2018-JAN-11
FSL version 7.5.993

MCAFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

170917 - Amazon Linux AMI ALAS-2018-940 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16820

Description

The scan detected that the host is missing the following update:
ALAS-2018-940

Observation

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

https://alas.aws.amazon.com/ALAS-2018-940.html

Amazon Linux AMI
x86_64
libcollectdclient-devel-5.8.0-2.19.amzn1
collectd-bind-5.8.0-2.19.amzn1
collectd-email-5.8.0-2.19.amzn1
collectd-write_sensu-5.8.0-2.19.amzn1
collectd-utils-5.8.0-2.19.amzn1
collectd-iptables-5.8.0-2.19.amzn1
collectd-chrony-5.8.0-2.19.amzn1
collectd-nginx-5.8.0-2.19.amzn1
collectd-synproxy-5.8.0-2.19.amzn1
collectd-lua-5.8.0-2.19.amzn1
collectd-zookeeper-5.8.0-2.19.amzn1
collectd-write_tsdb-5.8.0-2.19.amzn1
collectd-rrdcached-5.8.0-2.19.amzn1
collectd-curl-5.8.0-2.19.amzn1
collectd-notify_email-5.8.0-2.19.amzn1
collectd-mysql-5.8.0-2.19.amzn1
collectd-mcelog-5.8.0-2.19.amzn1
collectd-disk-5.8.0-2.19.amzn1
collectd-postgresql-5.8.0-2.19.amzn1
collectd-dbi-5.8.0-2.19.amzn1
collectd-write_http-5.8.0-2.19.amzn1
collectd-java-5.8.0-2.19.amzn1
collectd-netlink-5.8.0-2.19.amzn1
collectd-memcachec-5.8.0-2.19.amzn1
collectd-dns-5.8.0-2.19.amzn1
libcollectdclient-5.8.0-2.19.amzn1
collectd-snmp_agent-5.8.0-2.19.amzn1
collectd-5.8.0-2.19.amzn1

collectd-python-5.8.0-2.19.amzn1
collectd-debuginfo-5.8.0-2.19.amzn1
collectd-web-5.8.0-2.19.amzn1
collectd-varnish-5.8.0-2.19.amzn1
collectd-ipvs-5.8.0-2.19.amzn1
collectd-gmond-5.8.0-2.19.amzn1
collectd-ipmi-5.8.0-2.19.amzn1
collectd-hugepages-5.8.0-2.19.amzn1
collectd-openldap-5.8.0-2.19.amzn1
collectd-curl_xml-5.8.0-2.19.amzn1
collectd-rrdtool-5.8.0-2.19.amzn1
collectd-snmp-5.8.0-2.19.amzn1
collectd-drbd-5.8.0-2.19.amzn1
collectd-apache-5.8.0-2.19.amzn1
perl-Collectd-5.8.0-2.19.amzn1
collectd-generic-jmx-5.8.0-2.19.amzn1
collectd-lvm-5.8.0-2.19.amzn1
collectd-amqp-5.8.0-2.19.amzn1

i686
libcollectdclient-devel-5.8.0-2.19.amzn1
collectd-snmp-5.8.0-2.19.amzn1
collectd-email-5.8.0-2.19.amzn1
collectd-write_sensu-5.8.0-2.19.amzn1
collectd-utils-5.8.0-2.19.amzn1
collectd-iptables-5.8.0-2.19.amzn1
collectd-chrony-5.8.0-2.19.amzn1
collectd-nginx-5.8.0-2.19.amzn1
collectd-synproxy-5.8.0-2.19.amzn1
collectd-lua-5.8.0-2.19.amzn1
collectd-zookeeper-5.8.0-2.19.amzn1
collectd-write_tsdb-5.8.0-2.19.amzn1
collectd-web-5.8.0-2.19.amzn1
collectd-curl-5.8.0-2.19.amzn1
collectd-notify_email-5.8.0-2.19.amzn1
collectd-mysql-5.8.0-2.19.amzn1
collectd-mcelog-5.8.0-2.19.amzn1
collectd-disk-5.8.0-2.19.amzn1
collectd-postgresql-5.8.0-2.19.amzn1
collectd-dbi-5.8.0-2.19.amzn1
collectd-write_http-5.8.0-2.19.amzn1
libcollectdclient-5.8.0-2.19.amzn1
collectd-netlink-5.8.0-2.19.amzn1
collectd-memcachec-5.8.0-2.19.amzn1
collectd-dns-5.8.0-2.19.amzn1
collectd-debuginfo-5.8.0-2.19.amzn1
collectd-snmp_agent-5.8.0-2.19.amzn1
collectd-5.8.0-2.19.amzn1
collectd-python-5.8.0-2.19.amzn1
collectd-bind-5.8.0-2.19.amzn1
collectd-rrdcached-5.8.0-2.19.amzn1
collectd-varnish-5.8.0-2.19.amzn1
collectd-ipvs-5.8.0-2.19.amzn1
collectd-gmond-5.8.0-2.19.amzn1
collectd-ipmi-5.8.0-2.19.amzn1
collectd-hugepages-5.8.0-2.19.amzn1
collectd-openldap-5.8.0-2.19.amzn1
collectd-curl_xml-5.8.0-2.19.amzn1
collectd-rrdtool-5.8.0-2.19.amzn1
collectd-drbd-5.8.0-2.19.amzn1

collectd-apache-5.8.0-2.19.amzn1
collectd-java-5.8.0-2.19.amzn1
perl-Collectd-5.8.0-2.19.amzn1
collectd-generic-jmx-5.8.0-2.19.amzn1
collectd-lvm-5.8.0-2.19.amzn1
collectd-amqp-5.8.0-2.19.amzn1

22972 - Microsoft Office 2016 Click-To-Run January 2018 Updates

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

Risk Level: High

CVE: CVE-2018-0791, CVE-2018-0792, CVE-2018-0793, CVE-2018-0794, CVE-2018-0795, CVE-2018-0796, CVE-2018-0798, CVE-2018-0801, CVE-2018-0802, CVE-2018-0804, CVE-2018-0805, CVE-2018-0806, CVE-2018-0807, CVE-2018-0812

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.

22894 - (VMSA-2017-0021) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: High

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

Description

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

Observation

VMware Workstation is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Pro. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code and cause denial of service.

130986 - Debian Linux 9.0 DSA-4080-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11144, CVE-2017-11145, CVE-2017-11628, CVE-2017-12932, CVE-2017-12933, CVE-2017-12934, CVE-2017-16642

Description

The scan detected that the host is missing the following update:
DSA-4080-1

Observation

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

http://www.debian.org/security/2018/dsa-4080

Debian 9.0
all
php7.0_7.0.27-0+deb9u1

130987 - Debian Linux 8.0 DSA-4082-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000407, CVE-2017-1000410, CVE-2017-15868, CVE-2017-16538, CVE-2017-16939, 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-2017-5754, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
DSA-4082-1

Observation

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

http://www.debian.org/security/2018/dsa-4082

Debian 8.0
all
input-modules-3.16.0-4-armmp-di_3.16.51-3+deb8u1
crypto-dm-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
input-modules-3.16.0-4-powerpc64-di_3.16.51-3+deb8u1
virtio-modules-3.16.0-4-sb1-bcm91250a-di_3.16.51-3+deb8u1
core-modules-3.16.0-4-armmp-di_3.16.51-3+deb8u1
jfs-modules-3.16.0-4-powerpc64-di_3.16.51-3+deb8u1
loop-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
input-modules-3.16.0-4-octeon-di_3.16.51-3+deb8u1
crypto-dm-modules-3.16.0-4-amd64-di_3.16.51-3+deb8u1
pata-modules-3.16.0-4-loongson-2e-di_3.16.51-3+deb8u1
nic-usb-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
scsi-modules-3.16.0-4-octeon-di_3.16.51-3+deb8u1
squashfs-modules-3.16.0-4-loongson-2e-di_3.16.51-3+deb8u1
xfs-modules-3.16.0-4-powerpc-di_3.16.51-3+deb8u1
cdrom-core-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
virtio-modules-3.16.0-4-powerpc-di_3.16.51-3+deb8u1
sata-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
jfs-modules-3.16.0-4-r5k-ip32-di_3.16.51-3+deb8u1
fat-modules-3.16.0-4-powerpc64-di_3.16.51-3+deb8u1
squashfs-modules-3.16.0-4-versatile-di_3.16.51-3+deb8u1
scsi-extra-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
btrfs-modules-3.16.0-4-loongson-3-di_3.16.51-3+deb8u1
usb-storage-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
virtio-modules-3.16.0-4-powerpc64le-di_3.16.51-3+deb8u1
squashfs-modules-3.16.0-4-loongson-3-di_3.16.51-3+deb8u1
sata-modules-3.16.0-4-powerpc-di_3.16.51-3+deb8u1
scsi-common-modules-3.16.0-4-powerpc-di_3.16.51-3+deb8u1
crypto-modules-3.16.0-4-s390x-di_3.16.51-3+deb8u1
ext4-modules-3.16.0-4-686-pae-di_3.16.51-3+deb8u1

fuse-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
loop-modules-3.16.0-4-r4k-ip22-di_3.16.51-3+deb8u1
cdrom-core-modules-3.16.0-4-versatile-di_3.16.51-3+deb8u1
kernel-image-3.16.0-4-r4k-ip22-di_3.16.51-3+deb8u1
scsi-extra-modules-3.16.0-4-powerpc64-di_3.16.51-3+deb8u1
fat-modules-3.16.0-4-armmp-di_3.16.51-3+deb8u1
loop-modules-3.16.0-4-armmp-di_3.16.51-3+deb8u1
fuse-modules-3.16.0-4-kirkwood-di_3.16.51-3+deb8u1
fuse-modules-3.16.0-4-r5k-ip32-di_3.16.51-3+deb8u1
nic-usb-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
nic-usb-modules-3.16.0-4-loongson-2e-di_3.16.51-3+deb8u1
firewire-core-modules-3.16.0-4-loongson-2e-di_3.16.51-3+deb8u1
fat-modules-3.16.0-4-orion5x-di_3.16.51-3+deb8u1
scsi-extra-modules-3.16.0-4-sb1-bcm91250a-di_3.16.51-3+deb8u1
cdrom-core-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
crypto-modules-3.16.0-4-r4k-ip22-di_3.16.51-3+deb8u1
udf-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
linux-image-3.16.0-4-r4k-ip22_3.16.51-3+deb8u1
mouse-modules-3.16.0-4-amd64-di_3.16.51-3+deb8u1
event-modules-3.16.0-4-amd64-di_3.16.51-3+deb8u1
nbd-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
speakup-modules-3.16.0-4-amd64-di_3.16.51-3+deb8u1
sata-modules-3.16.0-4-octeon-di_3.16.51-3+deb8u1
md-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
kernel-image-3.16.0-4-octeon-di_3.16.51-3+deb8u1
input-modules-3.16.0-4-sb1-bcm91250a-di_3.16.51-3+deb8u1
nic-shared-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
usb-storage-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
crypto-dm-modules-3.16.0-4-orion5x-di_3.16.51-3+deb8u1
mouse-modules-3.16.0-4-powerpc64le-di_3.16.51-3+deb8u1
usb-storage-modules-3.16.0-4-versatile-di_3.16.51-3+deb8u1
scsi-extra-modules-3.16.0-4-loongson-3-di_3.16.51-3+deb8u1
affs-modules-3.16.0-4-powerpc64-di_3.16.51-3+deb8u1
sata-modules-3.16.0-4-sb1-bcm91250a-di_3.16.51-3+deb8u1
sata-modules-3.16.0-4-amd64-di_3.16.51-3+deb8u1
scsi-core-modules-3.16.0-4-octeon-di_3.16.51-3+deb8u1
sata-modules-3.16.0-4-orion5x-di_3.16.51-3+deb8u1
usb-serial-modules-3.16.0-4-powerpc64le-di_3.16.51-3+deb8u1
nic-modules-3.16.0-4-armmp-di_3.16.51-3+deb8u1
cdrom-core-modules-3.16.0-4-orion5x-di_3.16.51-3+deb8u1
btrfs-modules-3.16.0-4-powerpc-di_3.16.51-3+deb8u1
core-modules-3.16.0-4-versatile-di_3.16.51-3+deb8u1
isofs-modules-3.16.0-4-kirkwood-di_3.16.51-3+deb8u1
ata-modules-3.16.0-4-sb1-bcm91250a-di_3.16.51-3+deb8u1
usb-serial-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
multipath-modules-3.16.0-4-amd64-di_3.16.51-3+deb8u1
linux-compiler-gcc-4.8-x86_3.16.51-3+deb8u1
usb-modules-3.16.0-4-686-pae-di_3.16.51-3+deb8u1
ata-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
firewire-core-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
ppp-modules-3.16.0-4-loongson-3-di_3.16.51-3+deb8u1
fat-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
scsi-extra-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
kernel-image-3.16.0-4-versatile-di_3.16.51-3+deb8u1
fb-modules-3.16.0-4-kirkwood-di_3.16.51-3+deb8u1
event-modules-3.16.0-4-686-pae-di_3.16.51-3+deb8u1
scsi-core-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
crc-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
crypto-dm-modules-3.16.0-4-powerpc64-di_3.16.51-3+deb8u1
nic-wireless-modules-3.16.0-4-armmp-di_3.16.51-3+deb8u1

md-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
nbd-modules-3.16.0-4-powerpc64le-di_3.16.51-3+deb8u1
nic-shared-modules-3.16.0-4-sb1-bcm91250a-di_3.16.51-3+deb8u1
nic-shared-modules-3.16.0-4-powerpc64le-di_3.16.51-3+deb8u1
cdrom-core-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
loop-modules-3.16.0-4-orion5x-di_3.16.51-3+deb8u1
usb-storage-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
squashfs-modules-3.16.0-4-powerpc-di_3.16.51-3+deb8u1
linux-headers-3.16.0-4-586_3.16.51-3+deb8u1
affs-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
event-modules-3.16.0-4-sb1-bcm91250a-di_3.16.51-3+deb8u1
mmc-core-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
event-modules-3.16.0-4-powerpc64le-di_3.16.51-3+deb8u1
sound-modules-3.16.0-4-octeon-di_3.16.51-3+deb8u1
nic-modules-3.16.0-4-s390x-di_3.16.51-3+deb8u1
fat-modules-3.16.0-4-versatile-di_3.16.51-3+deb8u1
scsi-common-modules-3.16.0-4-octeon-di_3.16.51-3+deb8u1
linux-image-3.16.0-4-r5k-ip32_3.16.51-3+deb8u1
scsi-core-modules-3.16.0-4-powerpc64-di_3.16.51-3+deb8u1
speakup-modules-3.16.0-4-686-pae-di_3.16.51-3+deb8u1
hyperv-modules-3.16.0-4-amd64-di_3.16.51-3+deb8u1
mouse-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
sata-modules-3.16.0-4-loongson-3-di_3.16.51-3+deb8u1
nic-shared-modules-3.16.0-4-armmp-di_3.16.51-3+deb8u1
core-modules-3.16.0-4-orion5x-di_3.16.51-3+deb8u1
loop-modules-3.16.0-4-r5k-ip32-di_3.16.51-3+deb8u1
efi-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
linux-support-3.16.0-4_3.16.51-3+deb8u1
input-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
event-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
fat-modules-3.16.0-4-s390x-di_3.16.51-3+deb8u1
crc-modules-3.16.0-4-686-pae-di_3.16.51-3+deb8u1
squashfs-modules-3.16.0-4-r4k-ip22-di_3.16.51-3+deb8u1
usb-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
virtio-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
scsi-extra-modules-3.16.0-4-loongson-2f-di_3.16.51-3+deb8u1
btrfs-modules-3.16.0-4-versatile-di_3.16.51-3+deb8u1
ata-modules-3.16.0-4-powerpc64le-di_3.16.51-3+deb8u1
usb-modules-3.16.0-4-arm64-di_3.16.51-3+deb8u1
scsi-modules-3.16.0-4-4kc-malta-di_3.16.51-3+deb8u1
xfs-modules-3.16.0-4-586-di_3.16.51-3+deb8u1
sound-modules-3.16.0-4-sb1-bcm91250a-di_3.16.51-3+deb8u1

130988 - Debian Linux 8.0 DSA-4081-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11142, CVE-2017-11143, CVE-2017-11144, CVE-2017-11145, CVE-2017-11628, CVE-2017-12933, CVE-2017-16642

Description

The scan detected that the host is missing the following update:
DSA-4081-1

Observation

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

http://www.debian.org/security/2018/dsa-4081

Debian 8.0
all
php5_5.6.33+dfsg-0+deb8u1

132424 - Oracle VM OVMSA-2018-0005 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15592, CVE-2017-15595, CVE-2017-17044, CVE-2017-17045, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0005

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000817.html

OVM3.4
x86_64
xen-tools-4.4.4-105.0.30.el6
xen-4.4.4-105.0.30.el6

132426 - Oracle VM OVMSA-2018-0003 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0003

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000814.html

OVM3.4
x86_64
microcode_ctl-1.17-25.2.0.1.el6_9

141835 - Red Hat Enterprise Linux RHSA-2018-0061 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7829, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

Description

The scan detected that the host is missing the following update:
RHSA-2018-0061

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-January/msg00053.html

RHEL7S
x86_64
thunderbird-debuginfo-52.5.2-1.el7_4
thunderbird-52.5.2-1.el7_4

RHEL6S
i386
thunderbird-52.5.2-1.el6_9
thunderbird-debuginfo-52.5.2-1.el6_9

x86_64
thunderbird-52.5.2-1.el6_9
thunderbird-debuginfo-52.5.2-1.el6_9

RHEL6WS
x86_64
thunderbird-52.5.2-1.el6_9
thunderbird-debuginfo-52.5.2-1.el6_9

i386
thunderbird-52.5.2-1.el6_9
thunderbird-debuginfo-52.5.2-1.el6_9

RHEL7D
x86_64
thunderbird-debuginfo-52.5.2-1.el7_4
thunderbird-52.5.2-1.el7_4

RHEL6D
x86_64
thunderbird-52.5.2-1.el6_9
thunderbird-debuginfo-52.5.2-1.el6_9

i386
thunderbird-52.5.2-1.el6_9
thunderbird-debuginfo-52.5.2-1.el6_9

RHEL7WS
x86_64
thunderbird-debuginfo-52.5.2-1.el7_4
thunderbird-52.5.2-1.el7_4

146209 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0055-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000445, CVE-2017-1000476, CVE-2017-11449, CVE-2017-11751, CVE-2017-12430, CVE-2017-12642, CVE-2017-14249, CVE-2017-17680, CVE-2017-17882, CVE-2017-9409

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0055-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003582.html

SuSE SLED 12 SP2
x86_64
ImageMagick-debugsource-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.23.1
ImageMagick-debuginfo-6.8.8.1-71.23.1
libMagick++-6_Q16-3-6.8.8.1-71.23.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.23.1
ImageMagick-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.23.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.23.1
libMagickWand-6_Q16-1-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.23.1

SuSE SLES 12 SP3
x86_64
libMagickCore-6_Q16-1-6.8.8.1-71.23.1
ImageMagick-debuginfo-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.23.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.23.1
ImageMagick-debugsource-6.8.8.1-71.23.1
libMagickWand-6_Q16-1-6.8.8.1-71.23.1

SuSE SLES 12 SP2
x86_64
libMagickCore-6_Q16-1-6.8.8.1-71.23.1
ImageMagick-debuginfo-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.23.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.23.1
ImageMagick-debugsource-6.8.8.1-71.23.1
libMagickWand-6_Q16-1-6.8.8.1-71.23.1

SuSE SLED 12 SP3
x86_64
ImageMagick-debugsource-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.23.1
ImageMagick-debuginfo-6.8.8.1-71.23.1
libMagick++-6_Q16-3-6.8.8.1-71.23.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.23.1
ImageMagick-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.23.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.23.1
libMagickWand-6_Q16-1-6.8.8.1-71.23.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.23.1

146210 - SuSE Linux 42.3 openSUSE-SU-2018:0022-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0022-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00001.html

SuSE Linux 42.3
x86_64
kernel-debug-devel-4.4.104-39.1
kernel-obs-build-debugsource-4.4.104-39.1
kernel-obs-build-4.4.104-39.1
kernel-default-debuginfo-4.4.104-39.1
kselftests-kmp-default-debuginfo-4.4.104-39.1
kernel-obs-qa-4.4.104-39.1
kernel-vanilla-debuginfo-4.4.104-39.1
kernel-debug-base-debuginfo-4.4.104-39.1
kernel-default-4.4.104-39.1
kselftests-kmp-vanilla-debuginfo-4.4.104-39.1
kernel-debug-devel-debuginfo-4.4.104-39.1
kernel-vanilla-debugsource-4.4.104-39.1
kselftests-kmp-debug-debuginfo-4.4.104-39.1
kernel-debug-debugsource-4.4.104-39.1
kernel-debug-base-4.4.104-39.1
kernel-vanilla-devel-4.4.104-39.1
kernel-vanilla-4.4.104-39.1
kernel-debug-debuginfo-4.4.104-39.1
kernel-default-devel-4.4.104-39.1
kernel-default-debugsource-4.4.104-39.1
kselftests-kmp-default-4.4.104-39.1
kernel-default-base-4.4.104-39.1
kselftests-kmp-debug-4.4.104-39.1
kernel-default-base-debuginfo-4.4.104-39.1
kernel-vanilla-base-debuginfo-4.4.104-39.1
kernel-vanilla-base-4.4.104-39.1
kernel-debug-4.4.104-39.1
kernel-syms-4.4.104-39.1
kselftests-kmp-vanilla-4.4.104-39.1

noarch
kernel-docs-pdf-4.4.104-39.1
kernel-docs-html-4.4.104-39.1
kernel-macros-4.4.104-39.1
kernel-devel-4.4.104-39.1
kernel-docs-4.4.104-39.1
kernel-source-4.4.104-39.1
kernel-source-vanilla-4.4.104-39.1

146211 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0044-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0044-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00014.html

SuSE Linux 42.2
i586
gimp-plugins-python-2.8.18-2.6.2
libgimp-2_0-0-debuginfo-2.8.18-2.6.2
gimp-plugin-aa-debuginfo-2.8.18-2.6.2
gimp-devel-2.8.18-2.6.2
gimp-debuginfo-2.8.18-2.6.2
gimp-debugsource-2.8.18-2.6.2
libgimp-2_0-0-2.8.18-2.6.2
gimp-2.8.18-2.6.2
gimp-plugin-aa-2.8.18-2.6.2
gimp-devel-debuginfo-2.8.18-2.6.2
gimp-plugins-python-debuginfo-2.8.18-2.6.2
libgimpui-2_0-0-2.8.18-2.6.2
libgimpui-2_0-0-debuginfo-2.8.18-2.6.2

noarch
gimp-lang-2.8.18-2.6.2

x86_64
gimp-plugins-python-2.8.18-2.6.2
libgimp-2_0-0-debuginfo-2.8.18-2.6.2
libgimp-2_0-0-debuginfo-32bit-2.8.18-2.6.2
gimp-plugin-aa-debuginfo-2.8.18-2.6.2
gimp-devel-2.8.18-2.6.2
libgimpui-2_0-0-32bit-2.8.18-2.6.2
libgimp-2_0-0-32bit-2.8.18-2.6.2
gimp-debuginfo-2.8.18-2.6.2
gimp-debugsource-2.8.18-2.6.2
libgimp-2_0-0-2.8.18-2.6.2
gimp-2.8.18-2.6.2
gimp-plugin-aa-2.8.18-2.6.2
gimp-devel-debuginfo-2.8.18-2.6.2
libgimpui-2_0-0-debuginfo-32bit-2.8.18-2.6.2
gimp-plugins-python-debuginfo-2.8.18-2.6.2
libgimpui-2_0-0-2.8.18-2.6.2
libgimpui-2_0-0-debuginfo-2.8.18-2.6.2

SuSE Linux 42.3
i586
libgimpui-2_0-0-2.8.18-6.3
gimp-plugin-aa-2.8.18-6.3
libgimpui-2_0-0-debuginfo-2.8.18-6.3
gimp-devel-debuginfo-2.8.18-6.3
gimp-debugsource-2.8.18-6.3
gimp-2.8.18-6.3

libgimp-2_0-0-debuginfo-2.8.18-6.3
libgimp-2_0-0-2.8.18-6.3
gimp-plugin-aa-debuginfo-2.8.18-6.3
gimp-plugins-python-debuginfo-2.8.18-6.3
gimp-debuginfo-2.8.18-6.3
gimp-plugins-python-2.8.18-6.3
gimp-devel-2.8.18-6.3

noarch
gimp-lang-2.8.18-6.3

x86_64
libgimpui-2_0-0-2.8.18-6.3
gimp-plugin-aa-2.8.18-6.3
libgimpui-2_0-0-debuginfo-2.8.18-6.3
libgimp-2_0-0-32bit-2.8.18-6.3
gimp-devel-debuginfo-2.8.18-6.3
libgimpui-2_0-0-debuginfo-32bit-2.8.18-6.3
gimp-debugsource-2.8.18-6.3
gimp-2.8.18-6.3
libgimp-2_0-0-debuginfo-2.8.18-6.3
libgimp-2_0-0-2.8.18-6.3
gimp-plugin-aa-debuginfo-2.8.18-6.3
gimp-plugins-python-debuginfo-2.8.18-6.3
libgimp-2_0-0-debuginfo-32bit-2.8.18-6.3
libgimpui-2_0-0-32bit-2.8.18-6.3
gimp-debuginfo-2.8.18-6.3
gimp-plugins-python-2.8.18-6.3
gimp-devel-2.8.18-6.3

146212 - SuSE Linux 42.2 openSUSE-SU-2018:0027-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0027-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00006.html

SuSE Linux 42.2
noarch
clamav-database-201801010008-54.124.1

146215 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0042-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10081, CVE-2017-10086, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10105, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110,

CVE-2017-10111, CVE-2017-10114, CVE-2017-10115, CVE-2017-10116, CVE-2017-10118, CVE-2017-10125, CVE-2017-10135, CVE-2017-10176, CVE-2017-10193, CVE-2017-10198, CVE-2017-10243, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0042-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00013.html

SuSE Linux 42.2
i586
java-1_7_0-openjdk-bootstrap-1.7.0.161-42.6.1
java-1_7_0-openjdk-debugsource-1.7.0.161-42.6.1
java-1_7_0-openjdk-1.7.0.161-42.6.1
java-1_7_0-openjdk-demo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.161-42.6.1
java-1_7_0-openjdk-accessibility-1.7.0.161-42.6.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.161-42.6.1
java-1_7_0-openjdk-headless-1.7.0.161-42.6.1
java-1_7_0-openjdk-devel-1.7.0.161-42.6.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-src-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.161-42.6.1

noarch
java-1_7_0-openjdk-javadoc-1.7.0.161-42.6.1

x86_64
java-1_7_0-openjdk-bootstrap-1.7.0.161-42.6.1
java-1_7_0-openjdk-debugsource-1.7.0.161-42.6.1
java-1_7_0-openjdk-1.7.0.161-42.6.1
java-1_7_0-openjdk-demo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.161-42.6.1
java-1_7_0-openjdk-accessibility-1.7.0.161-42.6.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.161-42.6.1
java-1_7_0-openjdk-headless-1.7.0.161-42.6.1
java-1_7_0-openjdk-devel-1.7.0.161-42.6.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-src-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.161-42.6.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.161-42.6.1

SuSE Linux 42.3
i586
java-1_7_0-openjdk-accessibility-1.7.0.161-45.1
java-1_7_0-openjdk-demo-1.7.0.161-45.1
java-1_7_0-openjdk-debugsource-1.7.0.161-45.1
java-1_7_0-openjdk-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.161-45.1
java-1_7_0-openjdk-headless-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-src-1.7.0.161-45.1
java-1_7_0-openjdk-devel-1.7.0.161-45.1
java-1_7_0-openjdk-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.161-45.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.161-45.1

noarch
java-1_7_0-openjdk-javadoc-1.7.0.161-45.1

x86_64
java-1_7_0-openjdk-accessibility-1.7.0.161-45.1
java-1_7_0-openjdk-demo-1.7.0.161-45.1
java-1_7_0-openjdk-debugsource-1.7.0.161-45.1
java-1_7_0-openjdk-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.161-45.1
java-1_7_0-openjdk-headless-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-src-1.7.0.161-45.1
java-1_7_0-openjdk-devel-1.7.0.161-45.1
java-1_7_0-openjdk-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.161-45.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.161-45.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.161-45.1

146216 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0025-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0025-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00004.html

SuSE Linux 42.2
i586
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.15.1
libMagickCore-6_Q16-1-6.8.8.1-30.15.1
ImageMagick-extra-6.8.8.1-30.15.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.15.1
libMagick++-6_Q16-3-6.8.8.1-30.15.1
perl-PerlMagick-6.8.8.1-30.15.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.15.1
ImageMagick-debugsource-6.8.8.1-30.15.1
libMagickWand-6_Q16-1-6.8.8.1-30.15.1
ImageMagick-debuginfo-6.8.8.1-30.15.1
ImageMagick-extra-debuginfo-6.8.8.1-30.15.1
ImageMagick-devel-6.8.8.1-30.15.1
libMagick++-devel-6.8.8.1-30.15.1
perl-PerlMagick-debuginfo-6.8.8.1-30.15.1
ImageMagick-6.8.8.1-30.15.1

noarch
ImageMagick-doc-6.8.8.1-30.15.1

x86_64
libMagickWand-6_Q16-1-32bit-6.8.8.1-30.15.1
libMagick++-6_Q16-3-32bit-6.8.8.1-30.15.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.15.1
libMagickCore-6_Q16-1-6.8.8.1-30.15.1
ImageMagick-extra-6.8.8.1-30.15.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.15.1
libMagick++-6_Q16-3-6.8.8.1-30.15.1
perl-PerlMagick-6.8.8.1-30.15.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.15.1
libMagick++-devel-32bit-6.8.8.1-30.15.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-30.15.1
ImageMagick-debugsource-6.8.8.1-30.15.1
libMagickWand-6_Q16-1-6.8.8.1-30.15.1
ImageMagick-debuginfo-6.8.8.1-30.15.1
ImageMagick-extra-debuginfo-6.8.8.1-30.15.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-30.15.1
ImageMagick-devel-6.8.8.1-30.15.1
libMagick++-devel-6.8.8.1-30.15.1
perl-PerlMagick-debuginfo-6.8.8.1-30.15.1
ImageMagick-devel-32bit-6.8.8.1-30.15.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-30.15.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-30.15.1
ImageMagick-6.8.8.1-30.15.1

SuSE Linux 42.3
i586
libMagick++-6_Q16-3-6.8.8.1-43.1
perl-PerlMagick-6.8.8.1-43.1
ImageMagick-extra-6.8.8.1-43.1
libMagickWand-6_Q16-1-6.8.8.1-43.1
libMagick++-devel-6.8.8.1-43.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-43.1
ImageMagick-6.8.8.1-43.1
ImageMagick-debuginfo-6.8.8.1-43.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-43.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-43.1
ImageMagick-debugsource-6.8.8.1-43.1
ImageMagick-devel-6.8.8.1-43.1
ImageMagick-extra-debuginfo-6.8.8.1-43.1
perl-PerlMagick-debuginfo-6.8.8.1-43.1
libMagickCore-6_Q16-1-6.8.8.1-43.1

noarch
ImageMagick-doc-6.8.8.1-43.1

x86_64
libMagick++-6_Q16-3-6.8.8.1-43.1
perl-PerlMagick-6.8.8.1-43.1
libMagick++-devel-32bit-6.8.8.1-43.1
ImageMagick-extra-6.8.8.1-43.1
libMagickWand-6_Q16-1-6.8.8.1-43.1
libMagick++-devel-6.8.8.1-43.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-43.1
libMagick++-6_Q16-3-32bit-6.8.8.1-43.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-43.1
ImageMagick-devel-32bit-6.8.8.1-43.1
ImageMagick-6.8.8.1-43.1
ImageMagick-debuginfo-6.8.8.1-43.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-43.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-43.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-43.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-43.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-43.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-43.1
ImageMagick-debugsource-6.8.8.1-43.1
ImageMagick-devel-6.8.8.1-43.1
ImageMagick-extra-debuginfo-6.8.8.1-43.1
perl-PerlMagick-debuginfo-6.8.8.1-43.1
libMagickCore-6_Q16-1-6.8.8.1-43.1

146217 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0058-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0058-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00019.html

SuSE Linux 42.2
x86_64
irssi-debugsource-1.0.6-14.18.1
irssi-1.0.6-14.18.1
irssi-devel-1.0.6-14.18.1
irssi-debuginfo-1.0.6-14.18.1

i586
irssi-debugsource-1.0.6-14.18.1
irssi-1.0.6-14.18.1
irssi-devel-1.0.6-14.18.1
irssi-debuginfo-1.0.6-14.18.1

SuSE Linux 42.3
x86_64
irssi-1.0.6-21.1
irssi-debugsource-1.0.6-21.1
irssi-devel-1.0.6-21.1
irssi-debuginfo-1.0.6-21.1

i586
irssi-1.0.6-21.1
irssi-debugsource-1.0.6-21.1
irssi-devel-1.0.6-21.1
irssi-debuginfo-1.0.6-21.1

146218 - SuSE SLES 11 SP4 SUSE-SU-2018:0054-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13765, CVE-2017-13766, CVE-2017-13767, CVE-2017-15191, CVE-2017-15192, CVE-2017-15193, CVE-2017-17083, CVE-2017-17084, CVE-2017-17085, CVE-2017-9617, CVE-2017-9766

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0054-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003581.html

SuSE SLES 11 SP4
i586
wireshark-gtk-2.2.11-40.14.5
portaudio-19-234.18.1
wireshark-2.2.11-40.14.5
libwscodecs1-2.2.11-40.14.5
libwsutil7-2.2.11-40.14.5
libwireshark8-2.2.11-40.14.5
libsmi-0.4.5-2.7.2.1
libwiretap6-2.2.11-40.14.5

x86_64
wireshark-gtk-2.2.11-40.14.5
portaudio-19-234.18.1
wireshark-2.2.11-40.14.5
libwscodecs1-2.2.11-40.14.5
libwsutil7-2.2.11-40.14.5
libwireshark8-2.2.11-40.14.5
libsmi-0.4.5-2.7.2.1
libwiretap6-2.2.11-40.14.5

146219 - SuSE Linux 42.2 openSUSE-SU-2018:0023-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0023-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00003.html

SuSE Linux 42.2
x86_64
kernel-syms-4.4.104-18.44.1
kernel-debug-debugsource-4.4.104-18.44.1
kernel-vanilla-base-4.4.104-18.44.1
kernel-vanilla-4.4.104-18.44.1
kernel-obs-build-debugsource-4.4.104-18.44.1
kernel-obs-qa-4.4.104-18.44.1
kernel-default-4.4.104-18.44.1
kernel-debug-base-debuginfo-4.4.104-18.44.1
kernel-debug-base-4.4.104-18.44.1
kernel-obs-build-4.4.104-18.44.1
kernel-vanilla-base-debuginfo-4.4.104-18.44.1
kernel-default-base-4.4.104-18.44.1
kernel-default-base-debuginfo-4.4.104-18.44.1
kernel-vanilla-devel-4.4.104-18.44.1
kernel-default-debugsource-4.4.104-18.44.1
kernel-debug-devel-4.4.104-18.44.1
kernel-default-debuginfo-4.4.104-18.44.1
kernel-debug-debuginfo-4.4.104-18.44.1
kernel-vanilla-debuginfo-4.4.104-18.44.1
kernel-default-devel-4.4.104-18.44.1
kernel-vanilla-debugsource-4.4.104-18.44.1
kernel-debug-4.4.104-18.44.1
kernel-debug-devel-debuginfo-4.4.104-18.44.1

noarch
kernel-docs-4.4.104-18.44.1
kernel-source-vanilla-4.4.104-18.44.1
kernel-devel-4.4.104-18.44.1
kernel-docs-pdf-4.4.104-18.44.1
kernel-macros-4.4.104-18.44.1
kernel-docs-html-4.4.104-18.44.1
kernel-source-4.4.104-18.44.1

146221 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0047-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0047-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00015.html

SuSE Linux 42.2
i586
libvorbisenc2-debuginfo-1.3.3-5.3.1
libvorbis0-1.3.3-5.3.1
libvorbisfile3-debuginfo-1.3.3-5.3.1
libvorbis-debugsource-1.3.3-5.3.1
libvorbis0-debuginfo-1.3.3-5.3.1
libvorbis-devel-1.3.3-5.3.1
libvorbisfile3-1.3.3-5.3.1
libvorbisenc2-1.3.3-5.3.1

noarch
libvorbis-doc-1.3.3-5.3.1

x86_64
libvorbis-debugsource-1.3.3-5.3.1
libvorbis0-1.3.3-5.3.1
libvorbisfile3-32bit-1.3.3-5.3.1
libvorbisenc2-debuginfo-1.3.3-5.3.1
libvorbisfile3-debuginfo-32bit-1.3.3-5.3.1
libvorbis-devel-1.3.3-5.3.1
libvorbis0-32bit-1.3.3-5.3.1
libvorbisfile3-1.3.3-5.3.1
libvorbis0-debuginfo-32bit-1.3.3-5.3.1
libvorbisenc2-32bit-1.3.3-5.3.1
libvorbisenc2-debuginfo-32bit-1.3.3-5.3.1
libvorbis0-debuginfo-1.3.3-5.3.1
libvorbisfile3-debuginfo-1.3.3-5.3.1
libvorbisenc2-1.3.3-5.3.1

SuSE Linux 42.3
i586
libvorbisfile3-debuginfo-1.3.3-8.1
libvorbis-devel-1.3.3-8.1
libvorbisfile3-1.3.3-8.1
libvorbisenc2-1.3.3-8.1
libvorbisenc2-debuginfo-1.3.3-8.1
libvorbis-debugsource-1.3.3-8.1
libvorbis0-1.3.3-8.1
libvorbis0-debuginfo-1.3.3-8.1

noarch
libvorbis-doc-1.3.3-8.1

x86_64
libvorbis0-debuginfo-32bit-1.3.3-8.1
libvorbis-debugsource-1.3.3-8.1
libvorbisfile3-1.3.3-8.1
libvorbisfile3-debuginfo-32bit-1.3.3-8.1

libvorbisenc2-debuginfo-1.3.3-8.1
libvorbisenc2-32bit-1.3.3-8.1
libvorbis0-debuginfo-1.3.3-8.1
libvorbisfile3-32bit-1.3.3-8.1
libvorbisenc2-1.3.3-8.1
libvorbisenc2-debuginfo-32bit-1.3.3-8.1
libvorbis0-1.3.3-8.1
libvorbis-devel-1.3.3-8.1
libvorbis0-32bit-1.3.3-8.1
libvorbisfile3-debuginfo-1.3.3-8.1

146222 - SuSE SLES 11 SP4 SUSE-SU-2018:0043-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0043-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003578.html

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.78.17.1

x86_64
libMagickCore1-32bit-6.4.3.6-7.78.17.1
libMagickCore1-6.4.3.6-7.78.17.1

160346 - CentOS 6, 7 CESA-2018-0061 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7829, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

Description

The scan detected that the host is missing the following update:
CESA-2018-0061

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-January/022707.html
http://lists.centos.org/pipermail/centos-announce/2018-January/022706.html

CentOS 7
x86_64
thunderbird-52.5.2-1.el7.centos

CentOS 6
x86_64
thunderbird-52.5.2-1.el6.centos

i686
thunderbird-52.5.2-1.el6.centos

163523 - Oracle Enterprise Linux ELSA-2018-0061 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7829, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

Description

The scan detected that the host is missing the following update:
ELSA-2018-0061

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007447.html
http://oss.oracle.com/pipermail/el-errata/2018-January/007446.html

OEL7
x86_64
thunderbird-52.5.2-1.0.1.el7_4

OEL6
x86_64
thunderbird-52.5.2-1.0.1.el6_9

i386
thunderbird-52.5.2-1.0.1.el6_9

175311 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86_64 (1801-3134)

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

Risk Level: High

CVE: CVE-2017-7829, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86_64 (1801-3134)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1801&L=scientific-linux-errata&F=&S=&P=3134

SL7
x86_64
thunderbird-debuginfo-52.5.2-1.el7_4

thunderbird-52.5.2-1.el7_4

SL6
x86_64
thunderbird-52.5.2-1.el6_9
thunderbird-debuginfo-52.5.2-1.el6_9

i386
thunderbird-52.5.2-1.el6_9
thunderbird-debuginfo-52.5.2-1.el6_9

186033 - Ubuntu Linux 17.10 USN-3523-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16995, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3523-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004213.html

Ubuntu 17.10

linux-image-lowlatency_4.13.0.25.26
linux-image-4.13.0-25-generic_4.13.0-25.29
linux-image-4.13.0-25-lowlatency_4.13.0-25.29
linux-image-generic_4.13.0.25.26

193149 - Fedora Linux 26 FEDORA-2017-4603342f9a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16927

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4603342f9a

Observation

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

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

Fedora Core 26

xrdp-0.9.5-1.fc26

193152 - Fedora Linux 27 FEDORA-2017-1c73749b66 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16927

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1c73749b66

Observation

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

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

Fedora Core 27

xrdp-0.9.5-1.fc27

130989 - Debian Linux 8.0, 9.0 DSA-4079-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14517, CVE-2017-14518, CVE-2017-14519, CVE-2017-14520, CVE-2017-14975, CVE-2017-14976, CVE-2017-14977, CVE-2017-15565, CVE-2017-9406, CVE-2017-9408, CVE-2017-9775, CVE-2017-9776, CVE-2017-9865

Description

The scan detected that the host is missing the following update:
DSA-4079-1

Observation

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

http://www.debian.org/security/2018/dsa-4079

Debian 8.0
all
libpoppler-glib8_0.26.5-2+deb8u2
libpoppler-glib-doc_0.26.5-2+deb8u2
libpoppler-qt4-4_0.26.5-2+deb8u2
libpoppler-dev_0.26.5-2+deb8u2
poppler-utils_0.26.5-2+deb8u2
libpoppler-cpp-dev_0.26.5-2+deb8u2
libpoppler-glib-dev_0.26.5-2+deb8u2
libpoppler-qt4-dev_0.26.5-2+deb8u2
libpoppler-cpp0_0.26.5-2+deb8u2
poppler-dbg_0.26.5-2+deb8u2
libpoppler-private-dev_0.26.5-2+deb8u2
libpoppler-qt5-1_0.26.5-2+deb8u2
libpoppler-qt5-dev_0.26.5-2+deb8u2
gir1.2-poppler-0.18_0.26.5-2+deb8u2
libpoppler46_0.26.5-2+deb8u2

Debian 9.0
all
poppler-utils_0.48.0-2+deb9u1

libpoppler64_0.48.0-2+deb9u1
poppler-dbg_0.48.0-2+deb9u1
gir1.2-poppler-0.18_0.48.0-2+deb9u1
libpoppler-qt4-dev_0.48.0-2+deb9u1
libpoppler-glib8_0.48.0-2+deb9u1
libpoppler-glib-doc_0.48.0-2+deb9u1
libpoppler-qt4-4_0.48.0-2+deb9u1
libpoppler-cpp-dev_0.48.0-2+deb9u1
libpoppler-qt5-dev_0.48.0-2+deb9u1
libpoppler-glib-dev_0.48.0-2+deb9u1
libpoppler-cpp0v5_0.48.0-2+deb9u1
libpoppler-private-dev_0.48.0-2+deb9u1
libpoppler-dev_0.48.0-2+deb9u1
libpoppler-qt5-1_0.48.0-2+deb9u1

146223 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0029-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14919, CVE-2017-15896, CVE-2017-3735, CVE-2017-3736, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0029-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00007.html

SuSE Linux 42.2
i586
npm4-4.8.7-5.9.1
nodejs4-debuginfo-4.8.7-5.9.1
nodejs4-4.8.7-5.9.1
nodejs4-debugsource-4.8.7-5.9.1
nodejs4-devel-4.8.7-5.9.1

noarch
nodejs4-docs-4.8.7-5.9.1

x86_64
npm4-4.8.7-5.9.1
nodejs4-debuginfo-4.8.7-5.9.1
nodejs4-4.8.7-5.9.1
nodejs4-debugsource-4.8.7-5.9.1
nodejs4-devel-4.8.7-5.9.1

SuSE Linux 42.3
i586
nodejs4-debugsource-4.8.7-11.1
nodejs4-debuginfo-4.8.7-11.1
nodejs4-devel-4.8.7-11.1
nodejs4-4.8.7-11.1
npm4-4.8.7-11.1

noarch

nodejs4-docs-4.8.7-11.1

x86_64
nodejs4-debugsource-4.8.7-11.1
nodejs4-debuginfo-4.8.7-11.1
nodejs4-devel-4.8.7-11.1
nodejs4-4.8.7-11.1
npm4-4.8.7-11.1

186034 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3519-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5647, CVE-2017-5648, CVE-2017-5664, CVE-2017-7674

Description

The scan detected that the host is missing the following update:
USN-3519-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004207.html

Ubuntu 16.04

libtomcat8-java_8.0.32-1ubuntu1.5
tomcat8_8.0.32-1ubuntu1.5

Ubuntu 14.04

libtomcat7-java_7.0.52-1ubuntu0.13
tomcat7_7.0.52-1ubuntu0.13

Ubuntu 17.04

tomcat8_8.0.38-2ubuntu2.2
libtomcat8-java_8.0.38-2ubuntu2.2

193155 - Fedora Linux 27 FEDORA-2018-67b75f73fa Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2018-67b75f73fa

Observation

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

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

Fedora Core 27

gimp-2.8.22-3.fc27

193162 - Fedora Linux 26 FEDORA-2017-0ad0e2f390 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0ad0e2f390

Observation

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

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

Fedora Core 26

webkitgtk4-2.18.4-1.fc26

22959 - NVIDIA Windows Drivers Speculative Side Channels Vulnerabilities

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

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers.

Observation

NVIDIA is a technology company which manufactures graphics processing units.

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers. The flaws occur within the kernel mode layer. Successful exploitation could allow an attacker to disclose private information.

178565 - Gentoo Linux GLSA-201801-01 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-201801-01

Observation

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

https://security.gentoo.org/glsa/201801-01

Affected packages:
sys-devel/binutils < 2.29.1-r1

178566 - Gentoo Linux GLSA-201801-04 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-201801-04

Observation

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

https://security.gentoo.org/glsa/201801-04

Affected packages:
x11-libs/libXcursor < 1.1.15

178567 - Gentoo Linux GLSA-201801-09 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-201801-09

Observation

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

https://security.gentoo.org/glsa/201801-09

Affected packages:
net-libs/webkit-gtk < 2.18.4

178568 - Gentoo Linux GLSA-201801-02 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-201801-02

Observation

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

https://security.gentoo.org/glsa/201801-02

Affected packages:
media-gfx/optipng < 0.7.6-r2

178569 - Gentoo Linux GLSA-201801-10 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-201801-10

Observation

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

https://security.gentoo.org/glsa/201801-10

Affected packages:
x11-libs/libXfont < 1.5.4
x11-libs/libXfont2 < 2.0.3

178570 - Gentoo Linux GLSA-201801-05 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-201801-05

Observation

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

https://security.gentoo.org/glsa/201801-05

Affected packages:
net-misc/openssh < 7.5_p1-r3

178571 - Gentoo Linux GLSA-201801-03 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-201801-03

Observation

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

https://security.gentoo.org/glsa/201801-03

Affected packages:
www-client/chromium < 63.0.3239.108
www-client/google-chrome < 63.0.3239.108

178572 - Gentoo Linux GLSA-201801-06 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-201801-06

Observation

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

https://security.gentoo.org/glsa/201801-06

Affected packages:
app-backup/backintime < 1.1.24

178573 - Gentoo Linux GLSA-201801-08 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-201801-08

Observation

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

https://security.gentoo.org/glsa/201801-08

Affected packages:
net-libs/miniupnpc < 2.0.20170509

193144 - Fedora Linux 27 FEDORA-2017-f0e5ad250c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17439

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f0e5ad250c

Observation

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

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

Fedora Core 27

heimdal-7.5.0-1.fc27

193150 - Fedora Linux 27 FEDORA-2017-3997279e65 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17083, CVE-2017-17084, CVE-2017-17085

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3997279e65

Observation

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

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

Fedora Core 27

wireshark-2.4.3-1.fc27

193158 - Fedora Linux 26 FEDORA-2017-2962e58478 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17439

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2962e58478

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=2

Fedora Core 26

heimdal-7.5.0-1.fc26

130990 - Debian Linux 9.0 DSA-4078-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
DSA-4078-1

Observation

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

http://www.debian.org/security/2018/dsa-4078

Debian 9.0
all
fuse-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2
linux-source-4.9_4.9.65-3+deb9u2
crypto-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
ata-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
hyperv-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
ext4-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
acpi-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
crypto-dm-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u2
crypto-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
crc-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
multipath-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
ata-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
firewire-core-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
usb-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
i2c-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u2
i2c-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
jfs-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
pata-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
event-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
multipath-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
virtio-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
loop-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
md-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
squashfs-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2
input-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
input-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
mmc-core-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
ext4-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
isofs-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
mouse-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
nbd-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u2
linux-headers-4.9.0-4-all-armel_4.9.65-3+deb9u2
scsi-core-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
scsi-core-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
md-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
fuse-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2

squashfs-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
mmc-core-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
fat-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u2
kernel-image-4.9.0-4-armmp-di_4.9.65-3+deb9u2
kernel-image-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
zlib-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
fuse-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
uinput-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
ata-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
loop-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
affs-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
nic-wireless-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
nic-shared-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
kernel-image-4.9.0-4-marvell-di_4.9.65-3+deb9u2
scsi-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
usb-storage-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
isofs-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
xfs-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
usb-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
sound-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
input-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2
nbd-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2
md-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
nic-wireless-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
sata-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
mtd-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u2
virtio-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
fat-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
usb-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
udf-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
dasd-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u2
btrfs-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
multipath-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u2
linux-image-4.9.0-4-4kc-malta-dbg_4.9.65-3+deb9u2
loop-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
serial-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
sata-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
ntfs-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
linux-headers-4.9.0-4-all_4.9.65-3+deb9u2
cdrom-core-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
usb-serial-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
linux-headers-4.9.0-4-all-armhf_4.9.65-3+deb9u2
minix-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
scsi-core-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
linux-headers-4.9.0-4-rt-amd64_4.9.65-3+deb9u2
linux-image-4.9.0-4-686-pae_4.9.65-3+deb9u2
loop-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2
ext4-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
pata-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u2
squashfs-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
nbd-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
crypto-dm-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
xfs-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
nbd-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
linux-image-4.9.0-4-octeon_4.9.65-3+deb9u2
virtio-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
cdrom-core-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2
crypto-dm-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2
nic-shared-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
crypto-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2

fuse-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
usb-storage-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
loop-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u2
fuse-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u2
ppp-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
linux-headers-4.9.0-4-arm64_4.9.65-3+deb9u2
nic-shared-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
squashfs-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
btrfs-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
mouse-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
crypto-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
input-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u2
cdrom-core-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
btrfs-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
nic-shared-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
cdrom-core-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
crypto-dm-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u2
efi-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
scsi-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
nic-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u2
jfs-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
crypto-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
leds-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
serial-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
linux-image-4.9.0-4-arm64_4.9.65-3+deb9u2
input-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
fb-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
nic-shared-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u2
linux-image-4.9.0-4-686_4.9.65-3+deb9u2
mmc-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
jfs-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u2
crypto-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
linux-headers-4.9.0-4-marvell_4.9.65-3+deb9u2
scsi-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u2
zlib-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
squashfs-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
input-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
crc-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u2
speakup-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
scsi-modules-4.9.0-4-686-di_4.9.65-3+deb9u2
event-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u2
btrfs-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u2
udf-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u2
ppp-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u2
linux-headers-4.9.0-4-all-mipsel_4.9.65-3+deb9u2

132423 - Oracle VM OVMSA-2018-0006 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-2018-0006

Observation

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

For more information see:

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000816.html

OVM3.4
x86_64
xen-4.4.4-155.0.12.el6
xen-tools-4.4.4-155.0.12.el6

132425 - Oracle VM OVMSA-2018-0004 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0004

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-January/000812.html

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

146213 - SuSE Linux 42.2 openSUSE-SU-2018:0026-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0026-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00005.html

SuSE Linux 42.2
noarch
kernel-firmware-20170530-7.12.1
ucode-amd-20170530-7.12.1

146214 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2018:0036-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0036-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003574.html

SuSE SLED 12 SP2
x86_64
qemu-block-curl-2.6.2-41.31.1
qemu-debugsource-2.6.2-41.31.1
qemu-tools-2.6.2-41.31.1
qemu-x86-2.6.2-41.31.1
qemu-tools-debuginfo-2.6.2-41.31.1
qemu-block-curl-debuginfo-2.6.2-41.31.1
qemu-2.6.2-41.31.1
qemu-kvm-2.6.2-41.31.1

noarch
qemu-sgabios-8-41.31.1
qemu-ipxe-1.0.0-41.31.1
qemu-vgabios-1.9.1-41.31.1
qemu-seabios-1.9.1-41.31.1

SuSE SLES 12 SP2
noarch
qemu-sgabios-8-41.31.1
qemu-ipxe-1.0.0-41.31.1
qemu-vgabios-1.9.1-41.31.1
qemu-seabios-1.9.1-41.31.1

x86_64
qemu-lang-2.6.2-41.31.1
qemu-x86-2.6.2-41.31.1
qemu-2.6.2-41.31.1
qemu-block-curl-2.6.2-41.31.1
qemu-tools-2.6.2-41.31.1
qemu-guest-agent-2.6.2-41.31.1
qemu-block-curl-debuginfo-2.6.2-41.31.1
qemu-block-ssh-debuginfo-2.6.2-41.31.1
qemu-kvm-2.6.2-41.31.1
qemu-block-rbd-2.6.2-41.31.1
qemu-block-rbd-debuginfo-2.6.2-41.31.1
qemu-tools-debuginfo-2.6.2-41.31.1
qemu-debugsource-2.6.2-41.31.1
qemu-block-ssh-2.6.2-41.31.1
qemu-guest-agent-debuginfo-2.6.2-41.31.1

146220 - SuSE Linux 42.3 openSUSE-SU-2018:0030-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:0030-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-01/msg00008.html

SuSE Linux 42.3
i586
qemu-linux-user-debugsource-2.9.1-38.1
qemu-linux-user-2.9.1-38.1
qemu-linux-user-debuginfo-2.9.1-38.1

noarch
qemu-sgabios-8-38.1
qemu-seabios-1.10.2-38.1
qemu-ipxe-1.0.0-38.1
qemu-vgabios-1.10.2-38.1

x86_64
qemu-extra-debuginfo-2.9.1-38.1
qemu-block-rbd-debuginfo-2.9.1-38.1
qemu-s390-debuginfo-2.9.1-38.1
qemu-tools-2.9.1-38.1
qemu-block-curl-debuginfo-2.9.1-38.1
qemu-block-ssh-2.9.1-38.1
qemu-s390-2.9.1-38.1
qemu-testsuite-2.9.1-38.2
qemu-x86-2.9.1-38.1
qemu-2.9.1-38.1
qemu-linux-user-debuginfo-2.9.1-38.1
qemu-arm-2.9.1-38.1
qemu-ksm-2.9.1-38.1
qemu-linux-user-debugsource-2.9.1-38.1
qemu-ppc-2.9.1-38.1
qemu-ppc-debuginfo-2.9.1-38.1
qemu-guest-agent-2.9.1-38.1
qemu-lang-2.9.1-38.1
qemu-x86-debuginfo-2.9.1-38.1
qemu-block-iscsi-debuginfo-2.9.1-38.1
qemu-extra-2.9.1-38.1
qemu-debugsource-2.9.1-38.1
qemu-guest-agent-debuginfo-2.9.1-38.1
qemu-kvm-2.9.1-38.1
qemu-block-ssh-debuginfo-2.9.1-38.1
qemu-block-iscsi-2.9.1-38.1
qemu-linux-user-2.9.1-38.1
qemu-block-rbd-2.9.1-38.1
qemu-tools-debuginfo-2.9.1-38.1
qemu-block-dmg-debuginfo-2.9.1-38.1
qemu-block-dmg-2.9.1-38.1
qemu-block-curl-2.9.1-38.1
qemu-arm-debuginfo-2.9.1-38.1

163520 - Oracle Enterprise Linux ELSA-2018-0024 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

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

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007439.html

OEL6
x86_64
qemu-guest-agent-0.12.1.2-2.503.el6_9.4
qemu-img-0.12.1.2-2.503.el6_9.4
qemu-kvm-0.12.1.2-2.503.el6_9.4
qemu-kvm-tools-0.12.1.2-2.503.el6_9.4

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

163521 - Oracle Enterprise Linux ELSA-2018-0030 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

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

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007440.html

OEL6
x86_64
libvirt-python-0.10.2-62.0.1.el6_9.1
libvirt-lock-sanlock-0.10.2-62.0.1.el6_9.1
libvirt-client-0.10.2-62.0.1.el6_9.1
libvirt-0.10.2-62.0.1.el6_9.1
libvirt-devel-0.10.2-62.0.1.el6_9.1

i386
libvirt-python-0.10.2-62.0.1.el6_9.1
libvirt-client-0.10.2-62.0.1.el6_9.1
libvirt-0.10.2-62.0.1.el6_9.1
libvirt-devel-0.10.2-62.0.1.el6_9.1

163522 - Oracle Enterprise Linux ELSA-2018-0029 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

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

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007441.html

OEL7
x86_64
libvirt-daemon-driver-storage-scsi-3.2.0-14.0.1.el7_4.7
libvirt-3.2.0-14.0.1.el7_4.7
libvirt-login-shell-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-storage-mpath-3.2.0-14.0.1.el7_4.7
libvirt-admin-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-secret-3.2.0-14.0.1.el7_4.7
libvirt-daemon-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-storage-gluster-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-storage-logical-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-storage-rbd-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-nodedev-3.2.0-14.0.1.el7_4.7
libvirt-libs-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-storage-disk-3.2.0-14.0.1.el7_4.7
libvirt-devel-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-storage-core-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-nwfilter-3.2.0-14.0.1.el7_4.7
libvirt-daemon-config-network-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-storage-iscsi-3.2.0-14.0.1.el7_4.7
libvirt-client-3.2.0-14.0.1.el7_4.7
libvirt-lock-sanlock-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-storage-3.2.0-14.0.1.el7_4.7
libvirt-daemon-config-nwfilter-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-qemu-3.2.0-14.0.1.el7_4.7
libvirt-daemon-kvm-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-network-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-lxc-3.2.0-14.0.1.el7_4.7
libvirt-nss-3.2.0-14.0.1.el7_4.7
libvirt-daemon-lxc-3.2.0-14.0.1.el7_4.7
libvirt-daemon-driver-interface-3.2.0-14.0.1.el7_4.7
libvirt-docs-3.2.0-14.0.1.el7_4.7

163524 - Oracle Enterprise Linux ELSA-2018-0023 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

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

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-January/007438.html

OEL7
x86_64
qemu-kvm-common-1.5.3-141.el7_4.6
qemu-img-1.5.3-141.el7_4.6
qemu-kvm-1.5.3-141.el7_4.6
qemu-kvm-tools-1.5.3-141.el7_4.6

186029 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3516-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
USN-3516-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004204.html

Ubuntu 16.04

firefox_57.0.4+build1-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_57.0.4+build1-0ubuntu0.14.04.1

Ubuntu 17.04

firefox_57.0.4+build1-0ubuntu0.17.04.1

Ubuntu 17.10

firefox_57.0.4+build1-0ubuntu0.17.10.1

186032 - Ubuntu Linux 16.04 USN-3522-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3522-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004211.html

Ubuntu 16.04

linux-image-generic_4.4.0.108.113
linux-image-4.4.0-108-generic_4.4.0-108.131
linux-image-euclid_4.4.0.9021.21
linux-image-4.4.0-108-lowlatency_4.4.0-108.131
linux-image-kvm_4.4.0.1015.15
linux-image-aws_4.4.0.1047.49
linux-image-4.4.0-1047-aws_4.4.0-1047.56
linux-image-4.4.0-9021-euclid_4.4.0-9021.22
linux-image-lowlatency_4.4.0.108.113
linux-image-4.4.0-1015-kvm_4.4.0-1015.20

186035 - Ubuntu Linux 14.04 USN-3524-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3524-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004215.html

Ubuntu 14.04

linux-image-3.13.0-139-lowlatency_3.13.0-139.188
linux-image-generic_3.13.0.139.148
linux-image-3.13.0-139-generic_3.13.0-139.188
linux-image-lowlatency_3.13.0.139.148

186037 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3521-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5753

Description

The scan detected that the host is missing the following update:
USN-3521-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004210.html

Ubuntu 16.04

nvidia-384_384.111-0ubuntu0.16.04.1

Ubuntu 14.04

nvidia-384_384.111-0ubuntu0.14.04.1

Ubuntu 17.04

nvidia-384_384.111-0ubuntu0.17.04.1

Ubuntu 17.10

nvidia-384_384.111-0ubuntu0.17.10.1

186038 - Ubuntu Linux 14.04 USN-3522-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5754

Description

The scan detected that the host is missing the following update:
USN-3522-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004212.html

Ubuntu 14.04

linux-image-4.4.0-108-generic_4.4.0-108.131~14.04.1
linux-image-generic-lts-xenial_4.4.0.108.91
linux-image-lowlatency-lts-xenial_4.4.0.108.91
linux-image-aws_4.4.0.1009.9
linux-image-4.4.0-108-lowlatency_4.4.0-108.131~14.04.1
linux-image-4.4.0-1009-aws_4.4.0-1009.9

88907 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-008-01 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
SSA:2018-008-01

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.432557

Slackware 14.0
x86_64
irssi-1.0.6-x86_64-1

Slackware 14.2
x86_64
irssi-1.0.6-x86_64-1

i586
irssi-1.0.6-i586-1

Slackware 14.1
x86_64
irssi-1.0.6-x86_64-1

182567 - FreeBSD irssi Multiple Vulnerabilities (a3764767-f31e-11e7-95f2-005056925db4)

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
irssi -- multiple vulnerabilities (a3764767-f31e-11e7-95f2-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/a3764767-f31e-11e7-95f2-005056925db4.html

Affected packages:
irssi < 1.0.6,1

182568 - FreeBSD awstats Remote Code Execution (4055aee5-f4c6-11e7-95f2-005056925db4)

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

Risk Level: Low

CVE: CVE-2017-1000501

Description

The scan detected that the host is missing the following update:
awstats -- remote code execution (4055aee5-f4c6-11e7-95f2-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/4055aee5-f4c6-11e7-95f2-005056925db4.html

Affected packages:
awstats < 7.7,1

182569 - FreeBSD mozilla Speculative Execution Side-channel Attack (8429711b-76ca-474e-94a0-6b980f1e2d47)

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:
mozilla -- Speculative execution side-channel attack (8429711b-76ca-474e-94a0-6b980f1e2d47)

Observation

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

http://www.vuxml.org/freebsd/8429711b-76ca-474e-94a0-6b980f1e2d47.html

Affected packages:
firefox < 57.0.4,1
waterfox < 56.0.2

182570 - FreeBSD Flash Player Information Disclosure (9c016563-f582-11e7-b33c-6451062f0f7a)

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

Risk Level: Low

CVE: CVE-2018-4871

Description

The scan detected that the host is missing the following update:
Flash Player -- information disclosure (9c016563-f582-11e7-b33c-6451062f0f7a)

Observation

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

http://www.vuxml.org/freebsd/9c016563-f582-11e7-b33c-6451062f0f7a.html

Affected packages:
linux-flashplayer < 28.0.0.137

186031 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3518-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000501

Description

The scan detected that the host is missing the following update:
USN-3518-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004208.html

Ubuntu 16.04

awstats_7.4+dfsg-1ubuntu0.2

Ubuntu 14.04

awstats_7.2+dfsg-1ubuntu0.1

Ubuntu 17.04

awstats_7.6+dfsg-1ubuntu0.17.04.1

Ubuntu 17.10

awstats_7.6+dfsg-1ubuntu0.17.10.1

193142 - Fedora Linux 27 FEDORA-2018-53f304b0d3 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-2018-53f304b0d3

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=2

Fedora Core 27

dracut-046-8.git20180105.fc27

193143 - Fedora Linux 27 FEDORA-2018-276558ff6f 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-2018-276558ff6f

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=2

Fedora Core 27

firefox-57.0.4-1.fc27

193145 - Fedora Linux 27 FEDORA-2017-41242dfe10 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17850

Description

The scan detected that the host is missing the following update:
FEDORA-2017-41242dfe10

Observation

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

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

Fedora Core 27

asterisk-14.7.5-1.fc27

193146 - Fedora Linux 26 FEDORA-2018-c4670f2981 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-c4670f2981

Observation

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

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

Fedora Core 26

linux-firmware-20171215-82.git2451bb22.fc26

193147 - Fedora Linux 27 FEDORA-2018-f0ee5b818d 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-f0ee5b818d

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=2

Fedora Core 27

electron-cash-3.1.1-1.fc27

193148 - Fedora Linux 27 FEDORA-2018-4978426286 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-2018-4978426286

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=2

Fedora Core 27

electrum-3.0.5-1.fc27

193151 - Fedora Linux 27 FEDORA-2018-4e65ec8cc4 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-2018-4e65ec8cc4

Observation

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

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

Fedora Core 27

thunderbird-52.5.2-1.fc27

193153 - Fedora Linux 26 FEDORA-2018-3ec87df5ba 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-2018-3ec87df5ba

Observation

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

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

Fedora Core 26

thunderbird-52.5.2-1.fc26

193154 - Fedora Linux 26 FEDORA-2018-20ba39cba9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000456

Description

The scan detected that the host is missing the following update:
FEDORA-2018-20ba39cba9

Observation

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

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

Fedora Core 26

poppler-0.52.0-11.fc26

193156 - Fedora Linux 27 FEDORA-2017-4c30d86843 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17866

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4c30d86843

Observation

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

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

Fedora Core 27

mupdf-1.12.0-1.fc27

193157 - Fedora Linux 26 FEDORA-2017-c28bfe0986 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6328

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c28bfe0986

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=2

Fedora Core 26

libexif-0.6.21-14.fc26

193159 - Fedora Linux 27 FEDORA-2018-048468d7a8 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000456

Description

The scan detected that the host is missing the following update:
FEDORA-2018-048468d7a8

Observation

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

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

Fedora Core 27

poppler-0.57.0-7.fc27

193160 - Fedora Linux 27 FEDORA-2018-41af2a8d65 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-2018-41af2a8d65

Observation

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

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

Fedora Core 27

linux-firmware-20171215-82.git2451bb22.fc27

193161 - Fedora Linux 26 FEDORA-2018-9bcc7b0b70 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-2018-9bcc7b0b70

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2018/1/?count=200&page=2

Fedora Core 26

dracut-046-8.git20180105.fc26

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.

182390 - FreeBSD oniguruma Multiple Vulnerabilities (b396cf6c-62e6-11e7-9def-b499baebfeaf)

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

Risk Level: High

CVE: CVE-2017-9224, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228

Update Details

FASLScript is updated

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

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

Risk Level: Medium

CVE: CVE-2017-5754

Update Details

FASLScript is updated

33353 - Oracle Solaris 145639-11 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33354 - Oracle Solaris 145638-11 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33375 - Oracle Solaris 145333-39 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33376 - Oracle Solaris 145334-39 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

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.