr-72.27.2

x86_64

MozillaFirefox-52.7.3esr-72.27.2

MozillaFirefox-translations-52.7.3esr-72.27.2

146587 - SuSE Linux 42.3 openSUSE-SU-2018:0917-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000132

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0917-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00021.html>

SuSE Linux 42.3

i586

mercurial-4.2.3-12.1

mercurial-debugsource-4.2.3-12.1

mercurial-debuginfo-4.2.3-12.1

noarch

mercurial-lang-4.2.3-12.1

x86_64

mercurial-4.2.3-12.1

mercurial-debugsource-4.2.3-12.1

mercurial-debuginfo-4.2.3-12.1

146589 - SuSE SLES 11 SP4 SUSE-SU-2018:0880-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11524, CVE-2017-12691, CVE-2017-12692, CVE-2017-12693, CVE-2017-13768, CVE-2017-14314, CVE-2017-14343, CVE-2017-14505, CVE-2017-15016, CVE-2017-15017, CVE-2017-16352, CVE-2017-16353, CVE-2017-18219, CVE-2017-9500, CVE-2018-7443, CVE-2018-8804

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0880-1

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-April/003876.html>

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-78.40.1

x86_64
libMagickCore1-32bit-6.4.3.6-78.40.1
libMagickCore1-6.4.3.6-78.40.1

146590 - SuSE Linux 42.3 openSUSE-SU-2018:0891-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14062

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0891-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00010.html>

SuSE Linux 42.3
x86_64
libidn-tools-1.28-9.3.1
libidn11-debuginfo-32bit-1.28-9.3.1
libidn11-debuginfo-1.28-9.3.1
libidn11-32bit-1.28-9.3.1
libidn-tools-debuginfo-1.28-9.3.1
libidn-devel-1.28-9.3.1
libidn-debugsource-1.28-9.3.1
libidn11-1.28-9.3.1

i586
libidn-tools-1.28-9.3.1
libidn11-debuginfo-1.28-9.3.1
libidn-tools-debuginfo-1.28-9.3.1
libidn-devel-1.28-9.3.1
libidn-debugsource-1.28-9.3.1
libidn11-1.28-9.3.1

146591 - SuSE Linux 42.3 openSUSE-SU-2018:0893-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11524, CVE-2017-12692, CVE-2017-12693, CVE-2017-13768, CVE-2017-14314, CVE-2017-14505, CVE-2017-14739, CVE-2017-15016, CVE-2017-15017, CVE-2017-16352, CVE-2017-16353, CVE-2017-18209, CVE-2017-18211, CVE-2017-9500, CVE-2018-7443, CVE-2018-7470, CVE-2018-8804

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0893-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00012.html>

SuSE Linux 42.3

i586

libMagickCore-6_Q16-1-6.8.8.1-58.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-58.1
ImageMagick-debuginfo-6.8.8.1-58.1
ImageMagick-extra-debuginfo-6.8.8.1-58.1
ImageMagick-debugsource-6.8.8.1-58.1
ImageMagick-6.8.8.1-58.1
ImageMagick-devel-6.8.8.1-58.1
libMagick++-devel-6.8.8.1-58.1
libMagick++-6_Q16-3-6.8.8.1-58.1
perl-PerlMagick-6.8.8.1-58.1
ImageMagick-extra-6.8.8.1-58.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-58.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-58.1
libMagickWand-6_Q16-1-6.8.8.1-58.1
perl-PerlMagick-debuginfo-6.8.8.1-58.1

noarch

ImageMagick-doc-6.8.8.1-58.1

x86_64

libMagickCore-6_Q16-1-6.8.8.1-58.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-58.1
ImageMagick-debuginfo-6.8.8.1-58.1
ImageMagick-extra-debuginfo-6.8.8.1-58.1
ImageMagick-debugsource-6.8.8.1-58.1
ImageMagick-6.8.8.1-58.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-58.1
ImageMagick-devel-6.8.8.1-58.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-58.1
libMagick++-devel-6.8.8.1-58.1
libMagick++-6_Q16-3-6.8.8.1-58.1
perl-PerlMagick-6.8.8.1-58.1
ImageMagick-extra-6.8.8.1-58.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-58.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-58.1
libMagick++-devel-32bit-6.8.8.1-58.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-58.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-58.1
libMagickWand-6_Q16-1-6.8.8.1-58.1
libMagick++-6_Q16-3-32bit-6.8.8.1-58.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-58.1
perl-PerlMagick-debuginfo-6.8.8.1-58.1

160380 - CentOS 6 CESA-2018-0647 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146

Description

The scan detected that the host is missing the following update:
CESA-2018-0647

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2018-April/022813.html>

CentOS 6
x86_64
thunderbird-52.7.0-1.el6.centos

i686
thunderbird-52.7.0-1.el6.centos

160381 - CentOS 7 CESA-2018-0648 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146

Description

The scan detected that the host is missing the following update:
CESA-2018-0648

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2018-April/022815.html>

CentOS 7
x86_64
thunderbird-52.7.0-1.el7.centos

160382 - CentOS 6 CESA-2018-0649 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5146

Description

The scan detected that the host is missing the following update:
CESA-2018-0649

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2018-April/022814.html>

CentOS 6
i686
libvorbis-devel-1.2.3-5.el6_9.1
libvorbis-1.2.3-5.el6_9.1

noarch
libvorbis-devel-docs-1.2.3-5.el6_9.1

x86_64
libvorbis-devel-1.2.3-5.el6_9.1
libvorbis-1.2.3-5.el6_9.1

163568 - Oracle Enterprise Linux ELSA-2018-0647 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146

Description

The scan detected that the host is missing the following update:
ELSA-2018-0647

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2018-April/007603.html>

OEL6
x86_64
thunderbird-52.7.0-1.0.1.el6_9

i386
thunderbird-52.7.0-1.0.1.el6_9

163570 - Oracle Enterprise Linux ELSA-2018-0648 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146

Description

The scan detected that the host is missing the following update:
ELSA-2018-0648

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2018-April/007600.html>

OEL7
x86_64
thunderbird-52.7.0-1.0.1.el7_4

163571 - Oracle Enterprise Linux ELSA-2018-4061 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1002101, CVE-2017-1002102

Description

The scan detected that the host is missing the following update:
ELSA-2018-4061

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2018-April/007602.html>

OEL7
x86_64
kubelet-1.9.1-2.1.5.el7
kubeadm-1.9.1-2.1.5.el7
kubernetes-1.9.1-2.1.5.el7
kubect1-1.9.1-2.1.5.el7

170951 - Amazon Linux AMI ALAS-2018-984 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5732, CVE-2018-5733

Description

The scan detected that the host is missing the following update:
ALAS-2018-984

Observation

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

<https://alas.aws.amazon.com/ALAS-2018-984.html>

Amazon Linux AMI
x86_64
dhcp-devel-4.1.1-53.P1.27.amzn1
dhcp-common-4.1.1-53.P1.27.amzn1
dhcp-4.1.1-53.P1.27.amzn1
dhclient-4.1.1-53.P1.27.amzn1
dhcp-debuginfo-4.1.1-53.P1.27.amzn1

i686
dhcp-devel-4.1.1-53.P1.27.amzn1
dhcp-common-4.1.1-53.P1.27.amzn1

dhclient-4.1.1-53.P1.27.amzn1
dhcp-4.1.1-53.P1.27.amzn1
dhcp-debuginfo-4.1.1-53.P1.27.amzn1

170953 - Amazon Linux AMI ALAS-2018-983 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17790, CVE-2018-1000073, CVE-2018-1000074, CVE-2018-1000075, CVE-2018-1000076, CVE-2018-1000077, CVE-2018-1000078, CVE-2018-1000079

Description

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

ALAS-2018-983

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2018-983.html>

Amazon Linux AMI

i686

rubygem20-io-console-0.4.2-1.31.amzn1
ruby23-devel-2.3.7-1.19.amzn1
rubygem23-psych-2.1.0.1-1.19.amzn1
rubygem24-bigdecimal-1.3.2-1.30.6.amzn1
ruby23-2.3.7-1.19.amzn1
ruby23-libs-2.3.7-1.19.amzn1
ruby22-libs-2.2.10-1.11.amzn1
ruby23-debuginfo-2.3.7-1.19.amzn1
ruby20-libs-2.0.0.648-1.31.amzn1
rubygem24-json-2.0.4-1.30.6.amzn1
rubygem23-io-console-0.4.5-1.19.amzn1
ruby20-devel-2.0.0.648-1.31.amzn1
ruby24-libs-2.4.4-1.30.6.amzn1
rubygem24-xmlrpc-0.2.1-1.30.6.amzn1
rubygem22-bigdecimal-1.2.6-1.11.amzn1
rubygem23-json-1.8.3.1-1.19.amzn1
ruby22-devel-2.2.10-1.11.amzn1
ruby20-2.0.0.648-1.31.amzn1
rubygem20-psych-2.0.0-1.31.amzn1
ruby22-debuginfo-2.2.10-1.11.amzn1
ruby24-debuginfo-2.4.4-1.30.6.amzn1
rubygem20-bigdecimal-1.2.0-1.31.amzn1
rubygem22-psych-2.0.8.1-1.11.amzn1
rubygem24-io-console-0.4.6-1.30.6.amzn1
rubygem23-bigdecimal-1.2.8-1.19.amzn1
ruby20-debuginfo-2.0.0.648-1.31.amzn1
rubygem22-io-console-0.4.3-1.11.amzn1
ruby24-devel-2.4.4-1.30.6.amzn1
ruby22-2.2.10-1.11.amzn1
rubygem24-psych-2.2.2-1.30.6.amzn1
ruby24-2.4.4-1.30.6.amzn1

noarch

ruby22-irb-2.2.10-1.11.amzn1
rubygem23-did_you_mean-1.0.0-1.19.amzn1

rubygems24-devel-2.6.14.1-1.30.6.amzn1
rubygems23-devel-2.5.2.3-1.19.amzn1
rubygems20-devel-2.0.14.1-1.31.amzn1
rubygems22-devel-2.4.5.2-1.11.amzn1
ruby24-irb-2.4.4-1.30.6.amzn1
ruby23-doc-2.3.7-1.19.amzn1
rubygem24-did_you_mean-1.1.0-1.30.6.amzn1
ruby22-doc-2.2.10-1.11.amzn1
ruby23-irb-2.3.7-1.19.amzn1
ruby20-doc-2.0.0.648-1.31.amzn1
rubygems22-2.4.5.2-1.11.amzn1
rubygems23-2.5.2.3-1.19.amzn1
ruby20-irb-2.0.0.648-1.31.amzn1
ruby24-doc-2.4.4-1.30.6.amzn1
rubygems20-2.0.14.1-1.31.amzn1
rubygems24-2.6.14.1-1.30.6.amzn1

x86_64

rubygem20-io-console-0.4.2-1.31.amzn1
ruby23-devel-2.3.7-1.19.amzn1
rubygem23-psych-2.1.0.1-1.19.amzn1
rubygem24-bigdecimal-1.3.2-1.30.6.amzn1
ruby23-2.3.7-1.19.amzn1
ruby23-libs-2.3.7-1.19.amzn1
ruby22-libs-2.2.10-1.11.amzn1
ruby23-debuginfo-2.3.7-1.19.amzn1
ruby20-libs-2.0.0.648-1.31.amzn1
rubygem24-json-2.0.4-1.30.6.amzn1
rubygem23-io-console-0.4.5-1.19.amzn1
ruby20-devel-2.0.0.648-1.31.amzn1
ruby24-libs-2.4.4-1.30.6.amzn1
rubygem24-xmlrpc-0.2.1-1.30.6.amzn1
rubygem22-bigdecimal-1.2.6-1.11.amzn1
rubygem23-json-1.8.3.1-1.19.amzn1
ruby22-devel-2.2.10-1.11.amzn1
rubygem23-bigdecimal-1.2.8-1.19.amzn1
rubygem20-psych-2.0.0-1.31.amzn1
ruby20-2.0.0.648-1.31.amzn1
ruby22-debuginfo-2.2.10-1.11.amzn1
ruby24-debuginfo-2.4.4-1.30.6.amzn1
rubygem20-bigdecimal-1.2.0-1.31.amzn1
rubygem22-psych-2.0.8.1-1.11.amzn1
rubygem24-io-console-0.4.6-1.30.6.amzn1
ruby20-debuginfo-2.0.0.648-1.31.amzn1
rubygem22-io-console-0.4.3-1.11.amzn1
ruby24-devel-2.4.4-1.30.6.amzn1
ruby22-2.2.10-1.11.amzn1
rubygem24-psych-2.2.2-1.30.6.amzn1
ruby24-2.4.4-1.30.6.amzn1

170956 - Amazon Linux AMI ALAS-2018-988 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7584

Description

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

ALAS-2018-988

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2018-988.html>

Amazon Linux AMI

x86_64

php70-7.0.29-1.28.amzn1

php70-ldap-7.0.29-1.28.amzn1

php70-recode-7.0.29-1.28.amzn1

php56-common-5.6.35-1.137.amzn1

php56-opcache-5.6.35-1.137.amzn1

php70-fpm-7.0.29-1.28.amzn1

php56-bcmath-5.6.35-1.137.amzn1

php56-5.6.35-1.137.amzn1

php70-snmp-7.0.29-1.28.amzn1

php70-debuginfo-7.0.29-1.28.amzn1

php56-devel-5.6.35-1.137.amzn1

php70-tidy-7.0.29-1.28.amzn1

php56-odbc-5.6.35-1.137.amzn1

php56-imap-5.6.35-1.137.amzn1

php56-xml-5.6.35-1.137.amzn1

php56-gmp-5.6.35-1.137.amzn1

php70-enchanted-7.0.29-1.28.amzn1

php70-bcmath-7.0.29-1.28.amzn1

php70-gmp-7.0.29-1.28.amzn1

php70-mysqlnd-7.0.29-1.28.amzn1

php56-intl-5.6.35-1.137.amzn1

php70-intl-7.0.29-1.28.amzn1

php56-soap-5.6.35-1.137.amzn1

php56-debuginfo-5.6.35-1.137.amzn1

php56-ldap-5.6.35-1.137.amzn1

php70-dbg-7.0.29-1.28.amzn1

php56-embedded-5.6.35-1.137.amzn1

php70-pdo-7.0.29-1.28.amzn1

php56-mbstring-5.6.35-1.137.amzn1

php70-devel-7.0.29-1.28.amzn1

php56-mcrypt-5.6.35-1.137.amzn1

php70-pspell-7.0.29-1.28.amzn1

php70-pgsql-7.0.29-1.28.amzn1

php70-cli-7.0.29-1.28.amzn1

php70-json-7.0.29-1.28.amzn1

php70-gd-7.0.29-1.28.amzn1

php70-zip-7.0.29-1.28.amzn1

php56-pgsql-5.6.35-1.137.amzn1

php70-soap-7.0.29-1.28.amzn1

php70-dba-7.0.29-1.28.amzn1

php56-recode-5.6.35-1.137.amzn1

php56-snmp-5.6.35-1.137.amzn1

php70-mbstring-7.0.29-1.28.amzn1

php56-mssql-5.6.35-1.137.amzn1

php56-mysqlnd-5.6.35-1.137.amzn1

php70-odbc-7.0.29-1.28.amzn1

php56-cli-5.6.35-1.137.amzn1

php70-xmlrpc-7.0.29-1.28.amzn1

php56-tidy-5.6.35-1.137.amzn1

php56-pdo-5.6.35-1.137.amzn1

php70-pdo-dblib-7.0.29-1.28.amzn1

php56-process-5.6.35-1.137.amzn1
php56-xmlrpc-5.6.35-1.137.amzn1
php56-dbg-5.6.35-1.137.amzn1
php70-common-7.0.29-1.28.amzn1
php70-process-7.0.29-1.28.amzn1
php56-dba-5.6.35-1.137.amzn1
php56-gd-5.6.35-1.137.amzn1
php70-xml-7.0.29-1.28.amzn1
php70-opcache-7.0.29-1.28.amzn1
php56-pspell-5.6.35-1.137.amzn1
php56-fpm-5.6.35-1.137.amzn1
php70-embedded-7.0.29-1.28.amzn1
php56-enchanted-5.6.35-1.137.amzn1
php70-mcrypt-7.0.29-1.28.amzn1
php70-imap-7.0.29-1.28.amzn1

i686

php70-7.0.29-1.28.amzn1
php70-ldap-7.0.29-1.28.amzn1
php70-recode-7.0.29-1.28.amzn1
php56-common-5.6.35-1.137.amzn1
php56-opcache-5.6.35-1.137.amzn1
php70-fpm-7.0.29-1.28.amzn1
php56-bcmath-5.6.35-1.137.amzn1
php56-5.6.35-1.137.amzn1
php70-snmp-7.0.29-1.28.amzn1
php70-debuginfo-7.0.29-1.28.amzn1
php56-devel-5.6.35-1.137.amzn1
php56-odbc-5.6.35-1.137.amzn1
php56-imap-5.6.35-1.137.amzn1
php56-xml-5.6.35-1.137.amzn1
php56-gmp-5.6.35-1.137.amzn1
php70-enchanted-7.0.29-1.28.amzn1
php70-bcmath-7.0.29-1.28.amzn1
php70-gmp-7.0.29-1.28.amzn1
php70-mysqlnd-7.0.29-1.28.amzn1
php56-intl-5.6.35-1.137.amzn1
php70-intl-7.0.29-1.28.amzn1
php56-soap-5.6.35-1.137.amzn1
php56-debuginfo-5.6.35-1.137.amzn1
php56-ldap-5.6.35-1.137.amzn1
php70-dbg-7.0.29-1.28.amzn1
php56-embedded-5.6.35-1.137.amzn1
php70-pdo-7.0.29-1.28.amzn1
php56-mbstring-5.6.35-1.137.amzn1
php70-devel-7.0.29-1.28.amzn1
php56-mcrypt-5.6.35-1.137.amzn1
php70-pspell-7.0.29-1.28.amzn1
php70-pgsql-7.0.29-1.28.amzn1
php70-cli-7.0.29-1.28.amzn1
php70-json-7.0.29-1.28.amzn1
php70-gd-7.0.29-1.28.amzn1
php70-zip-7.0.29-1.28.amzn1
php56-pgsql-5.6.35-1.137.amzn1
php70-soap-7.0.29-1.28.amzn1
php70-dba-7.0.29-1.28.amzn1
php56-recode-5.6.35-1.137.amzn1
php56-snmp-5.6.35-1.137.amzn1
php70-mbstring-7.0.29-1.28.amzn1
php56-mssql-5.6.35-1.137.amzn1

php56-mysqldb-5.6.35-1.137.amzn1
php70-odbc-7.0.29-1.28.amzn1
php56-cli-5.6.35-1.137.amzn1
php70-xmlrpc-7.0.29-1.28.amzn1
php56-tidy-5.6.35-1.137.amzn1
php56-pdo-5.6.35-1.137.amzn1
php70-tidy-7.0.29-1.28.amzn1
php70-pdo-dblib-7.0.29-1.28.amzn1
php56-process-5.6.35-1.137.amzn1
php56-xmlrpc-5.6.35-1.137.amzn1
php56-dbg-5.6.35-1.137.amzn1
php70-common-7.0.29-1.28.amzn1
php70-process-7.0.29-1.28.amzn1
php56-dba-5.6.35-1.137.amzn1
php56-gd-5.6.35-1.137.amzn1
php70-xml-7.0.29-1.28.amzn1
php70-opcache-7.0.29-1.28.amzn1
php56-ppspell-5.6.35-1.137.amzn1
php56-fpm-5.6.35-1.137.amzn1
php70-embedded-7.0.29-1.28.amzn1
php56-enchanted-5.6.35-1.137.amzn1
php70-mcrypt-7.0.29-1.28.amzn1
php70-imap-7.0.29-1.28.amzn1

175345 - Scientific Linux Security ERRATA Important: libvorbis on SL6.x i386/x86_64 (1804-76)

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

Risk Level: High

CVE: CVE-2018-5146

Description

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

Security ERRATA Important: libvorbis on SL6.x i386/x86_64 (1804-76)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1804&L=scientific-linux-errata&F=&S=&P=76>

SL6

i386

libvorbis-debuginfo-1.2.3-5.el6_9.1

libvorbis-1.2.3-5.el6_9.1

libvorbis-devel-1.2.3-5.el6_9.1

noarch

libvorbis-devel-docs-1.2.3-5.el6_9.1

x86_64

libvorbis-debuginfo-1.2.3-5.el6_9.1

libvorbis-1.2.3-5.el6_9.1

libvorbis-devel-1.2.3-5.el6_9.1

175346 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x i386/x86_64 (1804-409)

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146

Description

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

Security ERRATA Important: thunderbird on SL6.x i386/x86_64 (1804-409)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1804&L=scientific-linux-errata&F=&S=&P=409>

SL6

x86_64

thunderbird-52.7.0-1.el6_9

thunderbird-debuginfo-52.7.0-1.el6_9

i386

thunderbird-52.7.0-1.el6_9

thunderbird-debuginfo-52.7.0-1.el6_9

175347 - Scientific Linux Security ERRATA Important: thunderbird on SL7.x x86_64 (1804-832)

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

Risk Level: High

CVE: CVE-2018-5125, CVE-2018-5127, CVE-2018-5129, CVE-2018-5144, CVE-2018-5145, CVE-2018-5146

Description

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

Security ERRATA Important: thunderbird on SL7.x x86_64 (1804-832)

Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1804&L=scientific-linux-errata&F=&S=&P=832>

SL7

x86_64

thunderbird-debuginfo-52.7.0-1.el7_4

thunderbird-52.7.0-1.el7_4

186164 - Ubuntu Linux 14.04 USN-3619-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0861, CVE-2017-1000407, CVE-2017-11472, CVE-2017-15129, CVE-2017-16528, CVE-2017-16532, CVE-2017-16536, CVE-2017-16537, CVE-2017-16645, CVE-2017-16646, CVE-2017-16649, CVE-2017-16650, CVE-2017-16911, CVE-2017-16912, CVE-2017-16913, CVE-2017-16914, CVE-2017-16994, CVE-2017-16995, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-17741, CVE-2017-17805, CVE-2017-17806, CVE-2017-17807, CVE-2017-17862, CVE-2017-18075, CVE-2017-18203, CVE-2017-18204, CVE-2017-18208, CVE-2017-7518, CVE-2018-1000026, CVE-2018-5332, CVE-2018-5333, CVE-2018-5344, CVE-2018-6927, CVE-2018-7492, CVE-2018-8043

Description

The scan detected that the host is missing the following update:
USN-3619-2

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-April/004350.html>

Ubuntu 14.04

linux-image-powerpc-e500mc-lts-xenial_4.4.0.119.100
linux-image-generic-lpae-lts-xenial_4.4.0.119.100
linux-image-4.4.0-119-powerpc-e500mc_4.4.0-119.143~14.04.1
linux-image-powerpc64-emb-lts-xenial_4.4.0.119.100
linux-image-powerpc-smp-lts-xenial_4.4.0.119.100
linux-image-4.4.0-119-generic-lpae_4.4.0-119.143~14.04.1
linux-image-4.4.0-1016-aws_4.4.0-1016.16
linux-image-4.4.0-119-lowlatency_4.4.0-119.143~14.04.1
linux-image-aws_4.4.0.1016.16
linux-image-4.4.0-119-generic_4.4.0-119.143~14.04.1
linux-image-4.4.0-119-powerpc-smp_4.4.0-119.143~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.119.100
linux-image-lowlatency-lts-xenial_4.4.0.119.100
linux-image-4.4.0-119-powerpc64-emb_4.4.0-119.143~14.04.1
linux-image-4.4.0-119-powerpc64-smp_4.4.0-119.143~14.04.1
linux-image-generic-lts-xenial_4.4.0.119.100

186168 - Ubuntu Linux 17.10 USN-3617-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0861, CVE-2017-15129, CVE-2017-16532, CVE-2017-16537, CVE-2017-16645, CVE-2017-16646, CVE-2017-16647, CVE-2017-16649, CVE-2017-16650, CVE-2017-16994, CVE-2017-17448, CVE-2017-17450, CVE-2017-17741, CVE-2017-17805, CVE-2017-17806, CVE-2017-17807, CVE-2017-18204, CVE-2018-1000026, CVE-2018-5332, CVE-2018-5333, CVE-2018-5344

Description

The scan detected that the host is missing the following update:
USN-3617-3

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-April/004345.html>

Ubuntu 17.10

linux-image-4.13.0-1016-raspi2_4.13.0-1016.17
linux-image-raspi2_4.13.0.1016.14

186173 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3618-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7225

Description

The scan detected that the host is missing the following update:
USN-3618-1

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-April/004344.html>

Ubuntu 16.04

libvncserver1_0.9.10+dfsg-3ubuntu0.16.04.2

Ubuntu 14.04

libvncserver0_0.9.9+dfsg-1ubuntu1.3

Ubuntu 17.10

libvncclient1_0.9.11+dfsg-1ubuntu0.1

libvncserver1_0.9.11+dfsg-1ubuntu0.1

186174 - Ubuntu Linux 16.04 USN-3619-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0861, CVE-2017-1000407, CVE-2017-11472, CVE-2017-15129, CVE-2017-16528, CVE-2017-16532, CVE-2017-16536, CVE-2017-16537, CVE-2017-16645, CVE-2017-16646, CVE-2017-16649, CVE-2017-16650, CVE-2017-16911, CVE-2017-16912, CVE-2017-16913, CVE-2017-16914, CVE-2017-16994, CVE-2017-16995, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-17741, CVE-2017-17805, CVE-2017-17806, CVE-2017-17807, CVE-2017-17862, CVE-2017-18075, CVE-2017-18203, CVE-2017-18204, CVE-2017-18208, CVE-2017-7518, CVE-2018-1000026, CVE-2018-5332, CVE-2018-5333, CVE-2018-5344, CVE-2018-6927, CVE-2018-7492, CVE-2018-8043

Description

The scan detected that the host is missing the following update:
USN-3619-1

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-April/004346.html>

Ubuntu 16.04

linux-image-4.4.0-119-lowlatency_4.4.0-119.143

linux-image-4.4.0-119-generic_4.4.0-119.143

linux-image-snapdragon_4.4.0.1088.80

linux-image-4.4.0-119-powerpc-e500mc_4.4.0-119.143

linux-image-4.4.0-1054-aws_4.4.0-1054.63

linux-image-kvm_4.4.0.1020.19

linux-image-powerpc-smp_4.4.0.119.125

linux-image-4.4.0-119-generic-lpae_4.4.0-119.143

linux-image-aws_4.4.0.1054.56

linux-image-powerpc-e500mc_4.4.0.119.125
linux-image-4.4.0-1020-kvm_4.4.0-1020.25
linux-image-4.4.0-119-powerpc64-smp_4.4.0-119.143
linux-image-raspi2_4.4.0.1086.86
linux-image-4.4.0-119-powerpc64-emb_4.4.0-119.143
linux-image-4.4.0-1088-snapdragon_4.4.0-1088.93
linux-image-generic-lpae_4.4.0.119.125
linux-image-generic_4.4.0.119.125
linux-image-powerpc64-emb_4.4.0.119.125
linux-image-powerpc64-smp_4.4.0.119.125
linux-image-4.4.0-1086-raspi2_4.4.0-1086.94
linux-image-lowlatency_4.4.0.119.125
linux-image-4.4.0-119-powerpc-smp_4.4.0-119.143

193531 - Fedora Linux 27 FEDORA-2018-02e23192f5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14062

Description

The scan detected that the host is missing the following update:
FEDORA-2018-02e23192f5

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/2018/4/?count=200&page=3>

Fedora Core 27

libidn-1.34-1.fc27

193555 - Fedora Linux 28 FEDORA-2018-f749c70191 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14062

Description

The scan detected that the host is missing the following update:
FEDORA-2018-f749c70191

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/2018/4/?count=200&page=3>

Fedora Core 28

libidn-1.34-1.fc28

146574 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0876-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1058

Description

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

SUSE-SU-2018:0876-1

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-April/003872.html>

SuSE SLED 12 SP2

x86_64

postgresql94-debugsource-9.4.17-21.19.1

postgresql94-debuginfo-9.4.17-21.19.1

postgresql94-9.4.17-21.19.1

SuSE SLES 12 SP2

noarch

postgresql94-docs-9.4.17-21.19.1

x86_64

postgresql94-9.4.17-21.19.1

postgresql94-server-debuginfo-9.4.17-21.19.1

postgresql94-contrib-9.4.17-21.19.1

postgresql94-debugsource-9.4.17-21.19.1

postgresql94-contrib-debuginfo-9.4.17-21.19.1

postgresql94-server-9.4.17-21.19.1

postgresql94-debuginfo-9.4.17-21.19.1

146578 - SuSE Linux 42.3 openSUSE-SU-2018:0890-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1058

Description

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

openSUSE-SU-2018:0890-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00009.html>

SuSE Linux 42.3

i586

postgresql94-contrib-debuginfo-9.4.17-21.1

postgresql94-pltcl-9.4.17-21.1

postgresql94-devel-debuginfo-9.4.17-21.1

postgresql94-server-debuginfo-9.4.17-21.1

postgresql94-server-9.4.17-21.1

postgresql94-debugsource-9.4.17-21.1
postgresql94-plpython-9.4.17-21.1
postgresql94-devel-9.4.17-21.1
postgresql94-plperl-debuginfo-9.4.17-21.1
postgresql94-debuginfo-9.4.17-21.1
postgresql94-plpython-debuginfo-9.4.17-21.1
postgresql94-pltcl-debuginfo-9.4.17-21.1
postgresql94-libs-debugsource-9.4.17-21.1
postgresql94-plperl-9.4.17-21.1
postgresql94-contrib-9.4.17-21.1
postgresql94-9.4.17-21.1
postgresql94-test-9.4.17-21.1

noarch
postgresql94-docs-9.4.17-21.1

x86_64
postgresql94-contrib-debuginfo-9.4.17-21.1
postgresql94-pltcl-9.4.17-21.1
postgresql94-devel-debuginfo-9.4.17-21.1
postgresql94-server-debuginfo-9.4.17-21.1
postgresql94-server-9.4.17-21.1
postgresql94-debugsource-9.4.17-21.1
postgresql94-plpython-9.4.17-21.1
postgresql94-devel-9.4.17-21.1
postgresql94-plperl-debuginfo-9.4.17-21.1
postgresql94-debuginfo-9.4.17-21.1
postgresql94-plpython-debuginfo-9.4.17-21.1
postgresql94-pltcl-debuginfo-9.4.17-21.1
postgresql94-libs-debugsource-9.4.17-21.1
postgresql94-plperl-9.4.17-21.1
postgresql94-contrib-9.4.17-21.1
postgresql94-9.4.17-21.1
postgresql94-test-9.4.17-21.1

146586 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0909-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-7540, CVE-2018-7541

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0909-1

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-April/003883.html>

SuSE SLED 12 SP2

x86_64
xen-libs-32bit-4.7.5_02-43.27.1
xen-4.7.5_02-43.27.1
xen-libs-4.7.5_02-43.27.1
xen-libs-debuginfo-4.7.5_02-43.27.1
xen-debugsource-4.7.5_02-43.27.1

xen-libs-debuginfo-32bit-4.7.5_02-43.27.1

SuSE SLES 12 SP2

x86_64

xen-doc-html-4.7.5_02-43.27.1

xen-libs-32bit-4.7.5_02-43.27.1

xen-tools-4.7.5_02-43.27.1

xen-4.7.5_02-43.27.1

xen-libs-4.7.5_02-43.27.1

xen-libs-debuginfo-4.7.5_02-43.27.1

xen-tools-debuginfo-4.7.5_02-43.27.1

xen-tools-domU-4.7.5_02-43.27.1

xen-tools-domU-debuginfo-4.7.5_02-43.27.1

xen-debugsource-4.7.5_02-43.27.1

xen-libs-debuginfo-32bit-4.7.5_02-43.27.1

146588 - SuSE Linux 42.3 openSUSE-SU-2018:0883-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-7999

Description

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

openSUSE-SU-2018:0883-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00002.html>

SuSE Linux 42.3

x86_64

libgraphite2-3-1.3.1-7.3.1

graphite2-debugsource-1.3.1-7.3.1

graphite2-devel-1.3.1-7.3.1

graphite2-1.3.1-7.3.1

libgraphite2-3-debuginfo-32bit-1.3.1-7.3.1

libgraphite2-3-debuginfo-1.3.1-7.3.1

graphite2-debuginfo-1.3.1-7.3.1

libgraphite2-3-32bit-1.3.1-7.3.1

i586

libgraphite2-3-1.3.1-7.3.1

graphite2-debugsource-1.3.1-7.3.1

graphite2-devel-1.3.1-7.3.1

graphite2-1.3.1-7.3.1

libgraphite2-3-debuginfo-1.3.1-7.3.1

graphite2-debuginfo-1.3.1-7.3.1

170952 - Amazon Linux AMI ALAS-2018-985 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6893, CVE-2018-5950

Description

The scan detected that the host is missing the following update:
ALAS-2018-985

Observation

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

<https://alas.aws.amazon.com/ALAS-2018-985.html>

Amazon Linux AMI

x86_64

mailman-debuginfo-2.1.15-26.21.amzn1

mailman-2.1.15-26.21.amzn1

i686

mailman-debuginfo-2.1.15-26.21.amzn1

mailman-2.1.15-26.21.amzn1

170958 - Amazon Linux AMI ALAS-2018-990 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1058

Description

The scan detected that the host is missing the following update:
ALAS-2018-990

Observation

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

<https://alas.aws.amazon.com/ALAS-2018-990.html>

Amazon Linux AMI

x86_64

postgresql94-docs-9.4.17-1.74.amzn1

postgresql96-9.6.8-1.80.amzn1

postgresql95-devel-9.5.12-1.78.amzn1

postgresql93-plpython26-9.3.22-1.70.amzn1

postgresql93-9.3.22-1.70.amzn1

postgresql93-test-9.3.22-1.70.amzn1

postgresql94-plperl-9.4.17-1.74.amzn1

postgresql95-plpython27-9.5.12-1.78.amzn1

postgresql95-docs-9.5.12-1.78.amzn1

postgresql93-plpython27-9.3.22-1.70.amzn1

postgresql95-contrib-9.5.12-1.78.amzn1

postgresql96-static-9.6.8-1.80.amzn1

postgresql93-debuginfo-9.3.22-1.70.amzn1

postgresql94-devel-9.4.17-1.74.amzn1

postgresql96-devel-9.6.8-1.80.amzn1

postgresql95-plpython26-9.5.12-1.78.amzn1

postgresql95-static-9.5.12-1.78.amzn1

postgresql94-test-9.4.17-1.74.amzn1

postgresql96-test-9.6.8-1.80.amzn1

postgresql95-test-9.5.12-1.78.amzn1

postgresql93-devel-9.3.22-1.70.amzn1
postgresql96-plperl-9.6.8-1.80.amzn1
postgresql94-plpython26-9.4.17-1.74.amzn1
postgresql94-9.4.17-1.74.amzn1
postgresql93-pltcl-9.3.22-1.70.amzn1
postgresql96-debuginfo-9.6.8-1.80.amzn1
postgresql93-libs-9.3.22-1.70.amzn1
postgresql95-libs-9.5.12-1.78.amzn1
postgresql96-plpython26-9.6.8-1.80.amzn1
postgresql96-server-9.6.8-1.80.amzn1
postgresql94-server-9.4.17-1.74.amzn1
postgresql93-plperl-9.3.22-1.70.amzn1
postgresql94-plpython27-9.4.17-1.74.amzn1
postgresql93-contrib-9.3.22-1.70.amzn1
postgresql96-libs-9.6.8-1.80.amzn1
postgresql95-plperl-9.5.12-1.78.amzn1
postgresql94-debuginfo-9.4.17-1.74.amzn1
postgresql96-plpython27-9.6.8-1.80.amzn1
postgresql95-9.5.12-1.78.amzn1
postgresql95-server-9.5.12-1.78.amzn1
postgresql94-libs-9.4.17-1.74.amzn1
postgresql96-contrib-9.6.8-1.80.amzn1
postgresql96-docs-9.6.8-1.80.amzn1
postgresql95-debuginfo-9.5.12-1.78.amzn1
postgresql93-docs-9.3.22-1.70.amzn1
postgresql93-server-9.3.22-1.70.amzn1
postgresql94-contrib-9.4.17-1.74.amzn1

i686

postgresql94-libs-9.4.17-1.74.amzn1
postgresql96-9.6.8-1.80.amzn1
postgresql95-devel-9.5.12-1.78.amzn1
postgresql96-devel-9.6.8-1.80.amzn1
postgresql93-server-9.3.22-1.70.amzn1
postgresql93-test-9.3.22-1.70.amzn1
postgresql94-plperl-9.4.17-1.74.amzn1
postgresql95-plpython27-9.5.12-1.78.amzn1
postgresql95-docs-9.5.12-1.78.amzn1
postgresql93-plpython27-9.3.22-1.70.amzn1
postgresql95-contrib-9.5.12-1.78.amzn1
postgresql96-static-9.6.8-1.80.amzn1
postgresql93-debuginfo-9.3.22-1.70.amzn1
postgresql94-devel-9.4.17-1.74.amzn1
postgresql93-contrib-9.3.22-1.70.amzn1
postgresql95-plpython26-9.5.12-1.78.amzn1
postgresql95-static-9.5.12-1.78.amzn1
postgresql94-test-9.4.17-1.74.amzn1
postgresql96-test-9.6.8-1.80.amzn1
postgresql95-test-9.5.12-1.78.amzn1
postgresql93-devel-9.3.22-1.70.amzn1
postgresql96-plperl-9.6.8-1.80.amzn1
postgresql94-plpython26-9.4.17-1.74.amzn1
postgresql94-9.4.17-1.74.amzn1
postgresql93-pltcl-9.3.22-1.70.amzn1
postgresql96-debuginfo-9.6.8-1.80.amzn1
postgresql93-libs-9.3.22-1.70.amzn1
postgresql93-plpython26-9.3.22-1.70.amzn1
postgresql95-libs-9.5.12-1.78.amzn1
postgresql96-plpython26-9.6.8-1.80.amzn1
postgresql96-server-9.6.8-1.80.amzn1

postgresql94-server-9.4.17-1.74.amzn1
postgresql93-plperl-9.3.22-1.70.amzn1
postgresql94-plpython27-9.4.17-1.74.amzn1
postgresql96-libs-9.6.8-1.80.amzn1
postgresql95-plperl-9.5.12-1.78.amzn1
postgresql94-debuginfo-9.4.17-1.74.amzn1
postgresql96-plpython27-9.6.8-1.80.amzn1
postgresql95-9.5.12-1.78.amzn1
postgresql95-server-9.5.12-1.78.amzn1
postgresql94-docs-9.4.17-1.74.amzn1
postgresql96-contrib-9.6.8-1.80.amzn1
postgresql96-docs-9.6.8-1.80.amzn1
postgresql95-debuginfo-9.5.12-1.78.amzn1
postgresql93-docs-9.3.22-1.70.amzn1
postgresql93-9.3.22-1.70.amzn1
postgresql94-contrib-9.4.17-1.74.amzn1

193521 - Fedora Linux 27 FEDORA-2018-143886fdbd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6926, CVE-2017-6927, CVE-2017-6928, CVE-2017-6929, CVE-2017-6930, CVE-2017-6931, CVE-2017-6932

Description

The scan detected that the host is missing the following update:
FEDORA-2018-143886fdbd

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

Fedora Core 27

drupal7-7.58-1.fc27

193523 - Fedora Linux 28 FEDORA-2018-4a699532d3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6893

Description

The scan detected that the host is missing the following update:
FEDORA-2018-4a699532d3

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/2018/4/?count=200&page=2>

Fedora Core 28

mailman-2.1.26-1.fc28

193541 - Fedora Linux 28 FEDORA-2018-8a208fba70 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14731, CVE-2017-2816, CVE-2017-2920

Description

The scan detected that the host is missing the following update:
FEDORA-2018-8a208fba70

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/2018/4/?count=200&page=2>

Fedora Core 28

libofx-0.9.10-6.fc28

193546 - Fedora Linux 27 FEDORA-2018-c442aad4dc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18233, CVE-2017-18234, CVE-2017-18235, CVE-2017-18236, CVE-2017-18237, CVE-2018-7728, CVE-2018-7729, CVE-2018-7730, CVE-2018-7731

Description

The scan detected that the host is missing the following update:
FEDORA-2018-c442aad4dc

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/2018/4/?count=200&page=5>

Fedora Core 27

exempi-2.4.5-1.fc27

193548 - Fedora Linux 26 FEDORA-2018-d8269e4262 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6926, CVE-2017-6927, CVE-2017-6928, CVE-2017-6929, CVE-2017-6930, CVE-2017-6931, CVE-2017-6932

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d8269e4262

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

Fedora Core 26

drupal7-7.58-1.fc26

23341 - (K43121447) F5 BIG-IP Client SSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2018-5502

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in how virtual servers handle SSL client certificate authentication. Successful exploitation could allow attackers to cause a denial-of-service.

131077 - Debian Linux 8.0 DSA-4166-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

DSA-4166-1

Observation

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

For more information see:

<http://www.debian.org/security/2018/dsa-4166>

Debian 8.0

all

openjdk-7-jre-lib_7u171-2.6.13-1~deb8u1
openjdk-7-jdk_7u171-2.6.13-1~deb8u1
openjdk-7-dbg_7u171-2.6.13-1~deb8u1
icedtea-7-jre-jamvm_7u171-2.6.13-1~deb8u1
openjdk-7-jre-headless_7u171-2.6.13-1~deb8u1
openjdk-7-demo_7u171-2.6.13-1~deb8u1
openjdk-7-jre-zero_7u171-2.6.13-1~deb8u1
openjdk-7-doc_7u171-2.6.13-1~deb8u1
openjdk-7-source_7u171-2.6.13-1~deb8u1
openjdk-7-jre_7u171-2.6.13-1~deb8u1

141912 - Red Hat Enterprise Linux RHSA-2018-0980 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15906

Description

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

RHSA-2018-0980

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00016.html>

RHEL7D

x86_64

openssh-clients-7.4p1-16.el7

openssh-debuginfo-7.4p1-16.el7

openssh-7.4p1-16.el7

openssh-askpass-7.4p1-16.el7

openssh-ldap-7.4p1-16.el7

openssh-cavs-7.4p1-16.el7

openssh-keycat-7.4p1-16.el7

pam_ssh_agent_auth-0.10.3-2.16.el7

openssh-server-sysvinit-7.4p1-16.el7

openssh-server-7.4p1-16.el7

RHEL7S

x86_64

openssh-clients-7.4p1-16.el7

openssh-debuginfo-7.4p1-16.el7

openssh-7.4p1-16.el7

openssh-askpass-7.4p1-16.el7

openssh-ldap-7.4p1-16.el7

openssh-cavs-7.4p1-16.el7

openssh-keycat-7.4p1-16.el7

pam_ssh_agent_auth-0.10.3-2.16.el7

openssh-server-sysvinit-7.4p1-16.el7

openssh-server-7.4p1-16.el7

RHEL7WS

x86_64

openssh-clients-7.4p1-16.el7

openssh-debuginfo-7.4p1-16.el7

openssh-7.4p1-16.el7

openssh-askpass-7.4p1-16.el7

openssh-ldap-7.4p1-16.el7

openssh-cavs-7.4p1-16.el7

openssh-keycat-7.4p1-16.el7

pam_ssh_agent_auth-0.10.3-2.16.el7

openssh-server-sysvinit-7.4p1-16.el7

openssh-server-7.4p1-16.el7

146575 - SuSE Linux 42.3 openSUSE-SU-2018:0882-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11468

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0882-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00001.html>

SuSE Linux 42.3
x86_64
docker-distribution-registry-2.6.2-11.1
docker-distribution-registry-debuginfo-2.6.2-11.1
docker-distribution-debugsource-2.6.2-11.1

170954 - Amazon Linux AMI ALAS-2018-980 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15135, CVE-2018-1054

Description

The scan detected that the host is missing the following update:
ALAS-2018-980

Observation

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

<https://alas.aws.amazon.com/ALAS-2018-980.html>

Amazon Linux AMI
x86_64
389-ds-base-libs-1.3.6.1-28.54.amzn1
389-ds-base-debuginfo-1.3.6.1-28.54.amzn1
389-ds-base-1.3.6.1-28.54.amzn1
389-ds-base-devel-1.3.6.1-28.54.amzn1
389-ds-base-snmp-1.3.6.1-28.54.amzn1

i686
389-ds-base-debuginfo-1.3.6.1-28.54.amzn1
389-ds-base-libs-1.3.6.1-28.54.amzn1
389-ds-base-snmp-1.3.6.1-28.54.amzn1
389-ds-base-1.3.6.1-28.54.amzn1
389-ds-base-devel-1.3.6.1-28.54.amzn1

170959 - Amazon Linux AMI ALAS-2018-991 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6247, CVE-2018-6248, CVE-2018-6249, CVE-2018-6250, CVE-2018-6251, CVE-2018-6252, CVE-2018-6253

Description

The scan detected that the host is missing the following update:
ALAS-2018-991

Observation

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

<https://alas.aws.amazon.com/ALAS-2018-991.html>

Amazon Linux AMI

x86_64

nvidia-384.125-2017.09.109.amzn1

nvidia-dkms-384.125-2017.09.109.amzn1

178602 - Gentoo Linux GLSA-201804-07 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-201804-07

Observation

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

<https://security.gentoo.org/glsa/201804-07>

Affected packages:

app-emulation/libvirt < 4.1.0

178603 - Gentoo Linux GLSA-201804-01 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-201804-01

Observation

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

<https://security.gentoo.org/glsa/201804-01>

Affected packages:

dev-libs/libxslt < 1.1.30

178604 - Gentoo Linux GLSA-201804-09 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-201804-09

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201804-09>

Affected packages:

app-emulation/spice-vdagent < 0.17.0_p20180319

178605 - Gentoo Linux GLSA-201804-10 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-201804-10

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201804-10>

Affected packages:

dev-php/ZendFramework <= 1.12.9

178606 - Gentoo Linux GLSA-201804-02 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-201804-02

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201804-02>

Affected packages:

sys-libs/glibc < 2.25-r11

178607 - Gentoo Linux GLSA-201804-08 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-201804-08

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201804-08>

Affected packages:

app-emulation/qemu < 2.11.1-r1

178608 - Gentoo Linux GLSA-201804-05 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-201804-05

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201804-05>

Affected packages:

net-misc/dhcp < 4.3.6_p1

178609 - Gentoo Linux GLSA-201804-04 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-201804-04

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201804-04>

Affected packages:
net-misc/curl < 7.59.0

178610 - Gentoo Linux GLSA-201804-03 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-201804-03

Observation

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

<https://security.gentoo.org/glsa/201804-03>

Affected packages:
app-text/poppler < 0.61.1

178611 - Gentoo Linux GLSA-201804-06 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-201804-06

Observation

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

<https://security.gentoo.org/glsa/201804-06>

Affected packages:
mail-client/mailx < 8.1.2.20160123

178612 - Gentoo Linux GLSA-201803-14 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-201803-14

Observation

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

<https://security.gentoo.org/glsa/201803-14>

Affected packages:

mail-client/thunderbird < 52.6.0

mail-client/thunderbird-bin < 52.6.0

186167 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3622-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16612

Description

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

USN-3622-1

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-April/004353.html>

Ubuntu 16.04

libwayland-client0_1.12.0-1~ubuntu16.04.3

libwayland-server0_1.12.0-1~ubuntu16.04.3

libwayland-bin_1.12.0-1~ubuntu16.04.3

libwayland-doc_1.12.0-1~ubuntu16.04.3

libwayland-dev_1.12.0-1~ubuntu16.04.3

libwayland-cursor0_1.12.0-1~ubuntu16.04.3

Ubuntu 14.04

libwayland-cursor0_1.4.0-1ubuntu1.1

Ubuntu 17.10

libwayland-cursor0_1.14.0-1ubuntu0.1

193538 - Fedora Linux 28 FEDORA-2018-d187b44f75 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-2779, CVE-2017-11550

Description

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

FEDORA-2018-d187b44f75

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

Fedora Core 28

libid3tag-0.15.1b-28.fc28

193561 - Fedora Linux 27 FEDORA-2018-e06468b832 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-2779, CVE-2017-11550

Description

The scan detected that the host is missing the following update:
FEDORA-2018-e06468b832

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

Fedora Core 27

libid3tag-0.15.1b-26.fc27

132443 - Oracle VM OVMSA-2018-0029 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2018-April/000839.html>

OVM3.2

x86_64

xen-4.1.3-25.el5.223.166

xen-tools-4.1.3-25.el5.223.166

xen-devel-4.1.3-25.el5.223.166

141913 - Red Hat Enterprise Linux RHSA-2018-0666 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11368, CVE-2017-7562

Description

The scan detected that the host is missing the following update:
RHSA-2018-0666

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00019.html>

RHEL7D

x86_64
libkadm5-1.15.1-18.el7
krb5-server-ldap-1.15.1-18.el7
krb5-pkinit-1.15.1-18.el7
krb5-server-1.15.1-18.el7
krb5-libs-1.15.1-18.el7
krb5-debuginfo-1.15.1-18.el7
krb5-workstation-1.15.1-18.el7
krb5-devel-1.15.1-18.el7

RHEL7S

x86_64
krb5-pkinit-1.15.1-18.el7
libkadm5-1.15.1-18.el7
krb5-server-ldap-1.15.1-18.el7
krb5-devel-1.15.1-18.el7
krb5-server-1.15.1-18.el7
krb5-libs-1.15.1-18.el7
krb5-debuginfo-1.15.1-18.el7
krb5-workstation-1.15.1-18.el7

RHEL7WS

x86_64
krb5-pkinit-1.15.1-18.el7
libkadm5-1.15.1-18.el7
krb5-server-ldap-1.15.1-18.el7
krb5-devel-1.15.1-18.el7
krb5-server-1.15.1-18.el7
krb5-libs-1.15.1-18.el7
krb5-debuginfo-1.15.1-18.el7
krb5-workstation-1.15.1-18.el7

141914 - Red Hat Enterprise Linux RHSA-2018-0998 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3736, CVE-2017-3737, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
RHSA-2018-0998

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00013.html>

RHEL7D

x86_64
openssl-devel-1.0.2k-12.el7
openssl-static-1.0.2k-12.el7
openssl-perl-1.0.2k-12.el7
openssl-libs-1.0.2k-12.el7
openssl-1.0.2k-12.el7
openssl-debuginfo-1.0.2k-12.el7

RHEL7S

x86_64
openssl-devel-1.0.2k-12.el7
openssl-static-1.0.2k-12.el7
openssl-perl-1.0.2k-12.el7
openssl-libs-1.0.2k-12.el7
openssl-1.0.2k-12.el7
openssl-debuginfo-1.0.2k-12.el7

RHEL7WS

x86_64
openssl-devel-1.0.2k-12.el7
openssl-static-1.0.2k-12.el7
openssl-perl-1.0.2k-12.el7
openssl-libs-1.0.2k-12.el7
openssl-1.0.2k-12.el7
openssl-debuginfo-1.0.2k-12.el7

141916 - Red Hat Enterprise Linux RHSA-2018-0855 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
RHSA-2018-0855

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00011.html>

RHEL7D

x86_64
ntpdate-4.2.6p5-28.el7
sntp-4.2.6p5-28.el7
ntp-4.2.6p5-28.el7
ntp-debuginfo-4.2.6p5-28.el7

noarch

ntp-perl-4.2.6p5-28.el7
ntp-doc-4.2.6p5-28.el7

RHEL7S

noarch

ntp-perl-4.2.6p5-28.el7
ntp-doc-4.2.6p5-28.el7

x86_64
ntpdate-4.2.6p5-28.el7
snmp-4.2.6p5-28.el7
ntp-4.2.6p5-28.el7
ntp-debuginfo-4.2.6p5-28.el7

RHEL7WS
x86_64
ntpdate-4.2.6p5-28.el7
snmp-4.2.6p5-28.el7
ntp-4.2.6p5-28.el7
ntp-debuginfo-4.2.6p5-28.el7

noarch
ntp-perl-4.2.6p5-28.el7
ntp-doc-4.2.6p5-28.el7

141928 - Red Hat Enterprise Linux RHSA-2018-0842 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15131

Description

The scan detected that the host is missing the following update:
RHSA-2018-0842

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00018.html>

RHEL7D
x86_64
xdg-user-dirs-0.15-5.el7
xdg-user-dirs-debuginfo-0.15-5.el7

RHEL7S
x86_64
xdg-user-dirs-0.15-5.el7
xdg-user-dirs-debuginfo-0.15-5.el7

RHEL7WS
x86_64
xdg-user-dirs-0.15-5.el7
xdg-user-dirs-debuginfo-0.15-5.el7

146577 - SuSE SLES 11 SP4 SUSE-SU-2018:0874-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12133

Description

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

SUSE-SU-2018:0874-1

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-April/003870.html>

SuSE SLES 11 SP4

i686

glibc-devel-2.11.3-17.110.9.2

glibc-2.11.3-17.110.9.2

i586

glibc-info-2.11.3-17.110.9.2

glibc-html-2.11.3-17.110.9.2

glibc-profile-2.11.3-17.110.9.2

glibc-devel-2.11.3-17.110.9.2

glibc-locale-2.11.3-17.110.9.2

nscd-2.11.3-17.110.9.2

glibc-2.11.3-17.110.9.2

glibc-i18ndata-2.11.3-17.110.9.2

x86_64

glibc-info-2.11.3-17.110.9.2

glibc-32bit-2.11.3-17.110.9.2

glibc-profile-32bit-2.11.3-17.110.9.2

glibc-html-2.11.3-17.110.9.2

glibc-profile-2.11.3-17.110.9.2

glibc-devel-2.11.3-17.110.9.2

glibc-locale-32bit-2.11.3-17.110.9.2

glibc-devel-32bit-2.11.3-17.110.9.2

glibc-locale-2.11.3-17.110.9.2

nscd-2.11.3-17.110.9.2

glibc-2.11.3-17.110.9.2

glibc-i18ndata-2.11.3-17.110.9.2

146582 - SuSE Linux 42.3 openSUSE-SU-2018:0894-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11524

Description

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

openSUSE-SU-2018:0894-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00013.html>

SuSE Linux 42.3

x86_64

libGraphicsMagick++-Q16-12-debuginfo-1.3.25-82.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-82.1
GraphicsMagick-devel-1.3.25-82.1
libGraphicsMagick3-config-1.3.25-82.1
libGraphicsMagick++-devel-1.3.25-82.1
libGraphicsMagick++-Q16-12-1.3.25-82.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-82.1
GraphicsMagick-debuginfo-1.3.25-82.1
perl-GraphicsMagick-1.3.25-82.1
GraphicsMagick-1.3.25-82.1
perl-GraphicsMagick-debuginfo-1.3.25-82.1
libGraphicsMagickWand-Q16-2-1.3.25-82.1
GraphicsMagick-debugsource-1.3.25-82.1
libGraphicsMagick-Q16-3-1.3.25-82.1

i586

libGraphicsMagick++-Q16-12-debuginfo-1.3.25-82.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-82.1
GraphicsMagick-devel-1.3.25-82.1
libGraphicsMagick3-config-1.3.25-82.1
libGraphicsMagick++-devel-1.3.25-82.1
libGraphicsMagick++-Q16-12-1.3.25-82.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-82.1
GraphicsMagick-debuginfo-1.3.25-82.1
perl-GraphicsMagick-1.3.25-82.1
GraphicsMagick-1.3.25-82.1
perl-GraphicsMagick-debuginfo-1.3.25-82.1
libGraphicsMagickWand-Q16-2-1.3.25-82.1
GraphicsMagick-debugsource-1.3.25-82.1
libGraphicsMagick-Q16-3-1.3.25-82.1

146585 - SuSE Linux 42.3 openSUSE-SU-2018:0914-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15298

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0914-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-04/msg00019.html>

SuSE Linux 42.3

i586

git-svn-debuginfo-2.13.6-10.1
git-2.13.6-10.1
git-core-debuginfo-2.13.6-10.1
git-debugsource-2.13.6-10.1
git-daemon-2.13.6-10.1
git-svn-2.13.6-10.1
git-web-2.13.6-10.1
git-credential-gnome-keyring-2.13.6-10.1
git-gui-2.13.6-10.1

git-email-2.13.6-10.1
gitk-2.13.6-10.1
git-credential-gnome-keyring-debuginfo-2.13.6-10.1
git-arch-2.13.6-10.1
git-daemon-debuginfo-2.13.6-10.1
git-cvs-2.13.6-10.1
git-core-2.13.6-10.1

noarch
git-doc-2.13.6-10.1

x86_64
git-svn-debuginfo-2.13.6-10.1
git-2.13.6-10.1
git-core-debuginfo-2.13.6-10.1
git-debugsource-2.13.6-10.1
git-daemon-2.13.6-10.1
git-svn-2.13.6-10.1
git-web-2.13.6-10.1
git-credential-gnome-keyring-2.13.6-10.1
git-gui-2.13.6-10.1
git-email-2.13.6-10.1
gitk-2.13.6-10.1
git-credential-gnome-keyring-debuginfo-2.13.6-10.1
git-arch-2.13.6-10.1
git-daemon-debuginfo-2.13.6-10.1
git-cvs-2.13.6-10.1
git-core-2.13.6-10.1

193525 - Fedora Linux 26 FEDORA-2018-a233dae4ab Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1304, CVE-2018-1305

Description

The scan detected that the host is missing the following update:
FEDORA-2018-a233dae4ab

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/2018/4/?count=200&page=5>

Fedora Core 26

tomcat-8.0.50-1.fc26

193526 - Fedora Linux 26 FEDORA-2018-d5aa3e1d90 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15953, CVE-2017-15954, CVE-2017-15955

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d5aa3e1d90

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/2018/4/?count=200&page=3>

Fedora Core 26

bchunk-1.2.2-1.fc26

193528 - Fedora Linux 27 FEDORA-2018-1217b02061 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15953, CVE-2017-15954, CVE-2017-15955

Description

The scan detected that the host is missing the following update:
FEDORA-2018-1217b02061

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/2018/4/?count=200&page=3>

Fedora Core 27

bchunk-1.2.2-1.fc27

193537 - Fedora Linux 28 FEDORA-2018-60ec960104 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15953, CVE-2017-15954, CVE-2017-15955

Description

The scan detected that the host is missing the following update:
FEDORA-2018-60ec960104

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/2018/4/?count=200&page=3>

Fedora Core 28

bchunk-1.2.2-1.fc28

193540 - Fedora Linux 27 FEDORA-2018-50f0da5d38 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1304, CVE-2018-1305

Description

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

FEDORA-2018-50f0da5d38

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/2018/4/?count=200&page=5>

Fedora Core 27

tomcat-8.0.50-1.fc27

193543 - Fedora Linux 28 FEDORA-2018-1aeac808ce Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5711

Description

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

FEDORA-2018-1aeac808ce

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/2018/4/?count=200&page=5>

Fedora Core 28

gd-2.2.5-3.fc28

193547 - Fedora Linux 26 FEDORA-2018-331af74020 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5711

Description

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

FEDORA-2018-331af74020

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/2018/4/?count=200&page=5>

Fedora Core 26

gd-2.2.5-2.fc26

193551 - Fedora Linux 28 FEDORA-2018-1c9f6768cf Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-7728, CVE-2018-7729, CVE-2018-7730, CVE-2018-7731

Description

The scan detected that the host is missing the following update:
FEDORA-2018-1c9f6768cf

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/2018/4/?count=200&page=5>

Fedora Core 28

exempi-2.4.5-1.fc28

88934 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2018-096-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000156

Description

The scan detected that the host is missing the following update:
SSA:2018-096-01

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.529530>

Slackware 14.0

x86_64

patch-2.7.6-x86_64-1

Slackware 13.37

x86_64

patch-2.7.4-x86_64-2

Slackware 14.1

x86_64

patch-2.7.6-x86_64-1

Slackware 13.1

x86_64

patch-2.7.4-x86_64-2

Slackware 14.2
x86_64
patch-2.7.6-x86_64-1

i586
patch-2.7.6-i586-1

Slackware 13.0
x86_64
patch-2.7.4-x86_64-2

131074 - Debian Linux 8.0 DSA-4168-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-8741

Description

The scan detected that the host is missing the following update:
DSA-4168-1

Observation

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

<http://www.debian.org/security/2018/dsa-4168>

Debian 8.0
all
squirrelmail_2:1.4.23~svn20120406-2+deb8u2

131075 - Debian Linux 8.0, 9.0 DSA-4167-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000097

Description

The scan detected that the host is missing the following update:
DSA-4167-1

Observation

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

<http://www.debian.org/security/2018/dsa-4167>

Debian 8.0
all
sharutils_1:4.14-2+deb8u1

Debian 9.0
all
sharutils_1:4.15.2-2+deb9u1

131076 - Debian Linux 8.0, 9.0 DSA-4165-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-8763, CVE-2018-8764

Description

The scan detected that the host is missing the following update:
DSA-4165-1

Observation

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

<http://www.debian.org/security/2018/dsa-4165>

Debian 8.0

all

ldap-account-manager_4.7.1-1+deb8u1

Debian 9.0

all

ldap-account-manager_5.5-1+deb9u1

141924 - Red Hat Enterprise Linux RHSA-2018-0913 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1063

Description

The scan detected that the host is missing the following update:
RHSA-2018-0913

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00015.html>

RHEL7D

x86_64

policycoreutils-gui-2.5-22.el7

policycoreutils-devel-2.5-22.el7

policycoreutils-restorecond-2.5-22.el7

policycoreutils-debuginfo-2.5-22.el7

policycoreutils-python-2.5-22.el7

policycoreutils-newrole-2.5-22.el7

policycoreutils-2.5-22.el7

policycoreutils-sandbox-2.5-22.el7

RHEL7S

x86_64

policycoreutils-gui-2.5-22.el7

policycoreutils-devel-2.5-22.el7

policycoreutils-restorecond-2.5-22.el7

polycycoreutils-debuginfo-2.5-22.el7
polycycoreutils-python-2.5-22.el7
polycycoreutils-newrole-2.5-22.el7
polycycoreutils-2.5-22.el7
polycycoreutils-sandbox-2.5-22.el7

RHEL7WS

x86_64

polycycoreutils-gui-2.5-22.el7
polycycoreutils-devel-2.5-22.el7
polycycoreutils-restorecond-2.5-22.el7
polycycoreutils-debuginfo-2.5-22.el7
polycycoreutils-python-2.5-22.el7
polycycoreutils-newrole-2.5-22.el7
polycycoreutils-2.5-22.el7
polycycoreutils-sandbox-2.5-22.el7

182666 - FreeBSD FreeBSD Vt Console Memory Disclosure (a5cf3ecd-38db-11e8-8b7f-a4badb2f469b)

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

Risk Level: Low

CVE: CVE-2018-6917

Description

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

FreeBSD -- vt console memory disclosure (a5cf3ecd-38db-11e8-8b7f-a4badb2f469b)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/a5cf3ecd-38db-11e8-8b7f-a4badb2f469b.html>

Affected packages:

11.1 <= FreeBSD-kernel < 11.1_9

10.4 <= FreeBSD-kernel < 10.4_8

10.3 <= FreeBSD-kernel < 10.3_29

182667 - FreeBSD Flash Player Multiple Vulnerabilities (5c6f7482-3ced-11e8-b157-6451062f0f7a)

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

Risk Level: Low

CVE: CVE-2018-4932, CVE-2018-4933, CVE-2018-4934, CVE-2018-4935, CVE-2018-4936, CVE-2018-4937

Description

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

Flash Player -- multiple vulnerabilities (5c6f7482-3ced-11e8-b157-6451062f0f7a)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/5c6f7482-3ced-11e8-b157-6451062f0f7a.html>

Affected packages:

linux-flashplayer < 29.0.0.140

182668 - FreeBSD Gitlab Multiple Vulnerabilities (085a087b-3897-11e8-ac53-d8cb8abf62dd)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

Gitlab -- multiple vulnerabilities (085a087b-3897-11e8-ac53-d8cb8abf62dd)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/085a087b-3897-11e8-ac53-d8cb8abf62dd.html>

Affected packages:

10.6.0 <= gitlab < 10.6.3

10.5.0 <= gitlab < 10.5.7

8.6 <= gitlab < 10.4.7

182669 - FreeBSD FreeBSD Ipcrash Or Denial Of Service (c0c5afef-38db-11e8-8b7f-a4badb2f469b)

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

Risk Level: Low

CVE: CVE-2018-6918

Description

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

FreeBSD -- ipsec crash or denial of service (c0c5afef-38db-11e8-8b7f-a4badb2f469b)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/c0c5afef-38db-11e8-8b7f-a4badb2f469b.html>

Affected packages:

11.1 <= FreeBSD-kernel < 11.1_9

10.4 <= FreeBSD-kernel < 10.4_8

10.3 <= FreeBSD-kernel < 10.3_29

186169 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3623-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

USN-3623-1

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-April/004354.html>

Ubuntu 16.04

python3-distupgrade_16.04.25

Ubuntu 14.04

python3-distupgrade_0.220.10

Ubuntu 17.10

python3-distupgrade_17.10.11

186171 - Ubuntu Linux 14.04, 16.04 USN-3596-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5125, CVE-2018-5126, CVE-2018-5127, CVE-2018-5128, CVE-2018-5129, CVE-2018-5130, CVE-2018-5131, CVE-2018-5132, CVE-2018-5133, CVE-2018-5134, CVE-2018-5135, CVE-2018-5136, CVE-2018-5137, CVE-2018-5140, CVE-2018-5141, CVE-2018-5142, CVE-2018-5143

Description

The scan detected that the host is missing the following update:
USN-3596-2

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-April/004351.html>

Ubuntu 14.04

firefox_59.0.2+build1-0ubuntu0.14.04.4

Ubuntu 16.04

firefox_59.0.2+build1-0ubuntu0.16.04.3

193519 - Fedora Linux 27 FEDORA-2018-9490b422e7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-0739

Description

The scan detected that the host is missing the following update:
FEDORA-2018-9490b422e7

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

Fedora Core 27

compat-openssl10-1.0.2o-1.fc27

193520 - Fedora Linux 28 FEDORA-2018-aa5e668e64 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-aa5e668e64

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/2018/4/?count=200&page=2>

Fedora Core 28

thunderbird-52.7.0-1.fc28

193522 - Fedora Linux 28 FEDORA-2018-c40addbe0d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1002150

Description

The scan detected that the host is missing the following update:
FEDORA-2018-c40addbe0d

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/2018/4/?count=200&page=3>

Fedora Core 28

koji-1.15.1-1.fc28

193524 - Fedora Linux 26 FEDORA-2018-a61baabbac 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-a61baabbac

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

Fedora Core 26

firefox-59.0.2-1.fc26

193527 - Fedora Linux 27 FEDORA-2018-c923533479 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-c923533479

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/2018/4/?count=200&page=3>

Fedora Core 27

webkitgtk4-2.20.0-1.fc27

193529 - Fedora Linux 27 FEDORA-2018-375e3244b6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15710, CVE-2017-15715, CVE-2018-1283, CVE-2018-1301, CVE-2018-1303, CVE-2018-1312

Description

The scan detected that the host is missing the following update:
FEDORA-2018-375e3244b6

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

Fedora Core 27

httpd-2.4.33-2.fc27

193530 - Fedora Linux 26 FEDORA-2018-505e83d30e 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-2018-505e83d30e

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/2018/4/?count=200&page=3>

Fedora Core 26

webkitgtk4-2.20.0-1.fc26

193532 - Fedora Linux 28 FEDORA-2018-7eae87ec86 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1060, CVE-2018-1061

Description

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

FEDORA-2018-7eae87ec86

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/2018/4/?count=200&page=3>

Fedora Core 28

python3-3.6.5-1.fc28

193533 - Fedora Linux 28 FEDORA-2018-8049b2c488 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-7158, CVE-2018-7159, CVE-2018-7160

Description

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

FEDORA-2018-8049b2c488

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/2018/4/?count=200&page=2>

Fedora Core 28

nodejs-8.11.0-1.fc28

193534 - Fedora Linux 28 FEDORA-2018-6744ca470d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15710, CVE-2017-15715, CVE-2018-1283, CVE-2018-1301, CVE-2018-1303, CVE-2018-1312

Description

The scan detected that the host is missing the following update:
FEDORA-2018-6744ca470d

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

Fedora Core 28

httpd-2.4.33-2.fc28

193535 - Fedora Linux 28 FEDORA-2018-eec13e2e8d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1302

Description

The scan detected that the host is missing the following update:
FEDORA-2018-eec13e2e8d

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

Fedora Core 28

mod_http2-1.10.16-1.fc28

193536 - Fedora Linux 27 FEDORA-2018-99f551e4ff Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-18248

Description

The scan detected that the host is missing the following update:
FEDORA-2018-99f551e4ff

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/2018/4/?count=200&page=3>

Fedora Core 27

cups-2.2.4-9.fc27

193539 - Fedora Linux 26 FEDORA-2018-1b4f1158e2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-0739

Description

The scan detected that the host is missing the following update:
FEDORA-2018-1b4f1158e2

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

Fedora Core 26

compat-openssl10-1.0.2o-1.fc26

193542 - Fedora Linux 26 FEDORA-2018-aa8de9d66a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1060, CVE-2018-1061

Description

The scan detected that the host is missing the following update:
FEDORA-2018-aa8de9d66a

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

Fedora Core 26

python3-docs-3.6.5-1.fc26

python3-3.6.5-1.fc26

python-pip-9.0.3-1.fc26

193544 - Fedora Linux 26 FEDORA-2018-e672eaf4df Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-7158, CVE-2018-7159, CVE-2018-7160

Description

The scan detected that the host is missing the following update:
FEDORA-2018-e672eaf4df

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/2018/4/?count=200&page=3>

Fedora Core 26

nodejs-6.14.0-1.fc26

193545 - Fedora Linux 27 FEDORA-2018-0a95bff197 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1302

Description

The scan detected that the host is missing the following update:
FEDORA-2018-0a95bff197

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

Fedora Core 27

mod_http2-1.10.16-1.fc27

193549 - Fedora Linux 27 FEDORA-2018-f61d8bdd42 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1002150

Description

The scan detected that the host is missing the following update:
FEDORA-2018-f61d8bdd42

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/2018/4/?count=200&page=3>

Fedora Core 27

koji-1.15.1-1.fc27

193550 - Fedora Linux 27 FEDORA-2018-12f92ff831 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-2018-12f92ff831

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/2018/4/?count=200&page=3>

Fedora Core 27

php-7.1.16-1.fc27

193552 - Fedora Linux 28 FEDORA-2018-2f696a3be3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-0739

Description

The scan detected that the host is missing the following update:
FEDORA-2018-2f696a3be3

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

Fedora Core 28

compat-openssl10-1.0.2o-1.fc28

193553 - Fedora Linux 26 FEDORA-2018-ec5f10e626 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-18248

Description

The scan detected that the host is missing the following update:
FEDORA-2018-ec5f10e626

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

Fedora Core 26

cups-2.2.2-9.fc26

193554 - Fedora Linux 28 FEDORA-2018-2ef9089e89 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-2018-2ef9089e89

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/2018/4/?count=200&page=2>

Fedora Core 28

wordpress-4.9.5-1.fc28

193556 - Fedora Linux 26 FEDORA-2018-6f2df5ab6c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000140

Description

The scan detected that the host is missing the following update:
FEDORA-2018-6f2df5ab6c

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/2018/4/?count=200&page=3>

Fedora Core 26

librelp-1.2.15-1.fc26

193557 - Fedora Linux 26 FEDORA-2018-c71dd2e199 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-c71dd2e199

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/2018/4/?count=200&page=3>

Fedora Core 26

php-7.1.16-1.fc26

193558 - Fedora Linux 27 FEDORA-2018-223d8fc52a 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-2018-223d8fc52a

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

Fedora Core 27

java-1.8.0-openjdk-aarch32-1.8.0.161-1.180220.fc27

193559 - Fedora Linux 27 FEDORA-2018-2f9d3604d6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000140

Description

The scan detected that the host is missing the following update:
FEDORA-2018-2f9d3604d6

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/2018/4/?count=200&page=3>

Fedora Core 27

librelp-1.2.15-1.fc27

193560 - Fedora Linux 27 FEDORA-2018-a042f795b2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1060, CVE-2018-1061

Description

The scan detected that the host is missing the following update:
FEDORA-2018-a042f795b2

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

Fedora Core 27

python-pip-9.0.3-1.fc27
python3-3.6.5-1.fc27
python3-docs-3.6.5-1.fc27

141920 - Red Hat Enterprise Linux RHSA-2018-0849 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-11671

Description

The scan detected that the host is missing the following update:
RHSA-2018-0849

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-April/msg00014.html>

RHEL7D
x86_64
gcc-go-4.8.5-28.el7
libgo-devel-4.8.5-28.el7
gcc-objc-4.8.5-28.el7
libatomic-static-4.8.5-28.el7
libgcc-4.8.5-28.el7
libgo-static-4.8.5-28.el7
libitm-static-4.8.5-28.el7
libgfortran-4.8.5-28.el7
libstdc++-devel-4.8.5-28.el7
libmudflap-devel-4.8.5-28.el7
libgfortran-static-4.8.5-28.el7
libobjc-4.8.5-28.el7
libtsan-static-4.8.5-28.el7
libgnat-devel-4.8.5-28.el7
libmudflap-4.8.5-28.el7
gcc-4.8.5-28.el7

gcc-plugin-devel-4.8.5-28.el7
libstdc++-static-4.8.5-28.el7
cpp-4.8.5-28.el7
gcc-gnat-4.8.5-28.el7
libitm-4.8.5-28.el7
gcc-base-debuginfo-4.8.5-28.el7
libgnat-4.8.5-28.el7
libstdc++-docs-4.8.5-28.el7
libasan-static-4.8.5-28.el7
libatomic-4.8.5-28.el7
gcc-objc++-4.8.5-28.el7
libgomp-4.8.5-28.el7
libstdc++-4.8.5-28.el7
libitm-devel-4.8.5-28.el7
libquadmath-4.8.5-28.el7
libquadmath-devel-4.8.5-28.el7
libgo-4.8.5-28.el7
libquadmath-static-4.8.5-28.el7
libgnat-static-4.8.5-28.el7
gcc-debuginfo-4.8.5-28.el7
libmudflap-static-4.8.5-28.el7
libtsan-4.8.5-28.el7
libasan-4.8.5-28.el7
gcc-c++-4.8.5-28.el7
gcc-gfortran-4.8.5-28.el7

RHEL7S

x86_64
gcc-go-4.8.5-28.el7
libquadmath-devel-4.8.5-28.el7
gcc-objc-4.8.5-28.el7
libatomic-static-4.8.5-28.el7
libgcc-4.8.5-28.el7
libgo-static-4.8.5-28.el7
libitm-static-4.8.5-28.el7
libgfortran-4.8.5-28.el7
libstdc++-devel-4.8.5-28.el7
libmudflap-devel-4.8.5-28.el7
libgfortran-static-4.8.5-28.el7
libobjc-4.8.5-28.el7
libtsan-static-4.8.5-28.el7
libgnat-devel-4.8.5-28.el7
libmudflap-4.8.5-28.el7
gcc-4.8.5-28.el7
gcc-plugin-devel-4.8.5-28.el7
libstdc++-static-4.8.5-28.el7
cpp-4.8.5-28.el7
gcc-gnat-4.8.5-28.el7
libitm-4.8.5-28.el7
gcc-base-debuginfo-4.8.5-28.el7
libgnat-4.8.5-28.el7
libstdc++-docs-4.8.5-28.el7
libasan-static-4.8.5-28.el7
libatomic-4.8.5-28.el7
gcc-objc++-4.8.5-28.el7
libgomp-4.8.5-28.el7
libstdc++-4.8.5-28.el7
libitm-devel-4.8.5-28.el7
libgo-devel-4.8.5-28.el7
libquadmath-4.8.5-28.el7

libquadmath-static-4.8.5-28.el7
libgo-4.8.5-28.el7
libgnat-static-4.8.5-28.el7
gcc-debuginfo-4.8.5-28.el7
libmudflap-static-4.8.5-28.el7
libtsan-4.8.5-28.el7
libasan-4.8.5-28.el7
gcc-c++-4.8.5-28.el7
gcc-gfortran-4.8.5-28.el7

RHEL7WS

x86_64
gcc-go-4.8.5-28.el7
libquadmath-devel-4.8.5-28.el7
gcc-objc-4.8.5-28.el7
libatomic-static-4.8.5-28.el7
libgcc-4.8.5-28.el7
libgo-static-4.8.5-28.el7
libitm-static-4.8.5-28.el7
libgfortran-4.8.5-28.el7
libstdc++-devel-4.8.5-28.el7
libmudflap-devel-4.8.5-28.el7
libgfortran-static-4.8.5-28.el7
libobjc-4.8.5-28.el7
libtsan-static-4.8.5-28.el7
libgnat-devel-4.8.5-28.el7
libmudflap-4.8.5-28.el7
gcc-4.8.5-28.el7
gcc-plugin-devel-4.8.5-28.el7
libstdc++-static-4.8.5-28.el7
cpp-4.8.5-28.el7
gcc-gnat-4.8.5-28.el7
libitm-4.8.5-28.el7
gcc-base-debuginfo-4.8.5-28.el7
libgnat-4.8.5-28.el7
libstdc++-docs-4.8.5-28.el7
libasan-static-4.8.5-28.el7
libatomic-4.8.5-28.el7
gcc-objc++-4.8.5-28.el7
libgomp-4.8.5-28.el7
libstdc++-4.8.5-28.el7
libitm-devel-4.8.5-28.el7
libgo-devel-4.8.5-28.el7
libquadmath-4.8.5-28.el7
libquadmath-static-4.8.5-28.el7
libgo-4.8.5-28.el7
libgnat-static-4.8.5-28.el7
gcc-debuginfo-4.8.5-28.el7
libmudflap-static-4.8.5-28.el7
libtsan-4.8.5-28.el7
libasan-4.8.5-28.el7
gcc-c++-4.8.5-28.el7
gcc-gfortran-4.8.5-28.el7

23430 - Microsoft Office 2016 Click-To-Run April 2018 Updates

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run.

Observation

Microsoft Office 2016 Click-to-Run is an alternative to the Windows Installer-based (MSI) installation method of the popular office suite.

Multiple issues are present in some versions of Microsoft Office 2016 Click-to-Run. The flaws are present in multiple components. Such defects could lead the product to software vulnerabilities, malfunction or unexpected behavior in some of its affected components.

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.

186142 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3601-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000127

Update Details

Risk is updated

23288 - (BSRT-2018-001) BlackBerry UEM Management Console Reflected Cross-Site-Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-17442

Update Details

Risk is updated

193438 - Fedora Linux 26 FEDORA-2018-b0f6a5bdbc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-7563

Update Details

Risk is updated

193449 - Fedora Linux 27 FEDORA-2018-1b67b3a3a3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-7563

Update Details

Risk is updated

182664 - FreeBSD Gitlab Multiple Vulnerabilities (dc0c201c-31da-11e8-ac53-d8cb8abf62dd)

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

Risk Level: Low

CVE: CVE-2018-8801

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2018 McAfee, Inc.

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