2017-DEC-26
FSL version 7.5.989

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

22881 - (CTX230238) Citrix NetScaler TLS Padding Oracle Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-17382

Description

A vulnerability is present in some versions of Citrix NetScaler.

Observation

Citrix NetScaler is a widely used product that helps enterprises to protect, control and improve their services.

A vulnerability is present in some versions of Citrix NetScaler. The flaw takes advantage of RSA encryption in order to retrieve data. Successful exploitation could allow an attacker to obtain sensitive information from the target system.

22882 - (CTX230612) Citrix NetScaler Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-17549

Description

A vulnerability is present in some versions of Citrix NetScaler.

Observation

Citrix NetScaler is a widely used product that helps enterprises to protect, control and improve their services.

A vulnerability is present in some versions of Citrix NetScaler. The flaw is related with TLS issues. Successful exploitation could allow an attacker to obtain sensitive information from the target system.

130980 - Debian Linux 9.0 DSA-4073-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000407, CVE-2017-1000410, CVE-2017-16538, CVE-2017-16644, CVE-2017-16995, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-17712, CVE-2017-17741, CVE-2017-17805, CVE-2017-17806, CVE-2017-17807, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
DSA-4073-1

Observation

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

http://www.debian.org/security/2017/dsa-4073

Debian 9.0
all
multipath-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
mouse-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
fuse-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
hyperv-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
ext4-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
scsi-core-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
i2c-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
minix-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u1
isofs-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u1
crc-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
input-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
loop-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
md-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
mtd-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
crypto-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
jfs-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
fuse-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u1
serial-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
pata-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
nbd-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u1
multipath-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
usb-storage-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u1
loop-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
ext4-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
i2c-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u1
scsi-core-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u1
udf-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
virtio-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u1
pcmcia-storage-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
md-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
btrfs-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u1
linux-headers-4.9.0-4-all-armel_4.9.65-3+deb9u1
linux-cpupower_4.9.65-3+deb9u1
md-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
mmc-core-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
linux-image-4.9.0-4-loongson-3_4.9.65-3+deb9u1
sata-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
mmc-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u1
fuse-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
uinput-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
efi-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
linux-headers-4.9.0-4-armmp-lpae_4.9.65-3+deb9u1
firewire-core-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
nic-wireless-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
pata-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u1
scsi-core-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
kernel-image-4.9.0-4-marvell-di_4.9.65-3+deb9u1
nic-usb-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
zlib-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u1
isofs-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
udf-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u1
udf-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1

md-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
crypto-dm-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
linux-headers-4.9.0-4-all-amd64_4.9.65-3+deb9u1
squashfs-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
jfs-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
nic-wireless-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
hyperv-daemons_4.9.65-3+deb9u1
dasd-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u1
input-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
linux-image-4.9.0-4-4kc-malta-dbg_4.9.65-3+deb9u1
pcmcia-storage-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
squashfs-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
loop-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
udf-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u1
sata-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
mmc-core-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
nic-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
ntfs-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
xfs-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u1
crc-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u1
linux-headers-4.9.0-4-all_4.9.65-3+deb9u1
cdrom-core-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
fuse-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u1
crypto-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u1
fat-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u1
virtio-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
loop-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
linux-source-4.9_4.9.65-3+deb9u1
pata-modules-4.9.0-4-armmp-di_4.9.65-3+deb9u1
udf-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
usb-serial-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
nic-shared-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
cdrom-core-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
event-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
mmc-core-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
nic-shared-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
crypto-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
usb-serial-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
usb-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
nic-wireless-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
cdrom-core-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
ext4-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
virtio-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u1
xfs-modules-4.9.0-4-686-pae-di_4.9.65-3+deb9u1
isofs-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
linux-headers-4.9.0-4-arm64_4.9.65-3+deb9u1
acpi-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
kernel-image-4.9.0-4-s390x-di_4.9.65-3+deb9u1
crypto-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
pcmcia-storage-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
crc-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
cdrom-core-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
ppp-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
input-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
ata-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
mmc-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
linux-headers-4.9.0-4-5kc-malta_4.9.65-3+deb9u1
linux-image-4.9.0-4-rt-amd64-dbg_4.9.65-3+deb9u1
jfs-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u1
crypto-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u1

linux-image-4.9.0-4-arm64_4.9.65-3+deb9u1
nic-usb-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u1
linux-image-4.9.0-4-686_4.9.65-3+deb9u1
ppp-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
fb-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
usb-serial-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
btrfs-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
jffs2-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
crypto-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
usb-storage-modules-4.9.0-4-arm64-di_4.9.65-3+deb9u1
btrfs-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
isofs-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
usb-serial-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
fb-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
usb-storage-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
event-modules-4.9.0-4-octeon-di_4.9.65-3+deb9u1
i2c-modules-4.9.0-4-4kc-malta-di_4.9.65-3+deb9u1
ppp-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
scsi-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
crypto-dm-modules-4.9.0-4-686-di_4.9.65-3+deb9u1
linux-headers-4.9.0-4-octeon_4.9.65-3+deb9u1
usb-storage-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
zlib-modules-4.9.0-4-loongson-3-di_4.9.65-3+deb9u1
jfs-modules-4.9.0-4-marvell-di_4.9.65-3+deb9u1
md-modules-4.9.0-4-s390x-di_4.9.65-3+deb9u1
crypto-dm-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1
isofs-modules-4.9.0-4-powerpc64le-di_4.9.65-3+deb9u1
crc-modules-4.9.0-4-5kc-malta-di_4.9.65-3+deb9u1
crc-modules-4.9.0-4-amd64-di_4.9.65-3+deb9u1

146174 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:3410-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000410, CVE-2017-11600, CVE-2017-12193, CVE-2017-15115, CVE-2017-15265, CVE-2017-16528, CVE-2017-16536, CVE-2017-16537, CVE-2017-16645, CVE-2017-16646, CVE-2017-16994, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-7482, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3410-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003550.html

SuSE SLED 12 SP2
x86_64
kernel-default-4.4.103-92.53.1
kernel-default-devel-4.4.103-92.53.1
kernel-syms-4.4.103-92.53.1
kernel-default-extra-debuginfo-4.4.103-92.53.1
kernel-default-debuginfo-4.4.103-92.53.1
kernel-default-extra-4.4.103-92.53.1
kernel-default-debugsource-4.4.103-92.53.1

noarch
kernel-source-4.4.103-92.53.1
kernel-macros-4.4.103-92.53.1
kernel-devel-4.4.103-92.53.1

SuSE SLES 12 SP2
noarch
kernel-source-4.4.103-92.53.1
kernel-macros-4.4.103-92.53.1
kernel-devel-4.4.103-92.53.1

x86_64
kernel-default-4.4.103-92.53.1
kernel-default-debuginfo-4.4.103-92.53.1
kernel-default-base-debuginfo-4.4.103-92.53.1
kernel-default-devel-4.4.103-92.53.1
kernel-syms-4.4.103-92.53.1
kernel-default-base-4.4.103-92.53.1
kernel-default-debugsource-4.4.103-92.53.1

146175 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3411-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2016-9841, CVE-2017-10281, CVE-2017-10285, CVE-2017-10293, CVE-2017-10295, CVE-2017-10309, 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:
SUSE-SU-2017:3411-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003551.html

SuSE SLES 12 SP3
x86_64
java-1_8_0-ibm-1.8.0_sr5.5-30.13.1
java-1_8_0-ibm-alsa-1.8.0_sr5.5-30.13.1
java-1_8_0-ibm-plugin-1.8.0_sr5.5-30.13.1

SuSE SLES 12 SP2
x86_64
java-1_8_0-ibm-1.8.0_sr5.5-30.13.1
java-1_8_0-ibm-alsa-1.8.0_sr5.5-30.13.1
java-1_8_0-ibm-plugin-1.8.0_sr5.5-30.13.1

146176 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:3398-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000410, CVE-2017-11600, CVE-2017-12193, CVE-2017-15115, CVE-2017-16528, CVE-2017-16536, CVE-2017-16537, CVE-2017-16645, CVE-2017-16646, CVE-2017-16994, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-7482, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3398-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003549.html

SuSE SLED 12 SP3
x86_64
kernel-default-extra-debuginfo-4.4.103-6.33.1
kernel-default-debuginfo-4.4.103-6.33.1
kernel-default-devel-4.4.103-6.33.1
kernel-default-4.4.103-6.33.1
kernel-syms-4.4.103-6.33.1
kernel-default-extra-4.4.103-6.33.1
kernel-default-debugsource-4.4.103-6.33.1

noarch
kernel-devel-4.4.103-6.33.1
kernel-source-4.4.103-6.33.1
kernel-macros-4.4.103-6.33.1

SuSE SLES 12 SP3
noarch
kernel-devel-4.4.103-6.33.1
kernel-source-4.4.103-6.33.1
kernel-macros-4.4.103-6.33.1

x86_64
kernel-default-debuginfo-4.4.103-6.33.1
kernel-default-base-4.4.103-6.33.1
kernel-default-base-debuginfo-4.4.103-6.33.1
kernel-default-devel-4.4.103-6.33.1
kernel-default-4.4.103-6.33.1
kernel-syms-4.4.103-6.33.1
kernel-default-debugsource-4.4.103-6.33.1

146177 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3388-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11188, CVE-2017-11478, CVE-2017-11523, CVE-2017-11527, CVE-2017-11535, CVE-2017-11640, CVE-2017-11752, CVE-2017-12140, CVE-2017-12435, CVE-2017-12587, CVE-2017-12644, CVE-2017-12662, CVE-2017-12669, CVE-2017-12983, CVE-2017-13134, CVE-2017-13769, CVE-2017-14138, CVE-2017-14172, CVE-2017-14173, CVE-2017-14175, CVE-2017-14341, CVE-2017-14342, CVE-2017-14531, CVE-2017-14607, CVE-2017-14682, CVE-2017-14733, CVE-2017-14989, CVE-2017-15217, CVE-2017-15930, CVE-2017-16545, CVE-2017-16546, CVE-2017-16669

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3388-1

Observation

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

For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003544.html

SuSE SLED 12 SP2
x86_64
ImageMagick-debugsource-6.8.8.1-71.17.1
libMagick++-6_Q16-3-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.17.1
libMagickWand-6_Q16-1-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.17.1
ImageMagick-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.17.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-6.8.8.1-71.17.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.17.1
ImageMagick-debuginfo-6.8.8.1-71.17.1

SuSE SLES 12 SP3
x86_64
ImageMagick-debugsource-6.8.8.1-71.17.1
libMagickWand-6_Q16-1-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.17.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-6.8.8.1-71.17.1
ImageMagick-debuginfo-6.8.8.1-71.17.1

SuSE SLES 12 SP2
x86_64
ImageMagick-debugsource-6.8.8.1-71.17.1
libMagickWand-6_Q16-1-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.17.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-6.8.8.1-71.17.1
ImageMagick-debuginfo-6.8.8.1-71.17.1

SuSE SLED 12 SP3
x86_64
ImageMagick-debugsource-6.8.8.1-71.17.1
libMagick++-6_Q16-3-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.17.1
libMagickWand-6_Q16-1-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.17.1
ImageMagick-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.17.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.17.1
libMagickCore-6_Q16-1-6.8.8.1-71.17.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.17.1
ImageMagick-debuginfo-6.8.8.1-71.17.1

146181 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3427-1 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-2017:3427-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00101.html

SuSE Linux 42.2
x86_64
enigmail-1.9.9-2.13.1

i586
enigmail-1.9.9-2.13.1

SuSE Linux 42.3
x86_64
enigmail-1.9.9-9.1

i586
enigmail-1.9.9-9.1

146182 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3421-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12880

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3421-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00096.html

SuSE Linux 42.2
noarch
python-PyJWT-1.4.2-2.3.1

SuSE Linux 42.3
noarch
python-PyJWT-1.4.2-5.1

146184 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3420-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11188, CVE-2017-11478, CVE-2017-11523, CVE-2017-11527, CVE-2017-11535, CVE-2017-11640, CVE-2017-11752, CVE-2017-12140, CVE-2017-12435, CVE-2017-12587, CVE-2017-12644, CVE-2017-12662, CVE-2017-12669, CVE-2017-12983, CVE-2017-13134, CVE-2017-13769, CVE-2017-14138, CVE-2017-14172, CVE-2017-14173, CVE-2017-14175, CVE-2017-14341, CVE-2017-14342, CVE-2017-14531, CVE-2017-14607, CVE-2017-14682, CVE-2017-14733, CVE-2017-14989, CVE-2017-15217, CVE-2017-15930, CVE-2017-16545, CVE-2017-16546, CVE-2017-16669

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3420-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00095.html

SuSE Linux 42.2
i586
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.12.1
ImageMagick-6.8.8.1-30.12.1
ImageMagick-devel-6.8.8.1-30.12.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.12.1
libMagick++-devel-6.8.8.1-30.12.1
ImageMagick-extra-6.8.8.1-30.12.1
libMagickCore-6_Q16-1-6.8.8.1-30.12.1
libMagick++-6_Q16-3-6.8.8.1-30.12.1
libMagickWand-6_Q16-1-6.8.8.1-30.12.1
perl-PerlMagick-debuginfo-6.8.8.1-30.12.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.12.1
perl-PerlMagick-6.8.8.1-30.12.1
ImageMagick-debuginfo-6.8.8.1-30.12.1
ImageMagick-extra-debuginfo-6.8.8.1-30.12.1
ImageMagick-debugsource-6.8.8.1-30.12.1

noarch
ImageMagick-doc-6.8.8.1-30.12.1

x86_64
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.12.1
ImageMagick-6.8.8.1-30.12.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-30.12.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-30.12.1
ImageMagick-devel-32bit-6.8.8.1-30.12.1
ImageMagick-devel-6.8.8.1-30.12.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.12.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-30.12.1
libMagick++-devel-6.8.8.1-30.12.1
ImageMagick-extra-6.8.8.1-30.12.1
libMagickCore-6_Q16-1-6.8.8.1-30.12.1
libMagick++-6_Q16-3-6.8.8.1-30.12.1
libMagick++-devel-32bit-6.8.8.1-30.12.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-30.12.1
libMagickWand-6_Q16-1-6.8.8.1-30.12.1
perl-PerlMagick-debuginfo-6.8.8.1-30.12.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.12.1
perl-PerlMagick-6.8.8.1-30.12.1
libMagick++-6_Q16-3-32bit-6.8.8.1-30.12.1
ImageMagick-debuginfo-6.8.8.1-30.12.1
ImageMagick-extra-debuginfo-6.8.8.1-30.12.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-30.12.1
ImageMagick-debugsource-6.8.8.1-30.12.1

SuSE Linux 42.3
i586
libMagick++-6_Q16-3-debuginfo-6.8.8.1-40.1
libMagickWand-6_Q16-1-6.8.8.1-40.1
ImageMagick-extra-debuginfo-6.8.8.1-40.1

perl-PerlMagick-6.8.8.1-40.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-40.1
ImageMagick-debuginfo-6.8.8.1-40.1
perl-PerlMagick-debuginfo-6.8.8.1-40.1
ImageMagick-devel-6.8.8.1-40.1
ImageMagick-extra-6.8.8.1-40.1
ImageMagick-debugsource-6.8.8.1-40.1
libMagickCore-6_Q16-1-6.8.8.1-40.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-40.1
libMagick++-6_Q16-3-6.8.8.1-40.1
libMagick++-devel-6.8.8.1-40.1
ImageMagick-6.8.8.1-40.1

noarch
ImageMagick-doc-6.8.8.1-40.1

x86_64
libMagick++-6_Q16-3-debuginfo-6.8.8.1-40.1
libMagickWand-6_Q16-1-6.8.8.1-40.1
ImageMagick-extra-debuginfo-6.8.8.1-40.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-40.1
perl-PerlMagick-6.8.8.1-40.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-40.1
ImageMagick-debuginfo-6.8.8.1-40.1
perl-PerlMagick-debuginfo-6.8.8.1-40.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-40.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-40.1
ImageMagick-devel-6.8.8.1-40.1
ImageMagick-extra-6.8.8.1-40.1
ImageMagick-debugsource-6.8.8.1-40.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-40.1
libMagick++-devel-32bit-6.8.8.1-40.1
libMagickCore-6_Q16-1-6.8.8.1-40.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-40.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-40.1
libMagick++-6_Q16-3-6.8.8.1-40.1
libMagick++-devel-6.8.8.1-40.1
libMagick++-6_Q16-3-32bit-6.8.8.1-40.1
ImageMagick-6.8.8.1-40.1
ImageMagick-devel-32bit-6.8.8.1-40.1

146185 - SuSE SLES 11 SP4 SUSE-SU-2017:3378-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11188, CVE-2017-11478, CVE-2017-11527, CVE-2017-11535, CVE-2017-11640, CVE-2017-11752, CVE-2017-12140, CVE-2017-12435, CVE-2017-12587, CVE-2017-12644, CVE-2017-12662, CVE-2017-12669, CVE-2017-12983, CVE-2017-13134, CVE-2017-13769, CVE-2017-14172, CVE-2017-14173, CVE-2017-14175, CVE-2017-14341, CVE-2017-14342, CVE-2017-14531, CVE-2017-14607, CVE-2017-14733, CVE-2017-15930, CVE-2017-16545, CVE-2017-16546

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3378-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003541.html

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.78.14.1

x86_64
libMagickCore1-32bit-6.4.3.6-7.78.14.1
libMagickCore1-6.4.3.6-7.78.14.1

146187 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3434-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
openSUSE-SU-2017:3434-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00107.html

SuSE Linux 42.2
x86_64
MozillaThunderbird-translations-common-52.5.2-41.24.1
MozillaThunderbird-translations-other-52.5.2-41.24.1
MozillaThunderbird-debuginfo-52.5.2-41.24.1
MozillaThunderbird-buildsymbols-52.5.2-41.24.1
MozillaThunderbird-devel-52.5.2-41.24.1
MozillaThunderbird-debugsource-52.5.2-41.24.1
MozillaThunderbird-52.5.2-41.24.1

i586
MozillaThunderbird-translations-common-52.5.2-41.24.1
MozillaThunderbird-translations-other-52.5.2-41.24.1
MozillaThunderbird-debuginfo-52.5.2-41.24.1
MozillaThunderbird-buildsymbols-52.5.2-41.24.1
MozillaThunderbird-devel-52.5.2-41.24.1
MozillaThunderbird-debugsource-52.5.2-41.24.1
MozillaThunderbird-52.5.2-41.24.1

SuSE Linux 42.3
x86_64
MozillaThunderbird-devel-52.5.2-53.1
MozillaThunderbird-translations-common-52.5.2-53.1
MozillaThunderbird-debugsource-52.5.2-53.1
MozillaThunderbird-52.5.2-53.1
MozillaThunderbird-debuginfo-52.5.2-53.1
MozillaThunderbird-buildsymbols-52.5.2-53.1
MozillaThunderbird-translations-other-52.5.2-53.1

i586
MozillaThunderbird-devel-52.5.2-53.1
MozillaThunderbird-translations-common-52.5.2-53.1

MozillaThunderbird-debugsource-52.5.2-53.1
MozillaThunderbird-52.5.2-53.1
MozillaThunderbird-debuginfo-52.5.2-53.1
MozillaThunderbird-buildsymbols-52.5.2-53.1
MozillaThunderbird-translations-other-52.5.2-53.1

170909 - Amazon Linux AMI ALAS-2017-933 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
ALAS-2017-933

Observation

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

https://alas.aws.amazon.com/ALAS-2017-933.html

Amazon Linux AMI
i686
samba-test-4.6.2-12.37.amzn1
samba-debuginfo-4.6.2-12.37.amzn1
samba-client-4.6.2-12.37.amzn1
ctdb-tests-4.6.2-12.37.amzn1
samba-python-4.6.2-12.37.amzn1
samba-4.6.2-12.37.amzn1
samba-common-tools-4.6.2-12.37.amzn1
libsmbclient-4.6.2-12.37.amzn1
samba-winbind-krb5-locator-4.6.2-12.37.amzn1
samba-devel-4.6.2-12.37.amzn1
samba-winbind-clients-4.6.2-12.37.amzn1
ctdb-4.6.2-12.37.amzn1
samba-common-libs-4.6.2-12.37.amzn1
libwbclient-devel-4.6.2-12.37.amzn1
samba-libs-4.6.2-12.37.amzn1
samba-winbind-4.6.2-12.37.amzn1
libwbclient-4.6.2-12.37.amzn1
samba-krb5-printing-4.6.2-12.37.amzn1
samba-winbind-modules-4.6.2-12.37.amzn1
samba-client-libs-4.6.2-12.37.amzn1
samba-test-libs-4.6.2-12.37.amzn1
libsmbclient-devel-4.6.2-12.37.amzn1

noarch
samba-pidl-4.6.2-12.37.amzn1
samba-common-4.6.2-12.37.amzn1

x86_64
samba-winbind-krb5-locator-4.6.2-12.37.amzn1
samba-debuginfo-4.6.2-12.37.amzn1
samba-client-4.6.2-12.37.amzn1
ctdb-tests-4.6.2-12.37.amzn1
samba-common-libs-4.6.2-12.37.amzn1
samba-common-tools-4.6.2-12.37.amzn1

samba-4.6.2-12.37.amzn1
libsmbclient-4.6.2-12.37.amzn1
libwbclient-4.6.2-12.37.amzn1
samba-client-libs-4.6.2-12.37.amzn1
samba-winbind-clients-4.6.2-12.37.amzn1
ctdb-4.6.2-12.37.amzn1
samba-test-4.6.2-12.37.amzn1
libwbclient-devel-4.6.2-12.37.amzn1
samba-python-4.6.2-12.37.amzn1
samba-winbind-4.6.2-12.37.amzn1
samba-winbind-modules-4.6.2-12.37.amzn1
samba-krb5-printing-4.6.2-12.37.amzn1
samba-libs-4.6.2-12.37.amzn1
samba-devel-4.6.2-12.37.amzn1
samba-test-libs-4.6.2-12.37.amzn1
libsmbclient-devel-4.6.2-12.37.amzn1

170910 - Amazon Linux AMI ALAS-2017-932 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16943, CVE-2017-16944

Description

The scan detected that the host is missing the following update:
ALAS-2017-932

Observation

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

https://alas.aws.amazon.com/ALAS-2017-932.html

Amazon Linux AMI
x86_64
exim-pgsql-4.89-4.17.amzn1
exim-mon-4.89-4.17.amzn1
exim-mysql-4.89-4.17.amzn1
exim-4.89-4.17.amzn1
exim-debuginfo-4.89-4.17.amzn1
exim-greylist-4.89-4.17.amzn1

i686
exim-pgsql-4.89-4.17.amzn1
exim-mon-4.89-4.17.amzn1
exim-mysql-4.89-4.17.amzn1
exim-4.89-4.17.amzn1
exim-debuginfo-4.89-4.17.amzn1
exim-greylist-4.89-4.17.amzn1

170912 - Amazon Linux AMI ALAS-2017-934 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14167, CVE-2017-15289

Description

The scan detected that the host is missing the following update:
ALAS-2017-934

Observation

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

https://alas.aws.amazon.com/ALAS-2017-934.html

Amazon Linux AMI
x86_64
qemu-img-1.5.3-141.5.amzn1
qemu-kvm-common-1.5.3-141.5.amzn1
qemu-kvm-debuginfo-1.5.3-141.5.amzn1
qemu-kvm-tools-1.5.3-141.5.amzn1
qemu-kvm-1.5.3-141.5.amzn1

170913 - Amazon Linux AMI ALAS-2017-937 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0861, CVE-2017-1000405, CVE-2017-1000407, CVE-2017-15115, CVE-2017-16643, CVE-2017-16645, CVE-2017-16646, CVE-2017-16647, CVE-2017-16649, CVE-2017-16650, CVE-2017-16994

Description

The scan detected that the host is missing the following update:
ALAS-2017-937

Observation

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

https://alas.aws.amazon.com/ALAS-2017-937.html

Amazon Linux AMI
i686
kernel-tools-devel-4.9.70-22.55.amzn1
kernel-debuginfo-common-i686-4.9.70-22.55.amzn1
kernel-headers-4.9.70-22.55.amzn1
kernel-tools-4.9.70-22.55.amzn1
kernel-devel-4.9.70-22.55.amzn1
kernel-debuginfo-4.9.70-22.55.amzn1
kernel-tools-debuginfo-4.9.70-22.55.amzn1
perf-debuginfo-4.9.70-22.55.amzn1
perf-4.9.70-22.55.amzn1
kernel-4.9.70-22.55.amzn1

noarch
kernel-doc-4.9.70-22.55.amzn1

x86_64
kernel-headers-4.9.70-22.55.amzn1
perf-debuginfo-4.9.70-22.55.amzn1
kernel-tools-4.9.70-22.55.amzn1
kernel-devel-4.9.70-22.55.amzn1
kernel-debuginfo-4.9.70-22.55.amzn1
kernel-tools-debuginfo-4.9.70-22.55.amzn1

kernel-tools-devel-4.9.70-22.55.amzn1
kernel-debuginfo-common-x86_64-4.9.70-22.55.amzn1
perf-4.9.70-22.55.amzn1
kernel-4.9.70-22.55.amzn1

182562 - FreeBSD rsync Multiple Vulnerabilities (72fff788-e561-11e7-8097-0800271d4b9c)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
rsync -- multiple vulnerabilities (72fff788-e561-11e7-8097-0800271d4b9c)

Observation

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

http://www.vuxml.org/freebsd/72fff788-e561-11e7-8097-0800271d4b9c.html

Affected packages:
3.1.2 <= rsync <= 3.1.2_7

146178 - SuSE SLED 12 SP2, 12 SP3 SUSE-SU-2017:3392-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13735, CVE-2017-14608, CVE-2017-16909

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3392-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003548.html

SuSE SLED 12 SP3
x86_64
libraw-debugsource-0.15.4-16.1
libraw9-0.15.4-16.1
libraw9-debuginfo-0.15.4-16.1

SuSE SLED 12 SP2
x86_64
libraw-debugsource-0.15.4-16.1
libraw9-0.15.4-16.1
libraw9-debuginfo-0.15.4-16.1

146183 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3428-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000083

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3428-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003552.html

SuSE SLED 12 SP2
x86_64
evince-plugin-djvudocument-3.20.2-6.19.15
evince-debuginfo-3.20.2-6.19.15
libevview3-3-3.20.2-6.19.15
evince-plugin-xpsdocument-debuginfo-3.20.2-6.19.15
evince-plugin-psdocument-3.20.2-6.19.15
nautilus-evince-3.20.2-6.19.15
evince-plugin-dvidocument-3.20.2-6.19.15
libevdocument3-4-3.20.2-6.19.15
evince-plugin-pdfdocument-debuginfo-3.20.2-6.19.15
evince-plugin-psdocument-debuginfo-3.20.2-6.19.15
evince-plugin-djvudocument-debuginfo-3.20.2-6.19.15
evince-plugin-tiffdocument-3.20.2-6.19.15
evince-3.20.2-6.19.15
libevview3-3-debuginfo-3.20.2-6.19.15
evince-plugin-xpsdocument-3.20.2-6.19.15
evince-browser-plugin-3.20.2-6.19.15
evince-browser-plugin-debuginfo-3.20.2-6.19.15
evince-debugsource-3.20.2-6.19.15
typelib-1_0-EvinceDocument-3_0-3.20.2-6.19.15
evince-plugin-dvidocument-debuginfo-3.20.2-6.19.15
evince-plugin-pdfdocument-3.20.2-6.19.15
nautilus-evince-debuginfo-3.20.2-6.19.15
libevdocument3-4-debuginfo-3.20.2-6.19.15
typelib-1_0-EvinceView-3_0-3.20.2-6.19.15
evince-plugin-tiffdocument-debuginfo-3.20.2-6.19.15

noarch
evince-lang-3.20.2-6.19.15

SuSE SLES 12 SP3
noarch
evince-lang-3.20.2-6.19.15

x86_64
evince-plugin-djvudocument-3.20.2-6.19.15
evince-debuginfo-3.20.2-6.19.15
libevview3-3-3.20.2-6.19.15
evince-plugin-xpsdocument-debuginfo-3.20.2-6.19.15
evince-plugin-psdocument-3.20.2-6.19.15
nautilus-evince-3.20.2-6.19.15
evince-plugin-dvidocument-3.20.2-6.19.15
libevdocument3-4-3.20.2-6.19.15
evince-plugin-pdfdocument-debuginfo-3.20.2-6.19.15
evince-plugin-psdocument-debuginfo-3.20.2-6.19.15

evince-plugin-djvudocument-debuginfo-3.20.2-6.19.15
evince-plugin-tiffdocument-3.20.2-6.19.15
evince-3.20.2-6.19.15
libevview3-3-debuginfo-3.20.2-6.19.15
evince-plugin-xpsdocument-3.20.2-6.19.15
evince-browser-plugin-3.20.2-6.19.15
evince-browser-plugin-debuginfo-3.20.2-6.19.15
evince-debugsource-3.20.2-6.19.15
nautilus-evince-debuginfo-3.20.2-6.19.15
evince-plugin-dvidocument-debuginfo-3.20.2-6.19.15
evince-plugin-pdfdocument-3.20.2-6.19.15
libevdocument3-4-debuginfo-3.20.2-6.19.15
evince-plugin-tiffdocument-debuginfo-3.20.2-6.19.15

SuSE SLES 12 SP2
noarch
evince-lang-3.20.2-6.19.15

x86_64
evince-plugin-djvudocument-3.20.2-6.19.15
evince-debuginfo-3.20.2-6.19.15
libevview3-3-3.20.2-6.19.15
evince-plugin-xpsdocument-debuginfo-3.20.2-6.19.15
evince-plugin-psdocument-3.20.2-6.19.15
nautilus-evince-3.20.2-6.19.15
evince-plugin-dvidocument-3.20.2-6.19.15
libevdocument3-4-3.20.2-6.19.15
evince-plugin-pdfdocument-debuginfo-3.20.2-6.19.15
evince-plugin-psdocument-debuginfo-3.20.2-6.19.15
evince-plugin-djvudocument-debuginfo-3.20.2-6.19.15
evince-plugin-tiffdocument-3.20.2-6.19.15
evince-3.20.2-6.19.15
libevview3-3-debuginfo-3.20.2-6.19.15
evince-plugin-xpsdocument-3.20.2-6.19.15
evince-browser-plugin-3.20.2-6.19.15
evince-browser-plugin-debuginfo-3.20.2-6.19.15
evince-debugsource-3.20.2-6.19.15
nautilus-evince-debuginfo-3.20.2-6.19.15
evince-plugin-dvidocument-debuginfo-3.20.2-6.19.15
evince-plugin-pdfdocument-3.20.2-6.19.15
libevdocument3-4-debuginfo-3.20.2-6.19.15
evince-plugin-tiffdocument-debuginfo-3.20.2-6.19.15

SuSE SLED 12 SP3
x86_64
evince-plugin-djvudocument-3.20.2-6.19.15
evince-debuginfo-3.20.2-6.19.15
libevview3-3-3.20.2-6.19.15
evince-plugin-xpsdocument-debuginfo-3.20.2-6.19.15
evince-plugin-psdocument-3.20.2-6.19.15
nautilus-evince-3.20.2-6.19.15
evince-plugin-dvidocument-3.20.2-6.19.15
libevdocument3-4-3.20.2-6.19.15
evince-plugin-pdfdocument-debuginfo-3.20.2-6.19.15
evince-plugin-psdocument-debuginfo-3.20.2-6.19.15
evince-plugin-djvudocument-debuginfo-3.20.2-6.19.15
evince-plugin-tiffdocument-3.20.2-6.19.15
evince-3.20.2-6.19.15
libevview3-3-debuginfo-3.20.2-6.19.15
evince-plugin-xpsdocument-3.20.2-6.19.15

evince-browser-plugin-3.20.2-6.19.15
evince-browser-plugin-debuginfo-3.20.2-6.19.15
evince-debugsource-3.20.2-6.19.15
typelib-1_0-EvinceDocument-3_0-3.20.2-6.19.15
evince-plugin-dvidocument-debuginfo-3.20.2-6.19.15
evince-plugin-pdfdocument-3.20.2-6.19.15
nautilus-evince-debuginfo-3.20.2-6.19.15
libevdocument3-4-debuginfo-3.20.2-6.19.15
typelib-1_0-EvinceView-3_0-3.20.2-6.19.15
evince-plugin-tiffdocument-debuginfo-3.20.2-6.19.15

noarch
evince-lang-3.20.2-6.19.15

146186 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3431-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000083

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3431-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00104.html

SuSE Linux 42.2
x86_64
evince-devel-3.20.2-2.6.1
libevdocument3-4-3.20.2-2.6.1
typelib-1_0-EvinceDocument-3_0-3.20.2-2.6.1
evince-plugin-dvidocument-debuginfo-3.20.2-2.6.1
evince-browser-plugin-3.20.2-2.6.1
libevview3-3-3.20.2-2.6.1
evince-plugin-tiffdocument-3.20.2-2.6.1
evince-plugin-psdocument-3.20.2-2.6.1
typelib-1_0-EvinceView-3_0-3.20.2-2.6.1
nautilus-evince-debuginfo-3.20.2-2.6.1
evince-plugin-comicsdocument-3.20.2-2.6.1
evince-browser-plugin-debuginfo-3.20.2-2.6.1
libevview3-3-debuginfo-3.20.2-2.6.1
evince-plugin-djvudocument-3.20.2-2.6.1
evince-plugin-djvudocument-debuginfo-3.20.2-2.6.1
evince-debugsource-3.20.2-2.6.1
evince-plugin-tiffdocument-debuginfo-3.20.2-2.6.1
evince-plugin-xpsdocument-debuginfo-3.20.2-2.6.1
evince-plugin-dvidocument-3.20.2-2.6.1
evince-3.20.2-2.6.1
evince-plugin-pdfdocument-3.20.2-2.6.1
evince-plugin-xpsdocument-3.20.2-2.6.1
evince-plugin-pdfdocument-debuginfo-3.20.2-2.6.1
evince-debuginfo-3.20.2-2.6.1
libevdocument3-4-debuginfo-3.20.2-2.6.1
evince-plugin-psdocument-debuginfo-3.20.2-2.6.1

evince-plugin-comicsdocument-debuginfo-3.20.2-2.6.1
nautilus-evince-3.20.2-2.6.1

noarch
evince-lang-3.20.2-2.6.1

SuSE Linux 42.3
x86_64
evince-plugin-djvudocument-debuginfo-3.20.2-6.1
evince-plugin-comicsdocument-3.20.2-6.1
evince-plugin-pdfdocument-3.20.2-6.1
libevdocument3-4-debuginfo-3.20.2-6.1
evince-plugin-djvudocument-3.20.2-6.1
evince-devel-3.20.2-6.1
nautilus-evince-debuginfo-3.20.2-6.1
evince-plugin-comicsdocument-debuginfo-3.20.2-6.1
evince-plugin-pdfdocument-debuginfo-3.20.2-6.1
evince-debugsource-3.20.2-6.1
libevview3-3-3.20.2-6.1
evince-browser-plugin-3.20.2-6.1
evince-plugin-dvidocument-3.20.2-6.1
evince-3.20.2-6.1
nautilus-evince-3.20.2-6.1
libevdocument3-4-3.20.2-6.1
evince-debuginfo-3.20.2-6.1
libevview3-3-debuginfo-3.20.2-6.1
evince-plugin-tiffdocument-debuginfo-3.20.2-6.1
evince-plugin-tiffdocument-3.20.2-6.1
evince-plugin-xpsdocument-debuginfo-3.20.2-6.1
typelib-1_0-EvinceDocument-3_0-3.20.2-6.1
evince-plugin-dvidocument-debuginfo-3.20.2-6.1
evince-plugin-xpsdocument-3.20.2-6.1
typelib-1_0-EvinceView-3_0-3.20.2-6.1
evince-browser-plugin-debuginfo-3.20.2-6.1
evince-plugin-psdocument-3.20.2-6.1
evince-plugin-psdocument-debuginfo-3.20.2-6.1

noarch
evince-lang-3.20.2-6.1

170914 - Amazon Linux AMI ALAS-2017-936 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10193, CVE-2017-10198, 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:
ALAS-2017-936

Observation

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

https://alas.aws.amazon.com/ALAS-2017-936.html

Amazon Linux AMI
i686
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.75.amzn1
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.75.amzn1
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.75.amzn1
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.75.amzn1
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.75.amzn1

noarch
java-1.7.0-openjdk-javadoc-1.7.0.161-2.6.12.0.75.amzn1

x86_64
java-1.7.0-openjdk-1.7.0.161-2.6.12.0.75.amzn1
java-1.7.0-openjdk-debuginfo-1.7.0.161-2.6.12.0.75.amzn1
java-1.7.0-openjdk-devel-1.7.0.161-2.6.12.0.75.amzn1
java-1.7.0-openjdk-demo-1.7.0.161-2.6.12.0.75.amzn1
java-1.7.0-openjdk-src-1.7.0.161-2.6.12.0.75.amzn1

22853 - Cisco NX-OS Software CLI Command Injection Vulnerability (cisco-sa-20171129-fxnx)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12329

Description

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

Observation

Cisco NX-OS is a network operating system .

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to insufficient input validation of command-line arguments. Successful exploitation could allow a remote attacker to execute arbitrary commands at the user's privilege level within the context of the affected application.

146179 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3391-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15098, CVE-2017-15099

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3391-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003547.html

SuSE SLES 12 SP2
noarch
postgresql96-docs-9.6.6-3.10.1

x86_64
postgresql96-contrib-9.6.6-3.10.1

postgresql96-debugsource-9.6.6-3.10.1
libecpg6-debuginfo-9.6.6-3.10.1
libpq5-debuginfo-32bit-9.6.6-3.10.1
postgresql96-libs-debugsource-9.6.6-3.10.1
postgresql96-server-debuginfo-9.6.6-3.10.1
postgresql96-server-9.6.6-3.10.1
postgresql96-9.6.6-3.10.1
libpq5-debuginfo-9.6.6-3.10.1
libecpg6-9.6.6-3.10.1
postgresql96-debuginfo-9.6.6-3.10.1
postgresql96-contrib-debuginfo-9.6.6-3.10.1
libpq5-9.6.6-3.10.1
libpq5-32bit-9.6.6-3.10.1

SuSE SLED 12 SP3
x86_64
libecpg6-9.6.6-3.10.1
libpq5-debuginfo-32bit-9.6.6-3.10.1
postgresql96-debuginfo-9.6.6-3.10.1
libpq5-9.6.6-3.10.1
libpq5-debuginfo-9.6.6-3.10.1
postgresql96-9.6.6-3.10.1
libpq5-32bit-9.6.6-3.10.1
postgresql96-debugsource-9.6.6-3.10.1
libecpg6-debuginfo-9.6.6-3.10.1
postgresql96-libs-debugsource-9.6.6-3.10.1

SuSE SLED 12 SP2
x86_64
libecpg6-9.6.6-3.10.1
libpq5-debuginfo-32bit-9.6.6-3.10.1
postgresql96-debuginfo-9.6.6-3.10.1
libpq5-9.6.6-3.10.1
libpq5-debuginfo-9.6.6-3.10.1
postgresql96-9.6.6-3.10.1
libpq5-32bit-9.6.6-3.10.1
postgresql96-debugsource-9.6.6-3.10.1
libecpg6-debuginfo-9.6.6-3.10.1
postgresql96-libs-debugsource-9.6.6-3.10.1

SuSE SLES 12 SP3
noarch
postgresql96-docs-9.6.6-3.10.1

x86_64
postgresql96-contrib-9.6.6-3.10.1
postgresql96-debugsource-9.6.6-3.10.1
libecpg6-debuginfo-9.6.6-3.10.1
libpq5-debuginfo-32bit-9.6.6-3.10.1
postgresql96-libs-debugsource-9.6.6-3.10.1
postgresql96-server-debuginfo-9.6.6-3.10.1
postgresql96-server-9.6.6-3.10.1
postgresql96-9.6.6-3.10.1
libpq5-debuginfo-9.6.6-3.10.1
libecpg6-9.6.6-3.10.1
postgresql96-debuginfo-9.6.6-3.10.1
postgresql96-contrib-debuginfo-9.6.6-3.10.1
libpq5-9.6.6-3.10.1
libpq5-32bit-9.6.6-3.10.1

146180 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3425-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15098, CVE-2017-15099

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3425-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00099.html

SuSE Linux 42.2
i586
postgresql96-plperl-debuginfo-9.6.6-8.1
libpq5-9.6.6-8.1
libecpg6-debuginfo-9.6.6-8.1
postgresql96-contrib-debuginfo-9.6.6-8.1
postgresql96-debugsource-9.6.6-8.1
postgresql96-devel-9.6.6-8.1
postgresql96-9.6.6-8.1
postgresql96-libs-debugsource-9.6.6-8.1
libpq5-debuginfo-9.6.6-8.1
postgresql96-server-debuginfo-9.6.6-8.1
postgresql96-plperl-9.6.6-8.1
postgresql96-plpython-debuginfo-9.6.6-8.1
postgresql96-server-9.6.6-8.1
postgresql96-devel-debuginfo-9.6.6-8.1
postgresql96-pltcl-9.6.6-8.1
postgresql96-test-9.6.6-8.1
postgresql96-contrib-9.6.6-8.1
postgresql96-pltcl-debuginfo-9.6.6-8.1
libecpg6-9.6.6-8.1
postgresql96-debuginfo-9.6.6-8.1
postgresql96-plpython-9.6.6-8.1

noarch
postgresql96-docs-9.6.6-8.1

x86_64
postgresql96-plperl-debuginfo-9.6.6-8.1
libpq5-9.6.6-8.1
libecpg6-debuginfo-9.6.6-8.1
postgresql96-contrib-debuginfo-9.6.6-8.1
postgresql96-debugsource-9.6.6-8.1
postgresql96-devel-9.6.6-8.1
libpq5-32bit-9.6.6-8.1
postgresql96-9.6.6-8.1
postgresql96-libs-debugsource-9.6.6-8.1
libpq5-debuginfo-9.6.6-8.1
postgresql96-server-debuginfo-9.6.6-8.1
libpq5-debuginfo-32bit-9.6.6-8.1
postgresql96-plperl-9.6.6-8.1
libecpg6-debuginfo-32bit-9.6.6-8.1
postgresql96-plpython-debuginfo-9.6.6-8.1

postgresql96-server-9.6.6-8.1
postgresql96-devel-debuginfo-9.6.6-8.1
postgresql96-pltcl-9.6.6-8.1
postgresql96-test-9.6.6-8.1
postgresql96-contrib-9.6.6-8.1
postgresql96-pltcl-debuginfo-9.6.6-8.1
libecpg6-9.6.6-8.1
libecpg6-32bit-9.6.6-8.1
postgresql96-debuginfo-9.6.6-8.1
postgresql96-plpython-9.6.6-8.1

SuSE Linux 42.3
i586
postgresql96-devel-9.6.6-9.1
postgresql96-plperl-9.6.6-9.1
postgresql96-server-9.6.6-9.1
postgresql96-debugsource-9.6.6-9.1
postgresql96-debuginfo-9.6.6-9.1
postgresql96-plpython-9.6.6-9.1
postgresql96-test-9.6.6-9.1
postgresql96-devel-debuginfo-9.6.6-9.1
postgresql96-libs-debugsource-9.6.6-9.1
postgresql96-pltcl-debuginfo-9.6.6-9.1
postgresql96-pltcl-9.6.6-9.1
postgresql96-plpython-debuginfo-9.6.6-9.1
libecpg6-9.6.6-9.1
postgresql96-contrib-debuginfo-9.6.6-9.1
libpq5-9.6.6-9.1
postgresql96-contrib-9.6.6-9.1
postgresql96-server-debuginfo-9.6.6-9.1
libecpg6-debuginfo-9.6.6-9.1
postgresql96-plperl-debuginfo-9.6.6-9.1
libpq5-debuginfo-9.6.6-9.1
postgresql96-9.6.6-9.1

noarch
postgresql96-docs-9.6.6-9.1

x86_64
postgresql96-devel-9.6.6-9.1
postgresql96-plperl-9.6.6-9.1
postgresql96-server-9.6.6-9.1
postgresql96-debugsource-9.6.6-9.1
postgresql96-debuginfo-9.6.6-9.1
postgresql96-plpython-9.6.6-9.1
postgresql96-test-9.6.6-9.1
postgresql96-devel-debuginfo-9.6.6-9.1
postgresql96-libs-debugsource-9.6.6-9.1
postgresql96-pltcl-debuginfo-9.6.6-9.1
libpq5-32bit-9.6.6-9.1
postgresql96-pltcl-9.6.6-9.1
postgresql96-plpython-debuginfo-9.6.6-9.1
libecpg6-9.6.6-9.1
libpq5-debuginfo-32bit-9.6.6-9.1
postgresql96-contrib-debuginfo-9.6.6-9.1
libpq5-9.6.6-9.1
libecpg6-debuginfo-32bit-9.6.6-9.1
postgresql96-contrib-9.6.6-9.1
libecpg6-32bit-9.6.6-9.1
postgresql96-server-debuginfo-9.6.6-9.1

libecpg6-debuginfo-9.6.6-9.1
postgresql96-plperl-debuginfo-9.6.6-9.1
libpq5-debuginfo-9.6.6-9.1
postgresql96-9.6.6-9.1

170911 - Amazon Linux AMI ALAS-2017-935 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
ALAS-2017-935

Observation

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

https://alas.aws.amazon.com/ALAS-2017-935.html

Amazon Linux AMI
i686
libsss_idmap-devel-1.15.2-50.34.amzn1
libsss_simpleifp-1.15.2-50.34.amzn1
python27-sss-1.15.2-50.34.amzn1
libsss_idmap-1.15.2-50.34.amzn1
sssd-libwbclient-devel-1.15.2-50.34.amzn1
sssd-proxy-1.15.2-50.34.amzn1
libsss_certmap-devel-1.15.2-50.34.amzn1
sssd-krb5-common-1.15.2-50.34.amzn1
sssd-krb5-1.15.2-50.34.amzn1
python27-libsss_nss_idmap-1.15.2-50.34.amzn1
sssd-common-1.15.2-50.34.amzn1
python27-sss-murmur-1.15.2-50.34.amzn1
sssd-client-1.15.2-50.34.amzn1
libsss_sudo-1.15.2-50.34.amzn1
libsss_nss_idmap-devel-1.15.2-50.34.amzn1
sssd-libwbclient-1.15.2-50.34.amzn1
libipa_hbac-devel-1.15.2-50.34.amzn1
sssd-tools-1.15.2-50.34.amzn1
libsss_nss_idmap-1.15.2-50.34.amzn1
python27-libipa_hbac-1.15.2-50.34.amzn1
sssd-ad-1.15.2-50.34.amzn1
libsss_simpleifp-devel-1.15.2-50.34.amzn1
libipa_hbac-1.15.2-50.34.amzn1
libsss_autofs-1.15.2-50.34.amzn1
sssd-common-pac-1.15.2-50.34.amzn1
sssd-debuginfo-1.15.2-50.34.amzn1
sssd-ldap-1.15.2-50.34.amzn1
sssd-1.15.2-50.34.amzn1
sssd-dbus-1.15.2-50.34.amzn1
libsss_certmap-1.15.2-50.34.amzn1
sssd-ipa-1.15.2-50.34.amzn1
sssd-winbind-idmap-1.15.2-50.34.amzn1

noarch
python27-sssdconfig-1.15.2-50.34.amzn1

x86_64
libsss_idmap-devel-1.15.2-50.34.amzn1
python27-libipa_hbac-1.15.2-50.34.amzn1
python27-sss-1.15.2-50.34.amzn1
libsss_idmap-1.15.2-50.34.amzn1
sssd-libwbclient-devel-1.15.2-50.34.amzn1
sssd-proxy-1.15.2-50.34.amzn1
libsss_certmap-devel-1.15.2-50.34.amzn1
sssd-krb5-common-1.15.2-50.34.amzn1
sssd-krb5-1.15.2-50.34.amzn1
python27-libsss_nss_idmap-1.15.2-50.34.amzn1
sssd-common-1.15.2-50.34.amzn1
python27-sss-murmur-1.15.2-50.34.amzn1
sssd-client-1.15.2-50.34.amzn1
libsss_sudo-1.15.2-50.34.amzn1
libsss_nss_idmap-devel-1.15.2-50.34.amzn1
sssd-libwbclient-1.15.2-50.34.amzn1
libipa_hbac-devel-1.15.2-50.34.amzn1
sssd-tools-1.15.2-50.34.amzn1
libsss_nss_idmap-1.15.2-50.34.amzn1
sssd-ad-1.15.2-50.34.amzn1
libsss_simpleifp-devel-1.15.2-50.34.amzn1
libipa_hbac-1.15.2-50.34.amzn1
libsss_autofs-1.15.2-50.34.amzn1
sssd-common-pac-1.15.2-50.34.amzn1
sssd-debuginfo-1.15.2-50.34.amzn1
libsss_simpleifp-1.15.2-50.34.amzn1
sssd-ldap-1.15.2-50.34.amzn1
sssd-1.15.2-50.34.amzn1
sssd-dbus-1.15.2-50.34.amzn1
libsss_certmap-1.15.2-50.34.amzn1
sssd-ipa-1.15.2-50.34.amzn1
sssd-winbind-idmap-1.15.2-50.34.amzn1

22878 - Cisco Jabber Clients Cross-Site Scripting Vulnerability (cisco-sa-20171129-jabber1)

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

Risk Level: Low

CVE: CVE-2017-12358

Description

A cross-site scripting vulnerability is present in some versions of Cisco Jabber.

Observation

Cisco Jabber is Cisco unified communication software solution.

A cross-site scripting vulnerability is present in some versions of Cisco Jabber. The flaw lies in the web-based management interface of Cisco Jabber. Successful exploitation could allow an attacker to execute remote code.

88905 - Slackware Linux 14.2 SSA:2017-356-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2017-356-01

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=2017&m=slackware-security.357916

Slackware 14.2
x86_64
mozilla-thunderbird-52.5.2-x86_64-1

i586
mozilla-thunderbird-52.5.2-i586-1

88906 - Slackware Linux 14.2 SSA:2017-353-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17405

Description

The scan detected that the host is missing the following update:
SSA:2017-353-01

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=2017&m=slackware-security.365977

Slackware 14.2
x86_64
ruby-2.2.9-x86_64-1

i586
ruby-2.2.9-i586-1

130977 - Debian Linux 8.0, 9.0 DSA-4070-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17843, CVE-2017-17844, CVE-2017-17845, CVE-2017-17846, CVE-2017-17847, CVE-2017-17848

Description

The scan detected that the host is missing the following update:
DSA-4070-1

Observation

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

http://www.debian.org/security/2017/dsa-4070

Debian 8.0
all
enigmail_2:1.9.9-1~deb8u1

Debian 9.0
all
enigmail_2:1.9.9-1~deb9u1

130978 - Debian Linux 8.0, 9.0 DSA-4069-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17476

Description

The scan detected that the host is missing the following update:
DSA-4069-1

Observation

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

http://www.debian.org/security/2017/dsa-4069

Debian 8.0
all
otrs2_3.3.18-1+deb8u4

Debian 9.0
all
otrs2_5.0.16-1+deb9u5

130979 - Debian Linux 9.0 DSA-4072-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13098

Description

The scan detected that the host is missing the following update:
DSA-4072-1

Observation

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

http://www.debian.org/security/2017/dsa-4072

Debian 9.0
all
libbcmail-java_1.56-1+deb9u1
libbcpkix-java_1.56-1+deb9u1
libbcmail-java-doc_1.56-1+deb9u1
libbcprov-java_1.56-1+deb9u1
libbcpg-java-doc_1.56-1+deb9u1

libbcprov-java-doc_1.56-1+deb9u1
libbcpg-java_1.56-1+deb9u1
libbcpkix-java-doc_1.56-1+deb9u1

130981 - Debian Linux 8.0, 9.0 DSA-4071-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17512

Description

The scan detected that the host is missing the following update:
DSA-4071-1

Observation

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

http://www.debian.org/security/2017/dsa-4071

Debian 8.0
all
sensible-utils_0.0.9+deb8u1

Debian 9.0
all
sensible-utils_0.0.9+deb9u1

141810 - Red Hat Enterprise Linux RHSA-2017-3490 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-3490

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00038.html

RHEL6_7S
i386
redhat-release-server-6Server-6.7.0.5.el6_7

x86_64
redhat-release-server-6Server-6.7.0.5.el6_7

182560 - FreeBSD phpMyAdmin XSRF/CSRF Vulnerability (63eb2b11-e802-11e7-a58c-6805ca0b3d42)

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:
phpMyAdmin -- XSRF/CSRF vulnerability (63eb2b11-e802-11e7-a58c-6805ca0b3d42)

Observation

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

http://www.vuxml.org/freebsd/63eb2b11-e802-11e7-a58c-6805ca0b3d42.html

Affected packages:
4.7.0 <= phpMyAdmin < 4.7.7

182561 - FreeBSD asterisk Crash In PJSIP Resource When Missing A Contact Header (2a3bc6ac-e7c6-11e7-a90b-001999f8d30b)

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

Risk Level: Low

CVE: CVE-2017-17850

Description

The scan detected that the host is missing the following update:
asterisk -- Crash in PJSIP resource when missing a contact header (2a3bc6ac-e7c6-11e7-a90b-001999f8d30b)

Observation

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

http://www.vuxml.org/freebsd/2a3bc6ac-e7c6-11e7-a90b-001999f8d30b.html

Affected packages:
asterisk13 < 13.18.5

182563 - FreeBSD mozilla Multiple Vulnerabilities (6a09c80e-6ec7-442a-bc65-d72ce69fd887)

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

Risk Level: Low

CVE: CVE-2017-7829, CVE-2017-7845, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (6a09c80e-6ec7-442a-bc65-d72ce69fd887)

Observation

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

http://www.vuxml.org/freebsd/6a09c80e-6ec7-442a-bc65-d72ce69fd887.html

Affected packages:
thunderbird < 52.5.2
linux-thunderbird < 52.5.2

182564 - FreeBSD MariaDB Unspecified Vulnerability (b7d89082-e7c0-11e7-ac58-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-15365

Description

The scan detected that the host is missing the following update:
MariaDB -- unspecified vulnerability (b7d89082-e7c0-11e7-ac58-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/b7d89082-e7c0-11e7-ac58-b499baebfeaf.html

Affected packages:
mariadb101-client < 10.1.30
mariadb102-client < 10.2.10

193109 - Fedora Linux 27 FEDORA-2017-1ebb87e7c0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17741

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1ebb87e7c0

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/2017/12/?count=200&page=1

Fedora Core 27

kernel-4.14.8-300.fc27

193110 - Fedora Linux 26 FEDORA-2017-6d952bdc53 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6d952bdc53

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/2017/12/?count=200&page=1

Fedora Core 26

json-c-0.12.1-5.fc26

193111 - Fedora Linux 27 FEDORA-2017-f7cb245861 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17712

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f7cb245861

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/2017/12/?count=200&page=1

Fedora Core 27

kernel-4.14.7-300.fc27

193112 - Fedora Linux 26 FEDORA-2017-7810b7c59f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17712, CVE-2017-17741

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7810b7c59f

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/2017/12/?count=200&page=1

Fedora Core 26

kernel-4.14.8-200.fc26

193113 - Fedora Linux 27 FEDORA-2017-20b18a4ffe Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2017-20b18a4ffe

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/2017/12/?count=200&page=1

Fedora Core 27

json-c-0.12.1-5.fc27

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

22357 - IBM WebSphere Application Server Multiple Java Vulnerabilities (swg22007002)

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

Risk Level: Medium

CVE: CVE-2017-10102, CVE-2017-10115, CVE-2017-10116

Update Details

FASLScript is updated

182493 - FreeBSD MySQL Multiple Vulnerabilities (c41bedfd-b3f9-11e7-ac58-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10165, CVE-2017-10167, CVE-2017-10203, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10277, CVE-2017-10279, CVE-2017-10283, CVE-2017-10284, CVE-2017-10286, CVE-2017-10294, CVE-2017-10296, CVE-2017-10311, CVE-2017-10313, CVE-2017-10314, CVE-2017-10320, CVE-2017-10365, CVE-2017-10376, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Update Details

CVE is updated

70017 - cisco.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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