2017-AUG-24
FSL version 7.5.954

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

130855 - Debian Linux 8.0 DSA-3945-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9940, CVE-2017-1000363, CVE-2017-1000365, CVE-2017-10911, CVE-2017-11176, CVE-2017-7346, CVE-2017-7482, CVE-2017-7533, CVE-2017-7541, CVE-2017-7542, CVE-2017-7889, CVE-2017-9605

Description

The scan detected that the host is missing the following update:
DSA-3945-1

Observation

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

http://www.debian.org/security/2017/dsa-3945

Debian 8.0
all
linux-headers-3.16.0-4-r4k-ip22_3.16.43-2+deb8u3
linux-image-3.16.0-4-powerpc-smp_3.16.43-2+deb8u3
usb-storage-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u3
efi-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
multipath-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u3
virtio-modules-3.16.0-4-loongson-3-di_3.16.43-2+deb8u3
firewire-core-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u3
nic-usb-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u3
linux-image-3.16.0-4-arm64-dbg_3.16.43-2+deb8u3
crypto-dm-modules-3.16.0-4-r5k-ip32-di_3.16.43-2+deb8u3
nbd-modules-3.16.0-4-r4k-ip22-di_3.16.43-2+deb8u3
sound-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u3
isofs-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u3
sata-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
ppp-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u3
scsi-core-modules-3.16.0-4-586-di_3.16.43-2+deb8u3
input-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u3
nbd-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
kernel-image-3.16.0-4-armmp-di_3.16.43-2+deb8u3
ata-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u3
hfs-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u3
pata-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
multipath-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
nic-modules-3.16.0-4-586-di_3.16.43-2+deb8u3
kernel-image-3.16.0-4-586-di_3.16.43-2+deb8u3
crc-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u3
nic-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u3

linux-headers-3.16.0-4-all_3.16.43-2+deb8u3
nbd-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u3
hfs-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
loop-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u3
nic-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u3
zlib-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u3
kernel-image-3.16.0-4-loongson-3-di_3.16.43-2+deb8u3
ata-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u3
multipath-modules-3.16.0-4-586-di_3.16.43-2+deb8u3
usb-storage-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u3
scsi-core-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
linux-manual-3.16_3.16.43-2+deb8u3
usb-storage-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u3
loop-modules-3.16.0-4-r5k-ip32-di_3.16.43-2+deb8u3
ppp-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
ext4-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u3
fuse-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u3
xfs-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u3
nic-shared-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u3
udf-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u3
firewire-core-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u3
scsi-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u3
affs-modules-3.16.0-4-octeon-di_3.16.43-2+deb8u3
jfs-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u3
fat-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u3
speakup-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
virtio-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u3
event-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
multipath-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u3
pata-modules-3.16.0-4-586-di_3.16.43-2+deb8u3
fuse-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u3
xfs-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u3
sound-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u3
nic-pcmcia-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
loop-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u3
firewire-core-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
crypto-modules-3.16.0-4-octeon-di_3.16.43-2+deb8u3
linux-image-3.16.0-4-armmp-lpae_3.16.43-2+deb8u3
crc-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
serial-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u3
acpi-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u3
mmc-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u3
fuse-modules-3.16.0-4-r5k-ip32-di_3.16.43-2+deb8u3
squashfs-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u3
isofs-modules-3.16.0-4-586-di_3.16.43-2+deb8u3
jfs-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u3
ppp-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u3
sound-modules-3.16.0-4-586-di_3.16.43-2+deb8u3
nic-shared-modules-3.16.0-4-r5k-ip32-di_3.16.43-2+deb8u3
cdrom-core-modules-3.16.0-4-586-di_3.16.43-2+deb8u3
linux-source-3.16_3.16.43-2+deb8u3
linux-image-3.16.0-4-arm64_3.16.43-2+deb8u3
core-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u3
ext4-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u3
isofs-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
cdrom-core-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u3
event-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u3
scsi-extra-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u3
mtd-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u3
usb-serial-modules-3.16.0-4-octeon-di_3.16.43-2+deb8u3

nic-usb-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u3
linux-headers-3.16.0-4-all-arm64_3.16.43-2+deb8u3
linux-image-3.16.0-4-loongson-3_3.16.43-2+deb8u3
usb-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u3
hypervisor-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u3
dasd-modules-3.16.0-4-s390x-di_3.16.43-2+deb8u3
crc-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u3
usb-storage-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u3
mouse-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u3
fuse-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u3
zlib-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u3
nbd-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u3
udf-modules-3.16.0-4-loongson-3-di_3.16.43-2+deb8u3
linux-compiler-gcc-4.8-s390_3.16.43-2+deb8u3
usb-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u3
squashfs-modules-3.16.0-4-r4k-ip22-di_3.16.43-2+deb8u3
md-modules-3.16.0-4-586-di_3.16.43-2+deb8u3
scsi-core-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
ppp-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u3
nic-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u3
linux-headers-3.16.0-4-armmp-lpae_3.16.43-2+deb8u3
minix-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u3
loop-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u3
kernel-image-3.16.0-4-arm64-di_3.16.43-2+deb8u3
crc-modules-3.16.0-4-octeon-di_3.16.43-2+deb8u3
linux-headers-3.16.0-4-sb1-bcm91250a_3.16.43-2+deb8u3
md-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u3
multipath-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u3
linux-image-3.16.0-4-versatile_3.16.43-2+deb8u3
core-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u3
loop-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u3
ppp-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u3
nic-usb-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u3
udf-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u3
usb-storage-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
crc-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u3
btrfs-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u3
usb-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
ata-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u3
linux-headers-3.16.0-4-all-amd64_3.16.43-2+deb8u3
xfs-modules-3.16.0-4-s390x-di_3.16.43-2+deb8u3
crypto-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u3
isofs-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u3
isofs-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u3
linux-headers-3.16.0-4-r5k-ip32_3.16.43-2+deb8u3
ext4-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u3

175211 - Scientific Linux Security ERRATA Moderate: libtasn1 on SL7.x x86_64 (1708-11423)

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

Risk Level: High

CVE: CVE-2015-2806, CVE-2015-3622

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libtasn1 on SL7.x x86_64 (1708-11423)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=11423

SL7
x86_64
libtasn1-4.10-1.el7
libtasn1-tools-4.10-1.el7
libtasn1-devel-4.10-1.el7
libtasn1-debuginfo-4.10-1.el7

175240 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1708-14699)

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

Risk Level: High

CVE: CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1708-14699)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=14699

SL7
x86_64
kernel-tools-libs-devel-3.10.0-693.el7
python-perf-3.10.0-693.el7
kernel-tools-3.10.0-693.el7
kernel-debug-3.10.0-693.el7
kernel-debug-devel-3.10.0-693.el7
kernel-debuginfo-common-x86_64-3.10.0-693.el7
kernel-debuginfo-3.10.0-693.el7
kernel-devel-3.10.0-693.el7
perf-debuginfo-3.10.0-693.el7
kernel-tools-debuginfo-3.10.0-693.el7
kernel-3.10.0-693.el7
kernel-headers-3.10.0-693.el7
kernel-debug-debuginfo-3.10.0-693.el7
kernel-tools-libs-3.10.0-693.el7
perf-3.10.0-693.el7
python-perf-debuginfo-3.10.0-693.el7

noarch
kernel-abi-whitelists-3.10.0-693.el7
kernel-doc-3.10.0-693.el7

178484 - Gentoo Linux GLSA-201708-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6706

Description

The scan detected that the host is missing the following update:
GLSA-201708-05

Observation

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

https://security.gentoo.org/glsa/201708-05

Affected packages:
app-arch/rar < 5.5.0_beta4
app-arch/unrar < 5.5.5

22295 - Mozilla Firefox Multiple Vulnerabilities Prior To 55

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7780, CVE-2017-7781, CVE-2017-7782, CVE-2017-7783, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7788, CVE-2017-7789, CVE-2017-7790, CVE-2017-7791, CVE-2017-7792, CVE-2017-7794, CVE-2017-7796, CVE-2017-7797, CVE-2017-7798, CVE-2017-7799, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7804, CVE-2017-7806, CVE-2017-7807, CVE-2017-7808, CVE-2017-7809

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, conduct spoofing attacks, retrieve sensitive data, remotely execute arbitrary code on the target system or cause a denial of service condition.

22296 - Mozilla Firefox Multiple Vulnerabilities Prior To 55

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7780, CVE-2017-7781, CVE-2017-7782, CVE-2017-7783, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7788, CVE-2017-7789, CVE-2017-7790, CVE-2017-7791, CVE-2017-7792, CVE-2017-7794, CVE-2017-7796, CVE-2017-7797, CVE-2017-7798, CVE-2017-7799, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7804, CVE-2017-7806, CVE-2017-7807, CVE-2017-7808, CVE-2017-7809

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, conduct spoofing attacks, retrieve sensitive data, remotely execute

arbitrary code on the target system or cause a denial of service condition.

22316 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52.3

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7782, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7804, CVE-2017-7807, CVE-2017-7809

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful exploitation could allow a malicious user to conduct spoofing and hijacking attacks, cause a denial of service condition, retrieve sensitive data or remotely execute arbitrary code on the target system.

22317 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 52.3

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7782, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7804, CVE-2017-7807, CVE-2017-7809

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. The flaws lie in several components. Successful exploitation could allow a malicious user to conduct spoofing and hijacking attacks, cause a denial of service condition, retrieve sensitive data or remotely execute arbitrary code on the target system.

175233 - Scientific Linux Security ERRATA Critical: firefox on SL6.x, SL7.x i386/x86_64 (1708-3457)

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7798, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7807, CVE-2017-7809

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL6.x, SL7.x i386/x86_64 (1708-3457)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=3457

SL7
x86_64
firefox-52.3.0-2.el7_4
firefox-debuginfo-52.3.0-2.el7_4

SL6
x86_64
firefox-52.3.0-3.el6_9
firefox-debuginfo-52.3.0-3.el6_9

i386
firefox-52.3.0-3.el6_9
firefox-debuginfo-52.3.0-3.el6_9

22307 - (K22317030) F5 BIG-IP iControl REST Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6145

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in iControl REST component. Successful exploitation could allow an attacker to bypass certain security restrictions.

22308 - (CTX225941) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-12134, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in multiple components. Successful exploitation could allow a malicious administrator of a guest VM to compromise the host.

22319 - (K20486351) F5 BIG-IP Glibc Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-1000366

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the glibc component. Successful exploitation could allow attackers to execute arbitrary code in the context of application, disclose sensitive information or cause a denial of service condition.

22212 - (HT207940) Apple Boot Camp Wi-Fi Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-9417

Description

A remote code execution vulnerability is present in some versions of Apple Boot Camp.

Observation

Apple Boot Camp is a multi boot utility for OS X.

A remote code execution vulnerability is present in some versions of Apple Boot Camp. The flaw is related with a memory corruption issue. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22255 - Rockwell Automation MicroLogix 1100 Controllers DOS Vulnerability

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

Risk Level: High

CVE: CVE-2017-7924

Description

A vulnerability is present in some versions of Rockwell Automation MicroLogix.

Observation

Rockwell Automation MicroLogix is a system controller managed by a web server.

A vulnerability is present in some versions of Rockwell Automation MicroLogix. The flaw lies in the Rockwell Automation MicroLogix 1100. Successful exploitation could allow an attacker to cause denial-of-service condition.

22281 - (SB10206) McAfee ePolicy Orchestrator Multiple Apache Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-3169, CVE-2017-7668, CVE-2017-7679

Description

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator.

Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator. The flaws lie in the Apache component. Successful exploitation could allow an attacker to retrieve sensitive data or cause a denial-of-service condition on the target system.

22287 - Fuji Electric Monitouch V-SFT Multiple Vulnerabilities Prior To 5.4.43.0

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

Risk Level: High

CVE: CVE-2017-9659, CVE-2017-9660, CVE-2017-9662

Description

Multiple Vulnerabilities are present in some versions of the Fuji Electric Monitouch V-SFT.

Observation

Fuji Electric Monitouch V-SFT is a configuration software offering tools for easy viewing of HMI displays and graphic indication of system configuration.

Multiple Vulnerabilities are present in some versions of the Fuji Electric Monitouch V-SFT. The flaws lie in multiple components. Successful exploitation could allow an attacker to escalate privileges, or remotely execute arbitrary code on the target system.

22291 - Solar Controls WATTConfig M Software Uncontrolled Search Path Element Vulnerability

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

Risk Level: High

CVE: CVE-2017-9648

Description

A vulnerability is present in some versions of Solar Control WATTConfig M.

Observation

WATTConfig M is a configuration Software used for WATTrouter M which is a programmable controller based smart home energy management system.

A vulnerability is present in some versions of Solar Control WATTConfig M. The flaw is related to an uncontrolled search path element. Successful exploitation could allow an attacker to execute arbitrary code on the system.

22292 - (K45439210) F5 BIG-IP libxml2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-8710

Description

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

Observation

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

A denial-of-service vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in HTMLparser.c in libxml2. Successful exploitation could allow an attacker to obtain sensitive information or cause denial-of-service condition.

22298 - (K75429050) F5 BIG-IP Apache HTTPD Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-7679

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in Apache HTTPD Service. Successful exploitation could allow an attacker to cause denial of service condition.

22300 - (K83043359) F5 BIG-IP Apache HTTPD Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-3169

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in Apache HTTPD. Successful exploitation could allow an attacker to cause denial of service condition.

22304 - PostgreSQL Multiple Vulnerabilities (Aug 2017)

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Description

Multiple vulnerabilities are present in some versions of PostgreSQL.

Observation

PostgreSQL is an open-source object-relational database management system.

Multiple vulnerabilities are present in some versions of PostgreSQL. The flaws lie in the core server. Successful exploitation could allow an attacker to bypass security measure, disclose private information or cause a denial-of-service.

22306 - (K15412203) F5 BIG-IP Linux kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-1000365

Description

Multiple vulnerabilities are present in some versions of F5 BIG-IP products.

Observation

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

Multiple vulnerabilities are present in some versions of F5 BIG-IP products. The flaws lie in Linux kernel. Successful exploitation could allow an attacker to cause unauthorized disclosure of information and denial of service condition.

22315 - (K14445) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2013-2094

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to escalate privileges on the target system.

22318 - (K23030550) F5 BIG-IP Linux kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-8399

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to execute arbitrary code within the context of the kernel.

130858 - Debian Linux 8.0, 9.0 DSA-3948-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11721

Description

The scan detected that the host is missing the following update:
DSA-3948-1

Observation

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

http://www.debian.org/security/2017/dsa-3948

Debian 8.0

all
ioquake3_1.36+u20140802+gca9eebb-2+deb8u2

Debian 9.0
all
ioquake3_1.36+u20161101+dfsg1-2+deb9u1

130859 - Debian Linux 8.0, 9.0 DSA-3950-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6886, CVE-2017-6887

Description

The scan detected that the host is missing the following update:
DSA-3950-1

Observation

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

http://www.debian.org/security/2017/dsa-3950

Debian 8.0
all
libraw-dev_0.16.0-9+deb8u3
libraw-bin_0.16.0-9+deb8u3
libraw-doc_0.16.0-9+deb8u3
libraw10_0.16.0-9+deb8u3

Debian 9.0
all
libraw-doc_0.17.2-6+deb9u1
libraw-bin_0.17.2-6+deb9u1
libraw15_0.17.2-6+deb9u1
libraw-dev_0.17.2-6+deb9u1

141687 - Red Hat Enterprise Linux RHSA-2017-2486 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6814

Description

The scan detected that the host is missing the following update:
RHSA-2017-2486

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-August/msg00068.html

RHEL7D
noarch
groovy-javadoc-1.8.9-8.el7_4

groovy-1.8.9-8.el7_4

RHEL7S
noarch
groovy-javadoc-1.8.9-8.el7_4
groovy-1.8.9-8.el7_4

RHEL7WS
noarch
groovy-javadoc-1.8.9-8.el7_4
groovy-1.8.9-8.el7_4

141688 - Red Hat Enterprise Linux RHSA-2017-2485 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
RHSA-2017-2485

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-August/msg00067.html

RHEL6S
i386
git-debuginfo-1.7.1-9.el6_9
git-1.7.1-9.el6_9
git-daemon-1.7.1-9.el6_9

noarch
git-cvs-1.7.1-9.el6_9
git-svn-1.7.1-9.el6_9
git-email-1.7.1-9.el6_9
emacs-git-1.7.1-9.el6_9
emacs-git-el-1.7.1-9.el6_9
git-gui-1.7.1-9.el6_9
perl-Git-1.7.1-9.el6_9
git-all-1.7.1-9.el6_9
gitk-1.7.1-9.el6_9
gitweb-1.7.1-9.el6_9

x86_64
git-debuginfo-1.7.1-9.el6_9
git-1.7.1-9.el6_9
git-daemon-1.7.1-9.el6_9

RHEL6WS
i386
git-1.7.1-9.el6_9
git-debuginfo-1.7.1-9.el6_9

noarch
perl-Git-1.7.1-9.el6_9

x86_64
git-1.7.1-9.el6_9
git-debuginfo-1.7.1-9.el6_9

RHEL6D
i386
git-debuginfo-1.7.1-9.el6_9
git-daemon-1.7.1-9.el6_9
git-1.7.1-9.el6_9

noarch
git-cvs-1.7.1-9.el6_9
git-all-1.7.1-9.el6_9
git-svn-1.7.1-9.el6_9
emacs-git-1.7.1-9.el6_9
emacs-git-el-1.7.1-9.el6_9
git-gui-1.7.1-9.el6_9
perl-Git-1.7.1-9.el6_9
git-email-1.7.1-9.el6_9
gitk-1.7.1-9.el6_9
gitweb-1.7.1-9.el6_9

x86_64
git-debuginfo-1.7.1-9.el6_9
git-daemon-1.7.1-9.el6_9
git-1.7.1-9.el6_9

141689 - Red Hat Enterprise Linux RHSA-2017-2489 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000115, CVE-2017-1000116

Description

The scan detected that the host is missing the following update:
RHSA-2017-2489

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-August/msg00069.html

RHEL7D
x86_64
mercurial-hgk-2.6.2-8.el7_4
mercurial-2.6.2-8.el7_4
emacs-mercurial-2.6.2-8.el7_4
emacs-mercurial-el-2.6.2-8.el7_4
mercurial-debuginfo-2.6.2-8.el7_4

RHEL7S
x86_64
mercurial-hgk-2.6.2-8.el7_4
emacs-mercurial-2.6.2-8.el7_4
mercurial-2.6.2-8.el7_4
emacs-mercurial-el-2.6.2-8.el7_4
mercurial-debuginfo-2.6.2-8.el7_4

RHEL7WS
x86_64
mercurial-hgk-2.6.2-8.el7_4
emacs-mercurial-2.6.2-8.el7_4
mercurial-2.6.2-8.el7_4
emacs-mercurial-el-2.6.2-8.el7_4
mercurial-debuginfo-2.6.2-8.el7_4

141690 - Red Hat Enterprise Linux RHSA-2017-2484 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
RHSA-2017-2484

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-August/msg00066.html

RHEL7D
x86_64
git-svn-1.8.3.1-12.el7_4
git-1.8.3.1-12.el7_4
git-daemon-1.8.3.1-12.el7_4
git-debuginfo-1.8.3.1-12.el7_4

noarch
emacs-git-1.8.3.1-12.el7_4
git-hg-1.8.3.1-12.el7_4
emacs-git-el-1.8.3.1-12.el7_4
gitk-1.8.3.1-12.el7_4
git-p4-1.8.3.1-12.el7_4
git-bzr-1.8.3.1-12.el7_4
perl-Git-SVN-1.8.3.1-12.el7_4
git-gui-1.8.3.1-12.el7_4
git-email-1.8.3.1-12.el7_4
perl-Git-1.8.3.1-12.el7_4
git-all-1.8.3.1-12.el7_4
git-cvs-1.8.3.1-12.el7_4
gitweb-1.8.3.1-12.el7_4

RHEL7S
noarch
emacs-git-1.8.3.1-12.el7_4
git-hg-1.8.3.1-12.el7_4
emacs-git-el-1.8.3.1-12.el7_4
gitk-1.8.3.1-12.el7_4
git-p4-1.8.3.1-12.el7_4
git-bzr-1.8.3.1-12.el7_4
perl-Git-SVN-1.8.3.1-12.el7_4
git-gui-1.8.3.1-12.el7_4
git-email-1.8.3.1-12.el7_4

perl-Git-1.8.3.1-12.el7_4
git-all-1.8.3.1-12.el7_4
git-cvs-1.8.3.1-12.el7_4
gitweb-1.8.3.1-12.el7_4

x86_64
git-svn-1.8.3.1-12.el7_4
git-1.8.3.1-12.el7_4
git-daemon-1.8.3.1-12.el7_4
git-debuginfo-1.8.3.1-12.el7_4

RHEL7WS
x86_64
git-svn-1.8.3.1-12.el7_4
git-1.8.3.1-12.el7_4
git-daemon-1.8.3.1-12.el7_4
git-debuginfo-1.8.3.1-12.el7_4

noarch
emacs-git-1.8.3.1-12.el7_4
git-hg-1.8.3.1-12.el7_4
emacs-git-el-1.8.3.1-12.el7_4
gitk-1.8.3.1-12.el7_4
git-p4-1.8.3.1-12.el7_4
git-bzr-1.8.3.1-12.el7_4
perl-Git-SVN-1.8.3.1-12.el7_4
git-gui-1.8.3.1-12.el7_4
git-email-1.8.3.1-12.el7_4
perl-Git-1.8.3.1-12.el7_4
git-all-1.8.3.1-12.el7_4
git-cvs-1.8.3.1-12.el7_4
gitweb-1.8.3.1-12.el7_4

141692 - Red Hat Enterprise Linux RHSA-2017-2483 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3167, CVE-2017-3169, CVE-2017-7659, CVE-2017-7668, CVE-2017-7679, CVE-2017-9788

Description

The scan detected that the host is missing the following update:
RHSA-2017-2483

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-August/msg00065.html

RHEL6_7S
x86_64
httpd24-httpd-2.4.25-9.el6.1
httpd24-mod_session-2.4.25-9.el6.1
httpd24-mod_ldap-2.4.25-9.el6.1
httpd24-httpd-devel-2.4.25-9.el6.1
httpd24-mod_ssl-2.4.25-9.el6.1
httpd24-httpd-tools-2.4.25-9.el6.1
httpd24-mod_proxy_html-2.4.25-9.el6.1

httpd24-httpd-debuginfo-2.4.25-9.el6.1

noarch
httpd24-httpd-manual-2.4.25-9.el6.1

RHEL6S
x86_64
httpd24-httpd-2.4.25-9.el6.1
httpd24-mod_session-2.4.25-9.el6.1
httpd24-mod_ldap-2.4.25-9.el6.1
httpd24-httpd-devel-2.4.25-9.el6.1
httpd24-mod_ssl-2.4.25-9.el6.1
httpd24-httpd-tools-2.4.25-9.el6.1
httpd24-mod_proxy_html-2.4.25-9.el6.1
httpd24-httpd-debuginfo-2.4.25-9.el6.1

noarch
httpd24-httpd-manual-2.4.25-9.el6.1

RHEL6WS
x86_64
httpd24-httpd-2.4.25-9.el6.1
httpd24-mod_session-2.4.25-9.el6.1
httpd24-mod_ldap-2.4.25-9.el6.1
httpd24-httpd-devel-2.4.25-9.el6.1
httpd24-mod_ssl-2.4.25-9.el6.1
httpd24-httpd-tools-2.4.25-9.el6.1
httpd24-mod_proxy_html-2.4.25-9.el6.1
httpd24-httpd-debuginfo-2.4.25-9.el6.1

noarch
httpd24-httpd-manual-2.4.25-9.el6.1

RHEL7S
x86_64
httpd24-httpd-devel-2.4.25-9.el7.1
httpd24-mod_session-2.4.25-9.el7.1
httpd24-httpd-debuginfo-2.4.25-9.el7.1
httpd24-httpd-tools-2.4.25-9.el7.1
httpd24-mod_proxy_html-2.4.25-9.el7.1
httpd24-mod_ssl-2.4.25-9.el7.1
httpd24-mod_ldap-2.4.25-9.el7.1
httpd24-httpd-2.4.25-9.el7.1

noarch
httpd24-httpd-manual-2.4.25-9.el7.1

RHEL7WS
x86_64
httpd24-httpd-devel-2.4.25-9.el7.1
httpd24-mod_session-2.4.25-9.el7.1
httpd24-httpd-debuginfo-2.4.25-9.el7.1
httpd24-httpd-tools-2.4.25-9.el7.1
httpd24-mod_proxy_html-2.4.25-9.el7.1
httpd24-mod_ssl-2.4.25-9.el7.1
httpd24-mod_ldap-2.4.25-9.el7.1
httpd24-httpd-2.4.25-9.el7.1

noarch
httpd24-httpd-manual-2.4.25-9.el7.1

145485 - SuSE SLES 12 SP3 SUSE-SU-2017:2202-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10983, CVE-2017-10984, CVE-2017-10985, CVE-2017-10986, CVE-2017-10987, CVE-2017-10988

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2202-1

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-August/003144.html

SuSE SLES 12 SP3
x86_64
freeradius-server-python-3.0.15-2.3.1
freeradius-server-utils-3.0.15-2.3.1
freeradius-server-debugsource-3.0.15-2.3.1
freeradius-server-krb5-debuginfo-3.0.15-2.3.1
freeradius-server-ldap-debuginfo-3.0.15-2.3.1
freeradius-server-mysql-debuginfo-3.0.15-2.3.1
freeradius-server-perl-debuginfo-3.0.15-2.3.1
freeradius-server-python-debuginfo-3.0.15-2.3.1
freeradius-server-sqlite-debuginfo-3.0.15-2.3.1
freeradius-server-krb5-3.0.15-2.3.1
freeradius-server-3.0.15-2.3.1
freeradius-server-ldap-3.0.15-2.3.1
freeradius-server-perl-3.0.15-2.3.1
freeradius-server-libs-debuginfo-3.0.15-2.3.1
freeradius-server-mysql-3.0.15-2.3.1
freeradius-server-libs-3.0.15-2.3.1
freeradius-server-postgresql-debuginfo-3.0.15-2.3.1
freeradius-server-debuginfo-3.0.15-2.3.1
freeradius-server-sqlite-3.0.15-2.3.1
freeradius-server-postgresql-3.0.15-2.3.1
freeradius-server-doc-3.0.15-2.3.1
freeradius-server-utils-debuginfo-3.0.15-2.3.1

145489 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2174-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000100, CVE-2017-1000101

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2174-1

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-August/003138.html

SuSE SLES 12 SP2
x86_64
curl-debugsource-7.37.0-37.3.1
curl-debuginfo-7.37.0-37.3.1
libcurl4-32bit-7.37.0-37.3.1
curl-7.37.0-37.3.1
libcurl4-7.37.0-37.3.1
libcurl4-debuginfo-7.37.0-37.3.1
libcurl4-debuginfo-32bit-7.37.0-37.3.1

SuSE SLED 12 SP3
x86_64
curl-debugsource-7.37.0-37.3.1
curl-debuginfo-7.37.0-37.3.1
libcurl4-32bit-7.37.0-37.3.1
curl-7.37.0-37.3.1
libcurl4-7.37.0-37.3.1
libcurl4-debuginfo-7.37.0-37.3.1
libcurl4-debuginfo-32bit-7.37.0-37.3.1

SuSE SLED 12 SP2
x86_64
curl-debugsource-7.37.0-37.3.1
curl-debuginfo-7.37.0-37.3.1
libcurl4-32bit-7.37.0-37.3.1
curl-7.37.0-37.3.1
libcurl4-7.37.0-37.3.1
libcurl4-debuginfo-7.37.0-37.3.1
libcurl4-debuginfo-32bit-7.37.0-37.3.1

SuSE SLES 12 SP3
x86_64
curl-debugsource-7.37.0-37.3.1
curl-debuginfo-7.37.0-37.3.1
libcurl4-32bit-7.37.0-37.3.1
curl-7.37.0-37.3.1
libcurl4-7.37.0-37.3.1
libcurl4-debuginfo-7.37.0-37.3.1
libcurl4-debuginfo-32bit-7.37.0-37.3.1

145490 - SuSE SLED 12 SP2, 12 SP3 SUSE-SU-2017:2234-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2834, CVE-2017-2835, CVE-2017-2836, CVE-2017-2837, CVE-2017-2838, CVE-2017-2839

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2234-1

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-August/003149.html

SuSE SLED 12 SP3
x86_64
freerdp-2.0.0~git.1463131968.4e66df7-12.3.2
freerdp-debugsource-2.0.0~git.1463131968.4e66df7-12.3.2
libfreerdp2-2.0.0~git.1463131968.4e66df7-12.3.2
freerdp-debuginfo-2.0.0~git.1463131968.4e66df7-12.3.2
libfreerdp2-debuginfo-2.0.0~git.1463131968.4e66df7-12.3.2

SuSE SLED 12 SP2
x86_64
freerdp-2.0.0~git.1463131968.4e66df7-12.3.2
freerdp-debugsource-2.0.0~git.1463131968.4e66df7-12.3.2
libfreerdp2-2.0.0~git.1463131968.4e66df7-12.3.2
freerdp-debuginfo-2.0.0~git.1463131968.4e66df7-12.3.2
libfreerdp2-debuginfo-2.0.0~git.1463131968.4e66df7-12.3.2

145491 - SuSE SLES 11 SP4 SUSE-SU-2017:2235-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5276, CVE-2016-10196, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469, CVE-2017-5470, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7755, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7761, CVE-2017-7763, CVE-2017-7764, CVE-2017-7765, CVE-2017-7768, CVE-2017-7778

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2235-1

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-August/003150.html

SuSE SLES 11 SP4
i586
mozilla-nss-tools-3.29.5-47.3.2
libsoftokn3-3.29.5-47.3.2
MozillaFirefox-branding-SLED-52-24.3.44
MozillaFirefox-translations-52.2.0esr-72.5.2
MozillaFirefox-52.2.0esr-72.5.2
libfreebl3-3.29.5-47.3.2
firefox-libffi4-5.3.1+r233831-7.1
mozilla-nss-3.29.5-47.3.2
firefox-libstdc++6-5.3.1+r233831-7.1

x86_64
mozilla-nss-tools-3.29.5-47.3.2
mozilla-nss-32bit-3.29.5-47.3.2
libsoftokn3-3.29.5-47.3.2
MozillaFirefox-branding-SLED-52-24.3.44
MozillaFirefox-translations-52.2.0esr-72.5.2
MozillaFirefox-52.2.0esr-72.5.2
libsoftokn3-32bit-3.29.5-47.3.2

libfreebl3-3.29.5-47.3.2
libfreebl3-32bit-3.29.5-47.3.2
firefox-libffi4-5.3.1+r233831-7.1
mozilla-nss-3.29.5-47.3.2
firefox-libstdc++6-5.3.1+r233831-7.1

145494 - SuSE SLES 12 SP3 SUSE-SU-2017:2212-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9263, CVE-2017-9265

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2212-1

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-August/003145.html

SuSE SLES 12 SP3
x86_64
openvswitch-debugsource-2.7.0-3.3.1
openvswitch-debuginfo-2.7.0-3.3.1
openvswitch-2.7.0-3.3.1

160291 - CentOS 6 CESA-2017-2485 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2485

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-August/022519.html

CentOS 6
i686
git-daemon-1.7.1-9.el6_9
git-1.7.1-9.el6_9

noarch
git-cvs-1.7.1-9.el6_9
git-all-1.7.1-9.el6_9
git-svn-1.7.1-9.el6_9
emacs-git-1.7.1-9.el6_9
emacs-git-el-1.7.1-9.el6_9
git-gui-1.7.1-9.el6_9

perl-Git-1.7.1-9.el6_9
git-email-1.7.1-9.el6_9
gitk-1.7.1-9.el6_9
gitweb-1.7.1-9.el6_9

x86_64
git-daemon-1.7.1-9.el6_9
git-1.7.1-9.el6_9

163440 - Oracle Enterprise Linux ELSA-2017-2486 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6814

Description

The scan detected that the host is missing the following update:
ELSA-2017-2486

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-August/007137.html

OEL7
x86_64
groovy-javadoc-1.8.9-8.el7_4
groovy-1.8.9-8.el7_4

163441 - Oracle Enterprise Linux ELSA-2017-2489 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000115, CVE-2017-1000116

Description

The scan detected that the host is missing the following update:
ELSA-2017-2489

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-August/007138.html

OEL7
x86_64
mercurial-hgk-2.6.2-8.el7_4
mercurial-2.6.2-8.el7_4
emacs-mercurial-2.6.2-8.el7_4
emacs-mercurial-el-2.6.2-8.el7_4

163443 - Oracle Enterprise Linux ELSA-2017-2484 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
ELSA-2017-2484

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-August/007133.html

OEL7
x86_64
emacs-git-1.8.3.1-12.el7_4
git-hg-1.8.3.1-12.el7_4
emacs-git-el-1.8.3.1-12.el7_4
gitk-1.8.3.1-12.el7_4
git-p4-1.8.3.1-12.el7_4
git-daemon-1.8.3.1-12.el7_4
git-svn-1.8.3.1-12.el7_4
git-bzr-1.8.3.1-12.el7_4
perl-Git-SVN-1.8.3.1-12.el7_4
git-gui-1.8.3.1-12.el7_4
git-email-1.8.3.1-12.el7_4
perl-Git-1.8.3.1-12.el7_4
git-all-1.8.3.1-12.el7_4
git-1.8.3.1-12.el7_4
git-cvs-1.8.3.1-12.el7_4
gitweb-1.8.3.1-12.el7_4

163445 - Oracle Enterprise Linux ELSA-2017-2485 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
ELSA-2017-2485

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-August/007136.html

OEL6
x86_64
git-cvs-1.7.1-9.el6_9
git-svn-1.7.1-9.el6_9
git-email-1.7.1-9.el6_9
emacs-git-1.7.1-9.el6_9
git-daemon-1.7.1-9.el6_9

emacs-git-el-1.7.1-9.el6_9
git-gui-1.7.1-9.el6_9
perl-Git-1.7.1-9.el6_9
git-1.7.1-9.el6_9
git-all-1.7.1-9.el6_9
gitk-1.7.1-9.el6_9
gitweb-1.7.1-9.el6_9

i386
git-cvs-1.7.1-9.el6_9
git-svn-1.7.1-9.el6_9
git-email-1.7.1-9.el6_9
emacs-git-1.7.1-9.el6_9
git-daemon-1.7.1-9.el6_9
emacs-git-el-1.7.1-9.el6_9
git-gui-1.7.1-9.el6_9
perl-Git-1.7.1-9.el6_9
git-1.7.1-9.el6_9
git-all-1.7.1-9.el6_9
gitk-1.7.1-9.el6_9
gitweb-1.7.1-9.el6_9

170847 - Amazon Linux AMI ALAS-2017-872 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778

Description

The scan detected that the host is missing the following update:
ALAS-2017-872

Observation

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

https://alas.aws.amazon.com/ALAS-2017-872.html

Amazon Linux AMI
x86_64
graphite2-devel-1.3.10-1.7.amzn1
graphite2-debuginfo-1.3.10-1.7.amzn1
graphite2-1.3.10-1.7.amzn1

i686
graphite2-devel-1.3.10-1.7.amzn1
graphite2-debuginfo-1.3.10-1.7.amzn1
graphite2-1.3.10-1.7.amzn1

170849 - Amazon Linux AMI ALAS-2017-874 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12065, CVE-2017-12066

Description

The scan detected that the host is missing the following update:
ALAS-2017-874

Observation

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

https://alas.aws.amazon.com/ALAS-2017-874.html

Amazon Linux AMI
noarch
cacti-1.1.16-1.16.amzn1

170850 - Amazon Linux AMI ALAS-2017-870 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11473, CVE-2017-7533, CVE-2017-7542

Description

The scan detected that the host is missing the following update:
ALAS-2017-870

Observation

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

https://alas.aws.amazon.com/ALAS-2017-870.html

Amazon Linux AMI
i686
perf-debuginfo-4.9.43-17.38.amzn1
kernel-devel-4.9.43-17.38.amzn1
kernel-debuginfo-common-i686-4.9.43-17.38.amzn1
perf-4.9.43-17.38.amzn1
kernel-headers-4.9.43-17.38.amzn1
kernel-tools-devel-4.9.43-17.38.amzn1
kernel-tools-4.9.43-17.38.amzn1
kernel-4.9.43-17.38.amzn1
kernel-tools-debuginfo-4.9.43-17.38.amzn1
kernel-debuginfo-4.9.43-17.38.amzn1

noarch
kernel-doc-4.9.43-17.38.amzn1

x86_64
perf-debuginfo-4.9.43-17.38.amzn1
kernel-devel-4.9.43-17.38.amzn1
kernel-tools-4.9.43-17.38.amzn1
kernel-4.9.43-17.38.amzn1
perf-4.9.43-17.38.amzn1
kernel-debuginfo-common-x86_64-4.9.43-17.38.amzn1
kernel-headers-4.9.43-17.38.amzn1
kernel-tools-devel-4.9.43-17.38.amzn1
kernel-tools-debuginfo-4.9.43-17.38.amzn1
kernel-debuginfo-4.9.43-17.38.amzn1

170851 - Amazon Linux AMI ALAS-2017-871 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9224, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, CVE-2017-9229

Description

The scan detected that the host is missing the following update:
ALAS-2017-871

Observation

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

https://alas.aws.amazon.com/ALAS-2017-871.html

Amazon Linux AMI
x86_64
php56-mysqlnd-5.6.31-1.134.amzn1
php56-cli-5.6.31-1.134.amzn1
php56-pspell-5.6.31-1.134.amzn1
php56-debuginfo-5.6.31-1.134.amzn1
php56-process-5.6.31-1.134.amzn1
php56-intl-5.6.31-1.134.amzn1
php56-devel-5.6.31-1.134.amzn1
php56-xmlrpc-5.6.31-1.134.amzn1
php56-embedded-5.6.31-1.134.amzn1
php56-5.6.31-1.134.amzn1
php56-xml-5.6.31-1.134.amzn1
php56-dba-5.6.31-1.134.amzn1
php56-gd-5.6.31-1.134.amzn1
php56-fpm-5.6.31-1.134.amzn1
php56-snmp-5.6.31-1.134.amzn1
php56-ldap-5.6.31-1.134.amzn1
php56-pgsql-5.6.31-1.134.amzn1
php56-mcrypt-5.6.31-1.134.amzn1
php56-opcache-5.6.31-1.134.amzn1
php56-tidy-5.6.31-1.134.amzn1
php56-gmp-5.6.31-1.134.amzn1
php56-mbstring-5.6.31-1.134.amzn1
php56-pdo-5.6.31-1.134.amzn1
php56-recode-5.6.31-1.134.amzn1
php56-mssql-5.6.31-1.134.amzn1
php56-imap-5.6.31-1.134.amzn1
php56-enchant-5.6.31-1.134.amzn1
php56-odbc-5.6.31-1.134.amzn1
php56-bcmath-5.6.31-1.134.amzn1
php56-dbg-5.6.31-1.134.amzn1
php56-soap-5.6.31-1.134.amzn1
php56-common-5.6.31-1.134.amzn1

i686
php56-mysqlnd-5.6.31-1.134.amzn1
php56-cli-5.6.31-1.134.amzn1
php56-pspell-5.6.31-1.134.amzn1
php56-debuginfo-5.6.31-1.134.amzn1
php56-process-5.6.31-1.134.amzn1
php56-intl-5.6.31-1.134.amzn1
php56-devel-5.6.31-1.134.amzn1

php56-xmlrpc-5.6.31-1.134.amzn1
php56-embedded-5.6.31-1.134.amzn1
php56-5.6.31-1.134.amzn1
php56-xml-5.6.31-1.134.amzn1
php56-dba-5.6.31-1.134.amzn1
php56-gd-5.6.31-1.134.amzn1
php56-fpm-5.6.31-1.134.amzn1
php56-snmp-5.6.31-1.134.amzn1
php56-ldap-5.6.31-1.134.amzn1
php56-pgsql-5.6.31-1.134.amzn1
php56-mcrypt-5.6.31-1.134.amzn1
php56-opcache-5.6.31-1.134.amzn1
php56-tidy-5.6.31-1.134.amzn1
php56-gmp-5.6.31-1.134.amzn1
php56-mbstring-5.6.31-1.134.amzn1
php56-pdo-5.6.31-1.134.amzn1
php56-recode-5.6.31-1.134.amzn1
php56-mssql-5.6.31-1.134.amzn1
php56-imap-5.6.31-1.134.amzn1
php56-enchant-5.6.31-1.134.amzn1
php56-odbc-5.6.31-1.134.amzn1
php56-bcmath-5.6.31-1.134.amzn1
php56-dbg-5.6.31-1.134.amzn1
php56-soap-5.6.31-1.134.amzn1
php56-common-5.6.31-1.134.amzn1

175210 - Scientific Linux Security ERRATA Important: log4j on SL7.x (noarch) (1708-5404)

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

Risk Level: High

CVE: CVE-2017-5645

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: log4j on SL7.x (noarch) (1708-5404)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=5404

SL7
noarch
log4j-javadoc-1.2.17-16.el7_4
log4j-1.2.17-16.el7_4
log4j-manual-1.2.17-16.el7_4

175214 - Scientific Linux Security ERRATA Moderate: gdm and gnome-session on SL7.x x86_64 (1708-6394)

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

Risk Level: High

CVE: CVE-2015-7496

Description

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

Security ERRATA Moderate: gdm and gnome-session on SL7.x x86_64 (1708-6394)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=6394

SL7
x86_64
gnome-session-3.22.3-4.el7
gnome-session-xsession-3.22.3-4.el7
gdm-3.22.3-11.el7
gnome-session-debuginfo-3.22.3-4.el7
gdm-devel-3.22.3-11.el7
gnome-session-custom-session-3.22.3-4.el7
gdm-debuginfo-3.22.3-11.el7

175217 - Scientific Linux Security ERRATA Moderate: gnutls on SL7.x x86_64 (1708-10261)

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

Risk Level: High

CVE: CVE-2016-7444, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2017-7507, CVE-2017-7869

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: gnutls on SL7.x x86_64 (1708-10261)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=10261

SL7
x86_64
gnutls-3.3.26-9.el7
gnutls-devel-3.3.26-9.el7
gnutls-debuginfo-3.3.26-9.el7
gnutls-utils-3.3.26-9.el7
gnutls-c++-3.3.26-9.el7
gnutls-dane-3.3.26-9.el7

175222 - Scientific Linux Security ERRATA Moderate: X.org X11 libraries on SL7.x x86_64 (1708-11032)

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

Risk Level: High

CVE: CVE-2016-10164, CVE-2017-2625, CVE-2017-2626

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: X.org X11 libraries on SL7.x x86_64 (1708-11032)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=11032

SL7
x86_64
libXfixes-devel-5.0.3-1.el7
libinput-devel-1.6.3-2.el7
libvdpau-debuginfo-1.1.1-3.el7
mesa-vulkan-drivers-17.0.1-6.20170307.el7
drm-utils-2.4.74-1.el7
libxkbfile-debuginfo-1.0.9-3.el7
libXcursor-debuginfo-1.1.14-8.el7
libXxf86vm-debuginfo-1.1.4-1.el7
libvdpau-1.1.1-3.el7
libevdev-1.5.6-1.el7
libXpm-3.5.12-1.el7
libxkbcommon-debuginfo-0.7.1-1.el7
libXfont2-devel-2.0.1-2.el7
libXaw-1.0.13-4.el7
mesa-libGL-17.0.1-6.20170307.el7
libXt-1.1.5-3.el7
libxkbfile-devel-1.0.9-3.el7
libXrandr-debuginfo-1.5.1-2.el7
libXrender-devel-0.9.10-1.el7
mesa-libgbm-17.0.1-6.20170307.el7
libXvMC-devel-1.0.10-1.el7
libXpm-devel-3.5.12-1.el7
libXv-1.0.11-1.el7
libXfont-debuginfo-1.5.2-1.el7
mesa-libxatracker-devel-17.0.1-6.20170307.el7
libXfont2-debuginfo-2.0.1-2.el7
libXdmcp-debuginfo-1.1.2-6.el7
libXtst-devel-1.2.3-1.el7
libICE-devel-1.0.9-9.el7
libXi-1.7.9-1.el7
libvdpau-devel-1.1.1-3.el7
libXtst-debuginfo-1.2.3-1.el7
mesa-libGLES-17.0.1-6.20170307.el7
libXaw-debuginfo-1.0.13-4.el7
vulkan-1.0.39.1-2.el7
libXfont-devel-1.5.2-1.el7
mesa-libglapi-17.0.1-6.20170307.el7
libXv-devel-1.0.11-1.el7
libX11-devel-1.6.5-1.el7
libXvMC-1.0.10-1.el7
libXxf86vm-devel-1.1.4-1.el7
mesa-private-llvm-debuginfo-3.9.1-3.el7
libfontenc-devel-1.1.3-3.el7
libxkbfile-1.0.9-3.el7
libxkbcommon-x11-devel-0.7.1-1.el7
libxcb-1.12-1.el7
libXvMC-debuginfo-1.0.10-1.el7
libdrm-debuginfo-2.4.74-1.el7
mesa-libOSMesa-devel-17.0.1-6.20170307.el7
mesa-dri-drivers-17.0.1-6.20170307.el7
libXfixes-5.0.3-1.el7
libwacom-0.24-1.el7
mesa-libGLES-devel-17.0.1-6.20170307.el7
mesa-libxatracker-17.0.1-6.20170307.el7

vulkan-devel-1.0.39.1-2.el7
mesa-libgbm-devel-17.0.1-6.20170307.el7
libX11-debuginfo-1.6.5-1.el7
libevdev-debuginfo-1.5.6-1.el7
libXt-devel-1.1.5-3.el7
mesa-libGL-devel-17.0.1-6.20170307.el7
libepoxy-1.3.1-1.el7
mesa-libOSMesa-17.0.1-6.20170307.el7
mesa-filesystem-17.0.1-6.20170307.el7
libXrender-0.9.10-1.el7
mesa-debuginfo-17.0.1-6.20170307.el7
libxcb-devel-1.12-1.el7
libevdev-devel-1.5.6-1.el7
libxkbcommon-x11-0.7.1-1.el7
libdrm-2.4.74-1.el7
libX11-1.6.5-1.el7
libXfixes-debuginfo-5.0.3-1.el7
libwacom-devel-0.24-1.el7
libinput-debuginfo-1.6.3-2.el7
libXrender-debuginfo-0.9.10-1.el7
libXfont2-2.0.1-2.el7
libXaw-devel-1.0.13-4.el7
libICE-debuginfo-1.0.9-9.el7
libXdmcp-devel-1.1.2-6.el7
libepoxy-devel-1.3.1-1.el7
libICE-1.0.9-9.el7
libevdev-utils-1.5.6-1.el7
libXfont-1.5.2-1.el7
libxkbcommon-devel-0.7.1-1.el7
libXt-debuginfo-1.1.5-3.el7
libXxf86vm-1.1.4-1.el7
libXi-devel-1.7.9-1.el7
libxkbcommon-0.7.1-1.el7
libfontenc-debuginfo-1.1.3-3.el7
libXcursor-devel-1.1.14-8.el7
mesa-private-llvm-devel-3.9.1-3.el7
libXrandr-1.5.1-2.el7
libwacom-debuginfo-0.24-1.el7
libinput-1.6.3-2.el7
libfontenc-1.1.3-3.el7
libXpm-debuginfo-3.5.12-1.el7
libXcursor-1.1.14-8.el7
libXtst-1.2.3-1.el7
mesa-libEGL-17.0.1-6.20170307.el7
libXdmcp-1.1.2-6.el7
libXi-debuginfo-1.7.9-1.el7
vulkan-debuginfo-1.0.39.1-2.el7
libxcb-debuginfo-1.12-1.el7
libepoxy-debuginfo-1.3.1-1.el7
libdrm-devel-2.4.74-1.el7
libXrandr-devel-1.5.1-2.el7
mesa-libEGL-devel-17.0.1-6.20170307.el7
mesa-private-llvm-3.9.1-3.el7
libXv-debuginfo-1.0.11-1.el7

noarch
libX11-common-1.6.5-1.el7
libvdpau-docs-1.1.1-3.el7
xkeyboard-config-2.20-1.el7
libxcb-doc-1.12-1.el7

vulkan-filesystem-1.0.39.1-2.el7
xcb-proto-1.12-2.el7
libwacom-data-0.24-1.el7
xkeyboard-config-devel-2.20-1.el7
xorg-x11-proto-devel-7.7-20.el7

175223 - Scientific Linux Security ERRATA Important: httpd on SL7.x x86_64 (1708-5015)

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

Risk Level: High

CVE: CVE-2017-3167, CVE-2017-3169, CVE-2017-7668, CVE-2017-7679, CVE-2017-9788

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: httpd on SL7.x x86_64 (1708-5015)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=5015

SL7
x86_64
mod_session-2.4.6-67.el7_4.2
httpd-2.4.6-67.el7_4.2
httpd-devel-2.4.6-67.el7_4.2
mod_ssl-2.4.6-67.el7_4.2
mod_proxy_html-2.4.6-67.el7_4.2
httpd-debuginfo-2.4.6-67.el7_4.2
httpd-tools-2.4.6-67.el7_4.2
mod_ldap-2.4.6-67.el7_4.2

noarch
httpd-manual-2.4.6-67.el7_4.2

175224 - Scientific Linux Security ERRATA Important: evince on SL7.x x86_64 (1708-7506)

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

Risk Level: High

CVE: CVE-2017-1000083

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: evince on SL7.x x86_64 (1708-7506)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=7506

SL7
x86_64
evince-3.22.1-5.2.el7_4
evince-devel-3.22.1-5.2.el7_4

evince-debuginfo-3.22.1-5.2.el7_4
evince-dvi-3.22.1-5.2.el7_4
evince-libs-3.22.1-5.2.el7_4
evince-nautilus-3.22.1-5.2.el7_4
evince-browser-plugin-3.22.1-5.2.el7_4

175225 - Scientific Linux Security ERRATA Important: groovy on SL7.x (noarch) (1708-2472)

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

Risk Level: High

CVE: CVE-2016-6814

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: groovy on SL7.x (noarch) (1708-2472)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=2472

SL7
noarch
groovy-javadoc-1.8.9-8.el7_4
groovy-1.8.9-8.el7_4

175227 - Scientific Linux Security ERRATA Moderate: glibc on SL7.x x86_64 (1708-12511)

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

Risk Level: High

CVE: CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: glibc on SL7.x x86_64 (1708-12511)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=12511

SL7
x86_64
glibc-debuginfo-2.17-196.el7
nscd-2.17-196.el7
glibc-utils-2.17-196.el7
glibc-debuginfo-common-2.17-196.el7
glibc-devel-2.17-196.el7
glibc-headers-2.17-196.el7
glibc-2.17-196.el7
glibc-static-2.17-196.el7
glibc-common-2.17-196.el7

175230 - Scientific Linux Security ERRATA Moderate: bash on SL7.x x86_64 (1708-16992)

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

Risk Level: High

CVE: CVE-2016-0634, CVE-2016-7543, CVE-2016-9401

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: bash on SL7.x x86_64 (1708-16992)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=16992

SL7
x86_64
bash-4.2.46-28.el7
bash-doc-4.2.46-28.el7
bash-debuginfo-4.2.46-28.el7

175231 - Scientific Linux Security ERRATA Important: git on SL6.x i386/x86_64 (1708-1146)

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: git on SL6.x i386/x86_64 (1708-1146)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=1146

SL6
i386
git-debuginfo-1.7.1-9.el6_9
git-daemon-1.7.1-9.el6_9
git-1.7.1-9.el6_9

noarch
git-cvs-1.7.1-9.el6_9
git-all-1.7.1-9.el6_9
git-svn-1.7.1-9.el6_9
emacs-git-1.7.1-9.el6_9
emacs-git-el-1.7.1-9.el6_9
git-gui-1.7.1-9.el6_9
perl-Git-1.7.1-9.el6_9
git-email-1.7.1-9.el6_9
gitk-1.7.1-9.el6_9
gitweb-1.7.1-9.el6_9

x86_64
git-debuginfo-1.7.1-9.el6_9
git-daemon-1.7.1-9.el6_9
git-1.7.1-9.el6_9

175232 - Scientific Linux Security ERRATA Moderate: openssh on SL7.x x86_64 (1708-13263)

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

Risk Level: High

CVE: CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openssh on SL7.x x86_64 (1708-13263)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=13263

SL7
x86_64
openssh-debuginfo-7.4p1-11.el7
openssh-keycat-7.4p1-11.el7
openssh-clients-7.4p1-11.el7
openssh-server-7.4p1-11.el7
pam_ssh_agent_auth-0.10.3-1.11.el7
openssh-server-sysvinit-7.4p1-11.el7
openssh-ldap-7.4p1-11.el7
openssh-askpass-7.4p1-11.el7
openssh-7.4p1-11.el7
openssh-cavs-7.4p1-11.el7

175234 - Scientific Linux Security ERRATA Moderate: libreoffice on SL7.x x86_64 (1708-9157)

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

Risk Level: High

CVE: CVE-2017-7870

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libreoffice on SL7.x x86_64 (1708-9157)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=9157

SL7
x86_64
libreoffice-glade-5.0.6.2-14.el7
libreoffice-langpack-nso-5.0.6.2-14.el7
libreoffice-langpack-mai-5.0.6.2-14.el7
libreoffice-langpack-lv-5.0.6.2-14.el7

libreoffice-bsh-5.0.6.2-14.el7
libreoffice-langpack-nn-5.0.6.2-14.el7
libreoffice-5.0.6.2-14.el7
libreoffice-writer-5.0.6.2-14.el7
libreoffice-pdfimport-5.0.6.2-14.el7
libreoffice-ure-5.0.6.2-14.el7
libreoffice-langpack-tn-5.0.6.2-14.el7
libreoffice-langpack-fi-5.0.6.2-14.el7
libreoffice-langpack-fr-5.0.6.2-14.el7
libreoffice-langpack-lt-5.0.6.2-14.el7
libreoffice-langpack-da-5.0.6.2-14.el7
libreoffice-wiki-publisher-5.0.6.2-14.el7
libreoffice-langpack-en-5.0.6.2-14.el7
libreoffice-emailmerge-5.0.6.2-14.el7
libreoffice-langpack-pa-5.0.6.2-14.el7
libreoffice-calc-5.0.6.2-14.el7
libreoffice-langpack-ja-5.0.6.2-14.el7
libreoffice-langpack-ga-5.0.6.2-14.el7
libreoffice-langpack-sr-5.0.6.2-14.el7
libreoffice-impress-5.0.6.2-14.el7
libreoffice-langpack-te-5.0.6.2-14.el7
libreoffice-langpack-sl-5.0.6.2-14.el7
libreoffice-langpack-fa-5.0.6.2-14.el7
libreoffice-langpack-el-5.0.6.2-14.el7
libreoffice-langpack-pt-BR-5.0.6.2-14.el7
libreoffice-langpack-bg-5.0.6.2-14.el7
libreoffice-langpack-mr-5.0.6.2-14.el7
libreoffice-langpack-eu-5.0.6.2-14.el7
libreoffice-langpack-br-5.0.6.2-14.el7
libreoffice-langpack-et-5.0.6.2-14.el7
libreoffice-langpack-nl-5.0.6.2-14.el7
libreoffice-langpack-ve-5.0.6.2-14.el7
libreoffice-gdb-debug-support-5.0.6.2-14.el7
libreofficekit-5.0.6.2-14.el7
libreoffice-draw-5.0.6.2-14.el7
libreoffice-langpack-sk-5.0.6.2-14.el7
libreoffice-librelogo-5.0.6.2-14.el7
libreoffice-langpack-pl-5.0.6.2-14.el7
libreoffice-langpack-si-5.0.6.2-14.el7
libreoffice-langpack-kk-5.0.6.2-14.el7
libreoffice-graphicfilter-5.0.6.2-14.el7
libreoffice-langpack-it-5.0.6.2-14.el7
libreoffice-langpack-zu-5.0.6.2-14.el7
libreoffice-langpack-ss-5.0.6.2-14.el7
libreoffice-langpack-ko-5.0.6.2-14.el7
libreoffice-filters-5.0.6.2-14.el7
libreoffice-officebean-5.0.6.2-14.el7
libreoffice-langpack-af-5.0.6.2-14.el7
libreoffice-langpack-zh-Hans-5.0.6.2-14.el7
libreoffice-langpack-hu-5.0.6.2-14.el7
libreoffice-langpack-kn-5.0.6.2-14.el7
libreoffice-langpack-cy-5.0.6.2-14.el7
libreoffice-rhino-5.0.6.2-14.el7
libreofficekit-devel-5.0.6.2-14.el7
libreoffice-base-5.0.6.2-14.el7
libreoffice-postgresql-5.0.6.2-14.el7
libreoffice-langpack-he-5.0.6.2-14.el7
libreoffice-core-5.0.6.2-14.el7
libreoffice-debuginfo-5.0.6.2-14.el7
libreoffice-langpack-as-5.0.6.2-14.el7

libreoffice-langpack-xh-5.0.6.2-14.el7
libreoffice-pyuno-5.0.6.2-14.el7
libreoffice-langpack-ro-5.0.6.2-14.el7
libreoffice-langpack-de-5.0.6.2-14.el7
libreoffice-langpack-nr-5.0.6.2-14.el7
libreoffice-langpack-zh-Hant-5.0.6.2-14.el7
libreoffice-langpack-tr-5.0.6.2-14.el7
libreoffice-math-5.0.6.2-14.el7
libreoffice-langpack-ca-5.0.6.2-14.el7
libreoffice-langpack-gl-5.0.6.2-14.el7
libreoffice-xsltfilter-5.0.6.2-14.el7
libreoffice-ogltrans-5.0.6.2-14.el7
libreoffice-langpack-uk-5.0.6.2-14.el7
libreoffice-nlpsolver-5.0.6.2-14.el7
libreoffice-langpack-nb-5.0.6.2-14.el7
libreoffice-langpack-or-5.0.6.2-14.el7
libreoffice-langpack-th-5.0.6.2-14.el7
libreoffice-langpack-sv-5.0.6.2-14.el7
libreoffice-langpack-dz-5.0.6.2-14.el7
libreoffice-langpack-pt-PT-5.0.6.2-14.el7
libreoffice-langpack-ru-5.0.6.2-14.el7
libreoffice-langpack-bn-5.0.6.2-14.el7
libreoffice-langpack-gu-5.0.6.2-14.el7
libreoffice-langpack-ts-5.0.6.2-14.el7
libreoffice-langpack-hi-5.0.6.2-14.el7
libreoffice-langpack-hr-5.0.6.2-14.el7
libreoffice-langpack-ar-5.0.6.2-14.el7
libreoffice-langpack-ml-5.0.6.2-14.el7
libreoffice-langpack-cs-5.0.6.2-14.el7
libreoffice-langpack-es-5.0.6.2-14.el7
libreoffice-sdk-5.0.6.2-14.el7
libreoffice-langpack-st-5.0.6.2-14.el7
libreoffice-sdk-doc-5.0.6.2-14.el7
libreoffice-langpack-ta-5.0.6.2-14.el7

noarch
autocorr-zh-5.0.6.2-14.el7
autocorr-it-5.0.6.2-14.el7
autocorr-en-5.0.6.2-14.el7
autocorr-fa-5.0.6.2-14.el7
autocorr-sk-5.0.6.2-14.el7
autocorr-lb-5.0.6.2-14.el7
autocorr-af-5.0.6.2-14.el7
autocorr-lt-5.0.6.2-14.el7
autocorr-pt-5.0.6.2-14.el7
autocorr-hu-5.0.6.2-14.el7
autocorr-mn-5.0.6.2-14.el7
autocorr-sr-5.0.6.2-14.el7
autocorr-ga-5.0.6.2-14.el7
autocorr-sl-5.0.6.2-14.el7
autocorr-is-5.0.6.2-14.el7
autocorr-tr-5.0.6.2-14.el7
autocorr-ja-5.0.6.2-14.el7
autocorr-ro-5.0.6.2-14.el7
autocorr-hr-5.0.6.2-14.el7
autocorr-bg-5.0.6.2-14.el7
autocorr-ru-5.0.6.2-14.el7
autocorr-da-5.0.6.2-14.el7
autocorr-sv-5.0.6.2-14.el7
autocorr-pl-5.0.6.2-14.el7

autocorr-es-5.0.6.2-14.el7
autocorr-vi-5.0.6.2-14.el7
autocorr-nl-5.0.6.2-14.el7
autocorr-fr-5.0.6.2-14.el7
autocorr-cs-5.0.6.2-14.el7
autocorr-ko-5.0.6.2-14.el7
autocorr-ca-5.0.6.2-14.el7
libreoffice-opensymbol-fonts-5.0.6.2-14.el7
autocorr-fi-5.0.6.2-14.el7
autocorr-de-5.0.6.2-14.el7

175235 - Scientific Linux Security ERRATA Moderate: gtk-vnc on SL7.x x86_64 (1708-13678)

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

Risk Level: High

CVE: CVE-2017-5884, CVE-2017-5885

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: gtk-vnc on SL7.x x86_64 (1708-13678)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=13678

SL7
x86_64
gtk-vnc2-0.7.0-2.el7
gtk-vnc-python-0.7.0-2.el7
gvnc-tools-0.7.0-2.el7
gvnc-devel-0.7.0-2.el7
gtk-vnc2-devel-0.7.0-2.el7
gtk-vnc-devel-0.7.0-2.el7
gtk-vnc-0.7.0-2.el7
gtk-vnc-debuginfo-0.7.0-2.el7
gvncpulse-0.7.0-2.el7
gvnc-0.7.0-2.el7
gvncpulse-devel-0.7.0-2.el7

175238 - Scientific Linux Security ERRATA Important: mercurial on SL7.x x86_64 (1708-2119)

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

Risk Level: High

CVE: CVE-2017-1000115, CVE-2017-1000116

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: mercurial on SL7.x x86_64 (1708-2119)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=2119

SL7
x86_64
mercurial-hgk-2.6.2-8.el7_4
mercurial-2.6.2-8.el7_4
emacs-mercurial-2.6.2-8.el7_4
emacs-mercurial-el-2.6.2-8.el7_4
mercurial-debuginfo-2.6.2-8.el7_4

175239 - Scientific Linux Security ERRATA Low: samba on SL7.x x86_64 (1708-12926)

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

Risk Level: High

CVE: CVE-2017-9461

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: samba on SL7.x x86_64 (1708-12926)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=12926

SL7
x86_64
samba-test-libs-4.6.2-8.el7
samba-test-4.6.2-8.el7
samba-4.6.2-8.el7
samba-vfs-glusterfs-4.6.2-8.el7
samba-winbind-krb5-locator-4.6.2-8.el7
samba-python-4.6.2-8.el7
samba-client-libs-4.6.2-8.el7
libwbclient-4.6.2-8.el7
samba-winbind-4.6.2-8.el7
libsmbclient-devel-4.6.2-8.el7
libwbclient-devel-4.6.2-8.el7
samba-client-4.6.2-8.el7
samba-dc-libs-4.6.2-8.el7
samba-dc-4.6.2-8.el7
samba-devel-4.6.2-8.el7
samba-libs-4.6.2-8.el7
samba-krb5-printing-4.6.2-8.el7
samba-common-libs-4.6.2-8.el7
samba-winbind-clients-4.6.2-8.el7
samba-debuginfo-4.6.2-8.el7
libsmbclient-4.6.2-8.el7
samba-common-tools-4.6.2-8.el7
samba-winbind-modules-4.6.2-8.el7

noarch
samba-pidl-4.6.2-8.el7
samba-common-4.6.2-8.el7

175241 - Scientific Linux Security ERRATA Moderate: curl on SL7.x x86_64 (1708-11786)

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

Risk Level: High

CVE: CVE-2016-7167

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: curl on SL7.x x86_64 (1708-11786)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=11786

SL7
x86_64
libcurl-7.29.0-42.el7
libcurl-devel-7.29.0-42.el7
curl-debuginfo-7.29.0-42.el7
curl-7.29.0-42.el7

175242 - Scientific Linux Security ERRATA Moderate: NetworkManager and libnl3 on SL7.x x86_64 (1708-9503)

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

Risk Level: High

CVE: CVE-2017-0553

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: NetworkManager and libnl3 on SL7.x x86_64 (1708-9503)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=9503

SL7
x86_64
libnl3-doc-3.2.28-4.el7
NetworkManager-bluetooth-1.8.0-9.el7
NetworkManager-glib-1.8.0-9.el7
libnm-gtk-1.8.0-3.el7
NetworkManager-tui-1.8.0-9.el7
NetworkManager-libnm-devel-1.8.0-9.el7
NetworkManager-libnm-1.8.0-9.el7
NetworkManager-wwan-1.8.0-9.el7
NetworkManager-team-1.8.0-9.el7
libnl3-devel-3.2.28-4.el7
NetworkManager-libreswan-1.2.4-2.el7
libnl3-debuginfo-3.2.28-4.el7
network-manager-applet-1.8.0-3.el7
NetworkManager-glib-devel-1.8.0-9.el7
libnl3-cli-3.2.28-4.el7
NetworkManager-libreswan-gnome-1.2.4-2.el7
libnma-1.8.0-3.el7
NetworkManager-debuginfo-1.8.0-9.el7

NetworkManager-libreswan-debuginfo-1.2.4-2.el7
NetworkManager-adsl-1.8.0-9.el7
NetworkManager-1.8.0-9.el7
libnma-devel-1.8.0-3.el7
nm-connection-editor-1.8.0-3.el7
libnm-gtk-devel-1.8.0-3.el7
network-manager-applet-debuginfo-1.8.0-3.el7
NetworkManager-ppp-1.8.0-9.el7
libnl3-3.2.28-4.el7
NetworkManager-wifi-1.8.0-9.el7

noarch
NetworkManager-dispatcher-routing-rules-1.8.0-9.el7
NetworkManager-config-server-1.8.0-9.el7

175243 - Scientific Linux Security ERRATA Moderate: tcpdump on SL7.x x86_64 (1708-9866)

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

Risk Level: High

CVE: CVE-2015-0261, CVE-2015-2153, CVE-2015-2154, CVE-2015-2155, CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5341, CVE-2017-5342, CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: tcpdump on SL7.x x86_64 (1708-9866)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=9866

SL7
x86_64
tcpdump-debuginfo-4.9.0-5.el7
tcpdump-4.9.0-5.el7

175244 - Scientific Linux Security ERRATA Important: git on SL7.x x86_64 (1708-1798)

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: git on SL7.x x86_64 (1708-1798)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=1798

SL7
x86_64
git-svn-1.8.3.1-12.el7_4
git-1.8.3.1-12.el7_4
git-daemon-1.8.3.1-12.el7_4
git-debuginfo-1.8.3.1-12.el7_4

noarch
emacs-git-1.8.3.1-12.el7_4
git-hg-1.8.3.1-12.el7_4
emacs-git-el-1.8.3.1-12.el7_4
gitk-1.8.3.1-12.el7_4
git-p4-1.8.3.1-12.el7_4
git-bzr-1.8.3.1-12.el7_4
perl-Git-SVN-1.8.3.1-12.el7_4
git-gui-1.8.3.1-12.el7_4
git-email-1.8.3.1-12.el7_4
perl-Git-1.8.3.1-12.el7_4
git-all-1.8.3.1-12.el7_4
git-cvs-1.8.3.1-12.el7_4
gitweb-1.8.3.1-12.el7_4

175245 - Scientific Linux Security ERRATA Important: freeradius on SL7.x x86_64 (1708-7083)

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10983, CVE-2017-10984, CVE-2017-10985, CVE-2017-10986, CVE-2017-10987

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: freeradius on SL7.x x86_64 (1708-7083)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=7083

SL7
x86_64
freeradius-3.0.13-8.el7_4
freeradius-krb5-3.0.13-8.el7_4
freeradius-devel-3.0.13-8.el7_4
freeradius-mysql-3.0.13-8.el7_4
freeradius-doc-3.0.13-8.el7_4
freeradius-postgresql-3.0.13-8.el7_4
freeradius-sqlite-3.0.13-8.el7_4
freeradius-debuginfo-3.0.13-8.el7_4
freeradius-ldap-3.0.13-8.el7_4
freeradius-perl-3.0.13-8.el7_4
freeradius-utils-3.0.13-8.el7_4
freeradius-unixODBC-3.0.13-8.el7_4
freeradius-python-3.0.13-8.el7_4

175247 - Scientific Linux Security ERRATA Important: libsoup on SL7.x x86_64 (1708-4353)

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

Risk Level: High

CVE: CVE-2017-2885

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libsoup on SL7.x x86_64 (1708-4353)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=4353

SL7
x86_64
libsoup-debuginfo-2.56.0-4.el7_4
libsoup-devel-2.56.0-4.el7_4
libsoup-2.56.0-4.el7_4

175248 - Scientific Linux Security ERRATA Important: subversion on SL7.x x86_64 (1708-2798)

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

Risk Level: High

CVE: CVE-2017-9800

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: subversion on SL7.x x86_64 (1708-2798)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=2798

SL7
x86_64
mod_dav_svn-1.7.14-11.el7_4
subversion-javahl-1.7.14-11.el7_4
subversion-python-1.7.14-11.el7_4
subversion-ruby-1.7.14-11.el7_4
subversion-kde-1.7.14-11.el7_4
subversion-libs-1.7.14-11.el7_4
subversion-debuginfo-1.7.14-11.el7_4
subversion-gnome-1.7.14-11.el7_4
subversion-devel-1.7.14-11.el7_4
subversion-1.7.14-11.el7_4
subversion-tools-1.7.14-11.el7_4
subversion-perl-1.7.14-11.el7_4

178482 - Gentoo Linux GLSA-201708-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6307, CVE-2017-6308, CVE-2017-6309, CVE-2017-6310, CVE-2017-8911

Description

The scan detected that the host is missing the following update:
GLSA-201708-02

Observation

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

https://security.gentoo.org/glsa/201708-02

Affected packages:
net-mail/tnef < 1.4.15

185841 - Ubuntu Linux 14.04 USN-3392-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000365, CVE-2017-10810, CVE-2017-7482, CVE-2017-7533

Description

The scan detected that the host is missing the following update:
USN-3392-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004009.html

Ubuntu 14.04

linux-image-powerpc64-smp-lts-xenial_4.4.0.92.76
linux-image-powerpc-smp-lts-xenial_4.4.0.92.76
linux-image-4.4.0-92-powerpc-smp_4.4.0-92.115~14.04.1
linux-image-generic-lts-xenial_4.4.0.92.76
linux-image-4.4.0-92-powerpc64-smp_4.4.0-92.115~14.04.1
linux-image-powerpc64-emb-lts-xenial_4.4.0.92.76
linux-image-generic-lpae-lts-xenial_4.4.0.92.76
linux-image-4.4.0-92-generic_4.4.0-92.115~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.92.76
linux-image-4.4.0-92-powerpc-e500mc_4.4.0-92.115~14.04.1
linux-image-4.4.0-92-powerpc64-emb_4.4.0-92.115~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.92.76
linux-image-4.4.0-92-generic-lpae_4.4.0-92.115~14.04.1
linux-image-4.4.0-92-lowlatency_4.4.0-92.115~14.04.1

185844 - Ubuntu Linux 16.04 USN-3392-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000365, CVE-2017-10810, CVE-2017-7482, CVE-2017-7533

Description

The scan detected that the host is missing the following update:
USN-3392-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004008.html

Ubuntu 16.04

linux-image-4.4.0-92-powerpc64-smp_4.4.0-92.115
linux-image-aws_4.4.0.1031.33
linux-image-4.4.0-92-powerpc-e500mc_4.4.0-92.115
linux-image-4.4.0-92-lowlatency_4.4.0-92.115
linux-image-4.4.0-92-powerpc64-emb_4.4.0-92.115
linux-image-4.4.0-1027-gke_4.4.0-1027.27
linux-image-4.4.0-92-generic_4.4.0-92.115
linux-image-4.4.0-1031-aws_4.4.0-1031.40
linux-image-powerpc-smp_4.4.0.92.97
linux-image-4.4.0-1072-snapdragon_4.4.0-1072.77
linux-image-4.4.0-92-powerpc-smp_4.4.0-92.115
linux-image-powerpc64-emb_4.4.0.92.97
linux-image-gke_4.4.0.1027.28
linux-image-powerpc-e500mc_4.4.0.92.97
linux-image-raspi2_4.4.0.1070.70
linux-image-generic-lpae_4.4.0.92.97
linux-image-snapdragon_4.4.0.1072.64
linux-image-powerpc64-smp_4.4.0.92.97
linux-image-lowlatency_4.4.0.92.97
linux-image-generic_4.4.0.92.97
linux-image-4.4.0-92-generic-lpae_4.4.0-92.115
linux-image-4.4.0-1070-raspi2_4.4.0-1070.78

185845 - Ubuntu Linux 14.04, 16.04 USN-3401-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10243

Description

The scan detected that the host is missing the following update:
USN-3401-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004022.html

Ubuntu 14.04

texlive-latex-base_2013.20140215-1ubuntu0.1
texlive-base_2013.20140215-1ubuntu0.1

Ubuntu 16.04

texlive-latex-base_2015.20160320-1ubuntu0.1
texlive-base_2015.20160320-1ubuntu0.1

192552 - Fedora Linux 26 FEDORA-2017-f9e66916ec Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f9e66916ec

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/2017/8/?count=200&page=1

Fedora Core 26

mingw-postgresql-9.6.4-1.fc26

192555 - Fedora Linux 26 FEDORA-2017-dd0d5d376f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2810

Description

The scan detected that the host is missing the following update:
FEDORA-2017-dd0d5d376f

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/2017/8/?count=200&page=1

Fedora Core 26

python-tablib-0.11.5-1.fc26

192557 - Fedora Linux 25 FEDORA-2017-a1fe6d2b86 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10686, CVE-2017-11111

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a1fe6d2b86

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/2017/8/?count=200&page=2

Fedora Core 25

nasm-2.13.01-3.fc25

192564 - Fedora Linux 25 FEDORA-2017-fe04b06b64 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2810

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fe04b06b64

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/2017/8/?count=200&page=1

Fedora Core 25

python-tablib-0.11.5-1.fc25

192568 - Fedora Linux 26 FEDORA-2017-6186f95179 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10686, CVE-2017-11111

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6186f95179

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/2017/8/?count=200&page=2

Fedora Core 26

nasm-2.13.01-3.fc26

22274 - Cisco NX-OS OSPF LSA Manipulation Vulnerability (CSCve47401)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-6770

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 lies in the OSPF Protocol Link State Advertisement (LSA) database. Successful exploitation could allow an attacker to bypass security restrictions and take control of the OSPF AS domain routing table.

22284 - SIMPlight SCADA Software DLL Hijacking Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-9661

Description

A DLL hijacking vulnerability is present in some versions of SIMPlight SCADA Software.

Observation

SIMPlight SCADA Software is a HMI/SCADA software used to create robust HMI screens to control machine, process.

A DLL hijacking vulnerability is present in some versions of SIMPlight SCADA Software. The flaw is related to an uncontrolled search path element. Successful exploitation could allow an attacker to execute arbitrary code on the system.

22299 - Moxa SoftNVR-IA Live Viewer Uncontrolled Search Path Element Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-5170

Description

A DLL hijacking vulnerability is present in some versions of Moxa SoftNVR-IA Live Viewer.

Observation

Moxa SoftNVR-IA Live Viewer is an IP surveillance software.

A DLL hijacking vulnerability is present in some versions of Moxa SoftNVR-IA Live Viewer. The flaw is related to an uncontrolled search path element. Successful exploitation could allow an attacker to execute arbitrary code on the system.

22303 - Apache Tomcat Multiple Vulnerabilities Prior To 8.5.16

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

Risk Level: Medium

CVE: CVE-2017-7674, CVE-2017-7675

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is a container for the Java Servlet and Java Server Pages Web applications.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in the HTTP/2 implementation and in the CORS

filter. Successful exploitation could allow an attacker to bypass security constraints or permit client or server cache poisoning.

22310 - (K47284724) F5 BIG-IP iControl Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-9256

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in iControl component. Successful exploitation could allow an attacker to bypass security access restrictions.

130856 - Debian Linux 8.0, 9.0 DSA-3946-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11423, CVE-2017-6419

Description

The scan detected that the host is missing the following update:
DSA-3946-1

Observation

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

http://www.debian.org/security/2017/dsa-3946

Debian 8.0
all
libmspack-dev_0.5-1+deb8u1
libmspack-dbg_0.5-1+deb8u1
libmspack0_0.5-1+deb8u1
libmspack-doc_0.5-1+deb8u1

Debian 9.0
all
libmspack-dev_0.5-1+deb9u1
libmspack-doc_0.5-1+deb9u1
libmspack-dbg_0.5-1+deb9u1
libmspack0_0.5-1+deb9u1

132391 - Oracle VM OVMSA-2017-0144 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10200, CVE-2016-9604, CVE-2016-9685, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0144

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000758.html

OVM3.3
x86_64
kernel-uek-firmware-3.8.13-118.19.4.el6uek
kernel-uek-3.8.13-118.19.4.el6uek

132392 - Oracle VM OVMSA-2017-0143 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10200, CVE-2016-6213, CVE-2016-9604, CVE-2017-7533, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0143

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000757.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-94.5.9.el6uek
kernel-uek-4.1.12-94.5.9.el6uek

141691 - Red Hat Enterprise Linux RHSA-2017-2491 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000117, CVE-2017-8386

Description

The scan detected that the host is missing the following update:
RHSA-2017-2491

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-August/msg00070.html

RHEL6S
x86_64
rh-git29-git-daemon-2.9.3-3.el6
rh-git29-git-svn-2.9.3-3.el6

rh-git29-git-debuginfo-2.9.3-3.el6
rh-git29-git-2.9.3-3.el6
rh-git29-git-core-2.9.3-3.el6
rh-git29-git-core-doc-2.9.3-3.el6

noarch
rh-git29-git-gui-2.9.3-3.el6
rh-git29-perl-Git-SVN-2.9.3-3.el6
rh-git29-emacs-git-el-2.9.3-3.el6
rh-git29-perl-Git-2.9.3-3.el6
rh-git29-gitk-2.9.3-3.el6
rh-git29-gitweb-2.9.3-3.el6
rh-git29-git-all-2.9.3-3.el6
rh-git29-git-p4-2.9.3-3.el6
rh-git29-git-cvs-2.9.3-3.el6
rh-git29-emacs-git-2.9.3-3.el6
rh-git29-git-email-2.9.3-3.el6

RHEL6WS
x86_64
rh-git29-git-daemon-2.9.3-3.el6
rh-git29-git-svn-2.9.3-3.el6
rh-git29-git-debuginfo-2.9.3-3.el6
rh-git29-git-2.9.3-3.el6
rh-git29-git-core-2.9.3-3.el6
rh-git29-git-core-doc-2.9.3-3.el6

noarch
rh-git29-git-gui-2.9.3-3.el6
rh-git29-perl-Git-SVN-2.9.3-3.el6
rh-git29-emacs-git-el-2.9.3-3.el6
rh-git29-perl-Git-2.9.3-3.el6
rh-git29-gitk-2.9.3-3.el6
rh-git29-gitweb-2.9.3-3.el6
rh-git29-git-all-2.9.3-3.el6
rh-git29-git-p4-2.9.3-3.el6
rh-git29-git-cvs-2.9.3-3.el6
rh-git29-emacs-git-2.9.3-3.el6
rh-git29-git-email-2.9.3-3.el6

RHEL7S
x86_64
rh-git29-git-daemon-2.9.3-3.el7
rh-git29-git-2.9.3-3.el7
rh-git29-git-debuginfo-2.9.3-3.el7
rh-git29-git-core-2.9.3-3.el7
rh-git29-git-svn-2.9.3-3.el7
rh-git29-git-core-doc-2.9.3-3.el7

noarch
rh-git29-git-email-2.9.3-3.el7
rh-git29-perl-Git-SVN-2.9.3-3.el7
rh-git29-perl-Git-2.9.3-3.el7
rh-git29-git-all-2.9.3-3.el7
rh-git29-gitk-2.9.3-3.el7
rh-git29-git-gui-2.9.3-3.el7
rh-git29-git-p4-2.9.3-3.el7
rh-git29-gitweb-2.9.3-3.el7
rh-git29-git-cvs-2.9.3-3.el7

RHEL7WS
x86_64
rh-git29-git-daemon-2.9.3-3.el7
rh-git29-git-2.9.3-3.el7
rh-git29-git-debuginfo-2.9.3-3.el7
rh-git29-git-core-2.9.3-3.el7
rh-git29-git-svn-2.9.3-3.el7
rh-git29-git-core-doc-2.9.3-3.el7

noarch
rh-git29-git-email-2.9.3-3.el7
rh-git29-perl-Git-SVN-2.9.3-3.el7
rh-git29-perl-Git-2.9.3-3.el7
rh-git29-git-all-2.9.3-3.el7
rh-git29-gitk-2.9.3-3.el7
rh-git29-git-gui-2.9.3-3.el7
rh-git29-git-p4-2.9.3-3.el7
rh-git29-gitweb-2.9.3-3.el7
rh-git29-git-cvs-2.9.3-3.el7

145484 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2217-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8288

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2217-1

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-August/003146.html

SuSE SLED 12 SP2
x86_64
gnome-shell-browser-plugin-3.20.4-77.7.5
gnome-shell-browser-plugin-debuginfo-3.20.4-77.7.5
gnome-shell-debuginfo-3.20.4-77.7.5
gnome-shell-calendar-debuginfo-3.20.4-77.7.5
gnome-shell-debugsource-3.20.4-77.7.5
gnome-shell-calendar-3.20.4-77.7.5
gnome-shell-3.20.4-77.7.5

noarch
gnome-shell-lang-3.20.4-77.7.5

SuSE SLES 12 SP3
noarch
gnome-shell-lang-3.20.4-77.7.5

x86_64
gnome-shell-debuginfo-3.20.4-77.7.5
gnome-shell-browser-plugin-debuginfo-3.20.4-77.7.5
gnome-shell-debugsource-3.20.4-77.7.5
gnome-shell-browser-plugin-3.20.4-77.7.5

gnome-shell-3.20.4-77.7.5

SuSE SLES 12 SP2
noarch
gnome-shell-lang-3.20.4-77.7.5

x86_64
gnome-shell-debuginfo-3.20.4-77.7.5
gnome-shell-browser-plugin-debuginfo-3.20.4-77.7.5
gnome-shell-debugsource-3.20.4-77.7.5
gnome-shell-browser-plugin-3.20.4-77.7.5
gnome-shell-3.20.4-77.7.5

SuSE SLED 12 SP3
x86_64
gnome-shell-browser-plugin-3.20.4-77.7.5
gnome-shell-browser-plugin-debuginfo-3.20.4-77.7.5
gnome-shell-debuginfo-3.20.4-77.7.5
gnome-shell-calendar-debuginfo-3.20.4-77.7.5
gnome-shell-debugsource-3.20.4-77.7.5
gnome-shell-calendar-3.20.4-77.7.5
gnome-shell-3.20.4-77.7.5

noarch
gnome-shell-lang-3.20.4-77.7.5

145486 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2199-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11403, CVE-2017-9439, CVE-2017-9440, CVE-2017-9501

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2199-1

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-August/003141.html

SuSE SLED 12 SP2
x86_64
ImageMagick-debuginfo-6.8.8.1-71.5.3
libMagickWand-6_Q16-1-6.8.8.1-71.5.3
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.5.3
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.5.3
ImageMagick-debugsource-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-6.8.8.1-71.5.3
libMagick++-6_Q16-3-6.8.8.1-71.5.3
ImageMagick-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.5.3

SuSE SLES 12 SP3
x86_64

ImageMagick-debuginfo-6.8.8.1-71.5.3
libMagickWand-6_Q16-1-6.8.8.1-71.5.3
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.5.3
ImageMagick-debugsource-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.5.3

SuSE SLES 12 SP2
x86_64
ImageMagick-debuginfo-6.8.8.1-71.5.3
libMagickWand-6_Q16-1-6.8.8.1-71.5.3
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.5.3
ImageMagick-debugsource-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.5.3

SuSE SLED 12 SP3
x86_64
ImageMagick-debuginfo-6.8.8.1-71.5.3
libMagickWand-6_Q16-1-6.8.8.1-71.5.3
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.5.3
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.5.3
ImageMagick-debugsource-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-6.8.8.1-71.5.3
libMagick++-6_Q16-3-6.8.8.1-71.5.3
ImageMagick-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.5.3
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.5.3

145488 - SuSE SLES 11 SP4 SUSE-SU-2017:2176-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11403, CVE-2017-9439, CVE-2017-9501

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2176-1

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-August/003140.html

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.78.5.2

x86_64
libMagickCore1-32bit-6.4.3.6-7.78.5.2
libMagickCore1-6.4.3.6-7.78.5.2

145492 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2237-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11103

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2237-1

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-August/003152.html

SuSE SLED 12 SP3
x86_64
libsmbclient0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-krb5pac0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-client-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbconf0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-standard0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libnetapi0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libtevent-util0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamdb0-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-client-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libwbclient0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-standard0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-errors0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-nbt0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-credentials0-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbldap0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbconf0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-errors0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-standard0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-hostconfig0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-krb5pac0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libtevent-util0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-libs-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-standard0-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr0-4.6.7+git.38.90b2cdb4f22-3.7.1
libnetapi0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libwbclient0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-hostconfig0-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-client-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-credentials0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamdb0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbclient0-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-passdb0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-libs-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-libs-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-client-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-winbind-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-hostconfig0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbldap0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1

libdcerpc-binding0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-errors0-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-krb5pac0-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbclient0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-credentials0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libwbclient0-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-passdb0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-passdb0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libnetapi0-4.6.7+git.38.90b2cdb4f22-3.7.1
libwbclient0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbconf0-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc-binding0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-errors0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc-binding0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-winbind-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbclient0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-krb5pac0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbldap0-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-nbt0-4.6.7+git.38.90b2cdb4f22-3.7.1
libtevent-util0-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc0-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamdb0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamdb0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-passdb0-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbldap0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-nbt0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libtevent-util0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbconf0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-util0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-winbind-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-hostconfig0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-credentials0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libnetapi0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-util0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-util0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc-binding0-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-nbt0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-util0-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-libs-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-debugsource-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-winbind-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1

noarch
samba-doc-4.6.7+git.38.90b2cdb4f22-3.7.1

SuSE SLES 12 SP3
noarch
samba-doc-4.6.7+git.38.90b2cdb4f22-3.7.1

x86_64
libsmbclient0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-krb5pac0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-client-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbconf0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-standard0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libnetapi0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libtevent-util0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamdb0-4.6.7+git.38.90b2cdb4f22-3.7.1

samba-client-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libwbclient0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-standard0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-errors0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-nbt0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-credentials0-4.6.7+git.38.90b2cdb4f22-3.7.1
libdcerpc0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-util0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbconf0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-errors0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-standard0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-hostconfig0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr-krb5pac0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libtevent-util0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-libs-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libndr0-4.6.7+git.38.90b2cdb4f22-3.7.1
libnetapi0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-hostconfig0-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-winbind-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-credentials0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamdb0-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
libsmbclient0-4.6.7+git.38.90b2cdb4f22-3.7.1
libsamba-passdb0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-libs-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-libs-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-client-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1
samba-winbind-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.7.1

145493 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2175-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10078, 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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2175-1

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-August/003139.html

SuSE SLES 12 SP2
x86_64
java-1_8_0-openjdk-demo-1.8.0.144-27.5.3
java-1_8_0-openjdk-debugsource-1.8.0.144-27.5.3
java-1_8_0-openjdk-demo-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-devel-1.8.0.144-27.5.3

java-1_8_0-openjdk-headless-1.8.0.144-27.5.3
java-1_8_0-openjdk-headless-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-devel-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-1.8.0.144-27.5.3

SuSE SLED 12 SP3
x86_64
java-1_8_0-openjdk-headless-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-debugsource-1.8.0.144-27.5.3
java-1_8_0-openjdk-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-headless-1.8.0.144-27.5.3
java-1_8_0-openjdk-1.8.0.144-27.5.3

SuSE SLED 12 SP2
x86_64
java-1_8_0-openjdk-headless-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-debugsource-1.8.0.144-27.5.3
java-1_8_0-openjdk-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-headless-1.8.0.144-27.5.3
java-1_8_0-openjdk-1.8.0.144-27.5.3

SuSE SLES 12 SP3
x86_64
java-1_8_0-openjdk-demo-1.8.0.144-27.5.3
java-1_8_0-openjdk-debugsource-1.8.0.144-27.5.3
java-1_8_0-openjdk-demo-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-devel-1.8.0.144-27.5.3
java-1_8_0-openjdk-headless-1.8.0.144-27.5.3
java-1_8_0-openjdk-headless-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-devel-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-debuginfo-1.8.0.144-27.5.3
java-1_8_0-openjdk-1.8.0.144-27.5.3

163439 - Oracle Enterprise Linux ELSA-2017-3606 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10200, CVE-2016-9604, CVE-2016-9685, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
ELSA-2017-3606

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-August/007143.html
http://oss.oracle.com/pipermail/el-errata/2017-August/007144.html

OEL7
x86_64
kernel-uek-debug-3.8.13-118.19.4.el7uek
kernel-uek-3.8.13-118.19.4.el7uek
kernel-uek-devel-3.8.13-118.19.4.el7uek
kernel-uek-doc-3.8.13-118.19.4.el7uek
kernel-uek-firmware-3.8.13-118.19.4.el7uek

dtrace-modules-3.8.13-118.19.4.el7uek-0.4.5-3.el7
kernel-uek-debug-devel-3.8.13-118.19.4.el7uek

OEL6
x86_64
kernel-uek-debug-devel-3.8.13-118.19.4.el6uek
kernel-uek-devel-3.8.13-118.19.4.el6uek
kernel-uek-firmware-3.8.13-118.19.4.el6uek
kernel-uek-3.8.13-118.19.4.el6uek
kernel-uek-doc-3.8.13-118.19.4.el6uek
kernel-uek-debug-3.8.13-118.19.4.el6uek
dtrace-modules-3.8.13-118.19.4.el6uek-0.4.5-3.el6

163442 - Oracle Enterprise Linux ELSA-2017-3607 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10200, CVE-2016-9604, CVE-2016-9685, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
ELSA-2017-3607

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-August/007145.html

OEL6
x86_64
kernel-uek-debug-devel-2.6.39-400.297.6.el6uek
kernel-uek-doc-2.6.39-400.297.6.el6uek
kernel-uek-devel-2.6.39-400.297.6.el6uek
kernel-uek-2.6.39-400.297.6.el6uek
kernel-uek-debug-2.6.39-400.297.6.el6uek
kernel-uek-firmware-2.6.39-400.297.6.el6uek

i386
kernel-uek-debug-devel-2.6.39-400.297.6.el6uek
kernel-uek-doc-2.6.39-400.297.6.el6uek
kernel-uek-devel-2.6.39-400.297.6.el6uek
kernel-uek-2.6.39-400.297.6.el6uek
kernel-uek-debug-2.6.39-400.297.6.el6uek
kernel-uek-firmware-2.6.39-400.297.6.el6uek

163444 - Oracle Enterprise Linux ELSA-2017-3605 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10200, CVE-2016-6213, CVE-2016-9604, CVE-2017-7533, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
ELSA-2017-3605

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-August/007134.html
http://oss.oracle.com/pipermail/el-errata/2017-August/007135.html

OEL7
x86_64
kernel-uek-debug-devel-4.1.12-94.5.9.el7uek
kernel-uek-devel-4.1.12-94.5.9.el7uek
kernel-uek-debug-4.1.12-94.5.9.el7uek
kernel-uek-doc-4.1.12-94.5.9.el7uek
dtrace-modules-4.1.12-94.5.9.el7uek-0.6.0-4.el7
kernel-uek-firmware-4.1.12-94.5.9.el7uek
kernel-uek-4.1.12-94.5.9.el7uek

OEL6
x86_64
kernel-uek-doc-4.1.12-94.5.9.el6uek
kernel-uek-devel-4.1.12-94.5.9.el6uek
kernel-uek-4.1.12-94.5.9.el6uek
dtrace-modules-4.1.12-94.5.9.el6uek-0.6.0-4.el6
kernel-uek-debug-devel-4.1.12-94.5.9.el6uek
kernel-uek-firmware-4.1.12-94.5.9.el6uek
kernel-uek-debug-4.1.12-94.5.9.el6uek

170848 - Amazon Linux AMI ALAS-2017-873 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5648, CVE-2017-5664

Description

The scan detected that the host is missing the following update:
ALAS-2017-873

Observation

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

https://alas.aws.amazon.com/ALAS-2017-873.html

Amazon Linux AMI
noarch
tomcat7-jsp-2.2-api-7.0.79-1.28.amzn1
tomcat7-javadoc-7.0.79-1.28.amzn1
tomcat7-lib-7.0.79-1.28.amzn1
tomcat7-el-2.2-api-7.0.79-1.28.amzn1
tomcat7-7.0.79-1.28.amzn1
tomcat7-admin-webapps-7.0.79-1.28.amzn1
tomcat7-servlet-3.0-api-7.0.79-1.28.amzn1
tomcat7-docs-webapp-7.0.79-1.28.amzn1
tomcat7-log4j-7.0.79-1.28.amzn1
tomcat7-webapps-7.0.79-1.28.amzn1

175213 - Scientific Linux Security ERRATA Important: spice on SL7.x x86_64 (1708-4031)

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

Risk Level: Medium

CVE: CVE-2017-7506

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: spice on SL7.x x86_64 (1708-4031)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=4031

SL7
x86_64
spice-debuginfo-0.12.8-2.el7.1
spice-server-devel-0.12.8-2.el7.1
spice-server-0.12.8-2.el7.1

175219 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1708-4679)

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

Risk Level: Medium

CVE: CVE-2017-7533

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1708-4679)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=4679

SL7
x86_64
kernel-devel-3.10.0-693.1.1.el7
kernel-tools-libs-devel-3.10.0-693.1.1.el7
perf-3.10.0-693.1.1.el7
kernel-headers-3.10.0-693.1.1.el7
python-perf-3.10.0-693.1.1.el7
kernel-debug-3.10.0-693.1.1.el7
kernel-debug-debuginfo-3.10.0-693.1.1.el7
kernel-debug-devel-3.10.0-693.1.1.el7
kernel-tools-3.10.0-693.1.1.el7
kernel-3.10.0-693.1.1.el7
perf-debuginfo-3.10.0-693.1.1.el7
kernel-tools-libs-3.10.0-693.1.1.el7
kernel-debuginfo-common-x86_64-3.10.0-693.1.1.el7
python-perf-debuginfo-3.10.0-693.1.1.el7
kernel-debuginfo-3.10.0-693.1.1.el7
kernel-tools-debuginfo-3.10.0-693.1.1.el7

noarch

kernel-abi-whitelists-3.10.0-693.1.1.el7
kernel-doc-3.10.0-693.1.1.el7

175220 - Scientific Linux Security ERRATA Moderate: mariadb on SL7.x x86_64 (1708-14039)

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

Risk Level: Medium

CVE: CVE-2016-5483, CVE-2016-5617, CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3600

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: mariadb on SL7.x x86_64 (1708-14039)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=14039

SL7
x86_64
mariadb-5.5.56-2.el7
mariadb-test-5.5.56-2.el7
mariadb-debuginfo-5.5.56-2.el7
mariadb-bench-5.5.56-2.el7
mariadb-embedded-devel-5.5.56-2.el7
mariadb-embedded-5.5.56-2.el7
mariadb-devel-5.5.56-2.el7
mariadb-server-5.5.56-2.el7
mariadb-libs-5.5.56-2.el7

175226 - Scientific Linux Security ERRATA Moderate: git on SL7.x x86_64 (1708-18176)

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

Risk Level: Medium

CVE: CVE-2014-9938, CVE-2017-8386

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: git on SL7.x x86_64 (1708-18176)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=18176

SL7
x86_64
git-svn-1.8.3.1-11.el7
git-debuginfo-1.8.3.1-11.el7
git-daemon-1.8.3.1-11.el7
git-1.8.3.1-11.el7

noarch
git-bzr-1.8.3.1-11.el7
git-gui-1.8.3.1-11.el7
git-cvs-1.8.3.1-11.el7
git-p4-1.8.3.1-11.el7
git-email-1.8.3.1-11.el7
gitk-1.8.3.1-11.el7
perl-Git-SVN-1.8.3.1-11.el7
git-all-1.8.3.1-11.el7
emacs-git-el-1.8.3.1-11.el7
gitweb-1.8.3.1-11.el7
emacs-git-1.8.3.1-11.el7
git-hg-1.8.3.1-11.el7
perl-Git-1.8.3.1-11.el7

175228 - Scientific Linux Security ERRATA Critical: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1708-5728)

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10081, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10115, CVE-2017-10116, CVE-2017-10135, CVE-2017-10243

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1708-5728)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=5728

SL7
x86_64
java-1.7.0-openjdk-accessibility-1.7.0.151-2.6.11.1.el7_4
java-1.7.0-openjdk-devel-1.7.0.151-2.6.11.1.el7_4
java-1.7.0-openjdk-debuginfo-1.7.0.151-2.6.11.1.el7_4
java-1.7.0-openjdk-headless-1.7.0.151-2.6.11.1.el7_4
java-1.7.0-openjdk-src-1.7.0.151-2.6.11.1.el7_4
java-1.7.0-openjdk-demo-1.7.0.151-2.6.11.1.el7_4
java-1.7.0-openjdk-1.7.0.151-2.6.11.1.el7_4

noarch
java-1.7.0-openjdk-javadoc-1.7.0.151-2.6.11.1.el7_4

SL6
i386
java-1.7.0-openjdk-src-1.7.0.151-2.6.11.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.151-2.6.11.0.el6_9
java-1.7.0-openjdk-1.7.0.151-2.6.11.0.el6_9
java-1.7.0-openjdk-devel-1.7.0.151-2.6.11.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.151-2.6.11.0.el6_9

noarch
java-1.7.0-openjdk-javadoc-1.7.0.151-2.6.11.0.el6_9

x86_64

java-1.7.0-openjdk-src-1.7.0.151-2.6.11.0.el6_9
java-1.7.0-openjdk-debuginfo-1.7.0.151-2.6.11.0.el6_9
java-1.7.0-openjdk-1.7.0.151-2.6.11.0.el6_9
java-1.7.0-openjdk-devel-1.7.0.151-2.6.11.0.el6_9
java-1.7.0-openjdk-demo-1.7.0.151-2.6.11.0.el6_9

175249 - Scientific Linux Security ERRATA Moderate: tigervnc and fltk on SL7.x x86_64 (1708-17357)

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

Risk Level: Medium

CVE: CVE-2016-10207, CVE-2017-5581, CVE-2017-7392, CVE-2017-7393, CVE-2017-7394, CVE-2017-7395, CVE-2017-7396

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: tigervnc and fltk on SL7.x x86_64 (1708-17357)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=17357

SL7
x86_64
fltk-static-1.3.4-1.el7
tigervnc-server-minimal-1.8.0-1.el7
tigervnc-debuginfo-1.8.0-1.el7
fltk-fluid-1.3.4-1.el7
fltk-devel-1.3.4-1.el7
tigervnc-server-module-1.8.0-1.el7
tigervnc-1.8.0-1.el7
fltk-1.3.4-1.el7
fltk-debuginfo-1.3.4-1.el7
tigervnc-server-1.8.0-1.el7

noarch
tigervnc-icons-1.8.0-1.el7
tigervnc-server-applet-1.8.0-1.el7
tigervnc-license-1.8.0-1.el7

175251 - Scientific Linux Security ERRATA Moderate: pidgin on SL7.x x86_64 (1708-16582)

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

Risk Level: Medium

CVE: CVE-2014-3694, CVE-2014-3695, CVE-2014-3696, CVE-2014-3698, CVE-2017-2640

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: pidgin on SL7.x x86_64 (1708-16582)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=16582

SL7
x86_64
pidgin-debuginfo-2.10.11-5.el7
pidgin-devel-2.10.11-5.el7
libpurple-devel-2.10.11-5.el7
libpurple-perl-2.10.11-5.el7
pidgin-perl-2.10.11-5.el7
libpurple-2.10.11-5.el7
pidgin-2.10.11-5.el7
finch-devel-2.10.11-5.el7
finch-2.10.11-5.el7
libpurple-tcl-2.10.11-5.el7

178486 - Gentoo Linux GLSA-201708-06 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10219, CVE-2016-10220, CVE-2017-5951, CVE-2017-6196, CVE-2017-7207, CVE-2017-8291

Description

The scan detected that the host is missing the following update:
GLSA-201708-06

Observation

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

https://security.gentoo.org/glsa/201708-06

Affected packages:
app-text/ghostscript-gpl < 9.21

182426 - FreeBSD Zabbix Remote Code Execution (5df8bd95-8290-11e7-93af-005056925db4)

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

Risk Level: Medium

CVE: CVE-2017-2824

Description

The scan detected that the host is missing the following update:
Zabbix -- Remote code execution (5df8bd95-8290-11e7-93af-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/5df8bd95-8290-11e7-93af-005056925db4.html

Affected packages:
zabbix2-server <= 2.0.20
zabbix2-proxy <= 2.0.20
zabbix22-server < 2.2.19
zabbix22-proxy < 2.2.19
zabbix3-server < 3.0.10
zabbix3-proxy < 3.0.10
zabbix32-server < 3.2.7

zabbix32-proxy < 3.2.7

185846 - Ubuntu Linux 16.04, 17.04 USN-3394-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11423, CVE-2017-6419

Description

The scan detected that the host is missing the following update:
USN-3394-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004012.html

Ubuntu 17.04

libmspack0_0.5-1ubuntu0.17.04.1

Ubuntu 16.04

libmspack0_0.5-1ubuntu0.16.04.1

185849 - Ubuntu Linux 12.04 USN-3393-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6418, CVE-2017-6419, CVE-2017-6420

Description

The scan detected that the host is missing the following update:
USN-3393-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004015.html

Ubuntu 12.04

clamav_0.99.2+addedllvm-0ubuntu0.12.04.2

185850 - Ubuntu Linux 14.04 USN-3396-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10081, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10115, CVE-2017-10116, CVE-2017-10118, CVE-2017-10135, CVE-2017-10176, CVE-2017-10243

Description

The scan detected that the host is missing the following update:
USN-3396-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004017.html

Ubuntu 14.04

openjdk-7-jre-lib_7u151-2.6.11-0ubuntu1.14.04.1
openjdk-7-jre_7u151-2.6.11-0ubuntu1.14.04.1
icedtea-7-jre-jamvm_7u151-2.6.11-0ubuntu1.14.04.1
openjdk-7-jre-headless_7u151-2.6.11-0ubuntu1.14.04.1
openjdk-7-jre-zero_7u151-2.6.11-0ubuntu1.14.04.1

185852 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3393-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6418, CVE-2017-6419, CVE-2017-6420

Description

The scan detected that the host is missing the following update:
USN-3393-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004011.html

Ubuntu 16.04

clamav_0.99.2+dfsg-0ubuntu0.16.04.2

Ubuntu 14.04

clamav_0.99.2+addedllvm-0ubuntu0.14.04.2

Ubuntu 17.04

clamav_0.99.2+dfsg-6ubuntu0.1

22305 - (K57211290) F5 BIG-IP IPv6 Fragmentation Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-10142

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the IPv6 protocol specification. Successful exploitation could allow an attacker to cause a denial of service condition.

141693 - Red Hat Enterprise Linux RHSA-2017-2492 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000061

Description

The scan detected that the host is missing the following update:
RHSA-2017-2492

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-August/msg00071.html

RHEL7D
x86_64
xmlsec1-nss-devel-1.2.20-7.el7_4
xmlsec1-1.2.20-7.el7_4
xmlsec1-openssl-1.2.20-7.el7_4
xmlsec1-gnutls-1.2.20-7.el7_4
xmlsec1-debuginfo-1.2.20-7.el7_4
xmlsec1-nss-1.2.20-7.el7_4
xmlsec1-gcrypt-1.2.20-7.el7_4
xmlsec1-gcrypt-devel-1.2.20-7.el7_4
xmlsec1-openssl-devel-1.2.20-7.el7_4
xmlsec1-devel-1.2.20-7.el7_4
xmlsec1-gnutls-devel-1.2.20-7.el7_4

RHEL7S
x86_64
xmlsec1-nss-devel-1.2.20-7.el7_4
xmlsec1-1.2.20-7.el7_4
xmlsec1-openssl-1.2.20-7.el7_4
xmlsec1-gnutls-1.2.20-7.el7_4
xmlsec1-debuginfo-1.2.20-7.el7_4
xmlsec1-nss-1.2.20-7.el7_4
xmlsec1-gcrypt-1.2.20-7.el7_4
xmlsec1-gcrypt-devel-1.2.20-7.el7_4
xmlsec1-openssl-devel-1.2.20-7.el7_4
xmlsec1-devel-1.2.20-7.el7_4
xmlsec1-gnutls-devel-1.2.20-7.el7_4

RHEL7WS
x86_64
xmlsec1-nss-devel-1.2.20-7.el7_4
xmlsec1-1.2.20-7.el7_4
xmlsec1-openssl-1.2.20-7.el7_4
xmlsec1-gnutls-1.2.20-7.el7_4
xmlsec1-debuginfo-1.2.20-7.el7_4
xmlsec1-nss-1.2.20-7.el7_4

xmlsec1-gcrypt-1.2.20-7.el7_4
xmlsec1-gcrypt-devel-1.2.20-7.el7_4
xmlsec1-openssl-devel-1.2.20-7.el7_4
xmlsec1-devel-1.2.20-7.el7_4
xmlsec1-gnutls-devel-1.2.20-7.el7_4

163446 - Oracle Enterprise Linux ELSA-2017-2492 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000061

Description

The scan detected that the host is missing the following update:
ELSA-2017-2492

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-August/007149.html

OEL7
x86_64
xmlsec1-nss-devel-1.2.20-7.el7_4
xmlsec1-1.2.20-7.el7_4
xmlsec1-openssl-1.2.20-7.el7_4
xmlsec1-gnutls-1.2.20-7.el7_4
xmlsec1-nss-1.2.20-7.el7_4
xmlsec1-gcrypt-1.2.20-7.el7_4
xmlsec1-gcrypt-devel-1.2.20-7.el7_4
xmlsec1-openssl-devel-1.2.20-7.el7_4
xmlsec1-devel-1.2.20-7.el7_4
xmlsec1-gnutls-devel-1.2.20-7.el7_4

175215 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1708-3130)

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

Risk Level: Medium

CVE: CVE-2017-10664

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1708-3130)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=3130

SL7
x86_64
qemu-img-1.5.3-141.el7_4.1
qemu-kvm-common-1.5.3-141.el7_4.1
qemu-kvm-1.5.3-141.el7_4.1

qemu-kvm-debuginfo-1.5.3-141.el7_4.1
qemu-kvm-tools-1.5.3-141.el7_4.1

175216 - Scientific Linux Security ERRATA Moderate: GStreamer on SL7.x x86_64 (1708-7833)

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

Risk Level: Medium

CVE: CVE-2016-10198, CVE-2016-10199, CVE-2016-9446, CVE-2016-9810, CVE-2016-9811, CVE-2017-5837, CVE-2017-5838, CVE-2017-5839, CVE-2017-5840, CVE-2017-5841, CVE-2017-5842, CVE-2017-5843, CVE-2017-5844, CVE-2017-5845, CVE-2017-5848

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: GStreamer on SL7.x x86_64 (1708-7833)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=7833

SL7
x86_64
gstreamer-plugins-bad-free-devel-0.10.23-23.el7
gstreamer-plugins-bad-free-0.10.23-23.el7
gstreamer1-plugins-base-tools-1.10.4-1.el7
clutter-gst2-devel-2.0.18-1.el7
gstreamer1-plugins-base-1.10.4-1.el7
gstreamer1-plugins-bad-free-gtk-1.10.4-2.el7
gstreamer1-devel-1.10.4-2.el7
gstreamer1-plugins-bad-free-1.10.4-2.el7
gstreamer1-plugins-good-1.10.4-2.el7
gstreamer-plugins-good-0.10.31-13.el7
orc-compiler-0.4.26-1.el7
gstreamer1-plugins-bad-free-debuginfo-1.10.4-2.el7
orc-debuginfo-0.4.26-1.el7
gstreamer1-debuginfo-1.10.4-2.el7
gstreamer1-plugins-good-debuginfo-1.10.4-2.el7
gstreamer1-plugins-base-devel-1.10.4-1.el7
gstreamer1-plugins-bad-free-devel-1.10.4-2.el7
gstreamer1-plugins-base-debuginfo-1.10.4-1.el7
gstreamer-plugins-bad-free-devel-docs-0.10.23-23.el7
clutter-gst2-2.0.18-1.el7
orc-0.4.26-1.el7
clutter-gst2-debuginfo-2.0.18-1.el7
gstreamer1-1.10.4-2.el7
gstreamer-plugins-bad-free-debuginfo-0.10.23-23.el7
orc-devel-0.4.26-1.el7
gstreamer-plugins-good-debuginfo-0.10.31-13.el7

noarch
orc-doc-0.4.26-1.el7
gstreamer1-devel-docs-1.10.4-2.el7
gstreamer1-plugins-base-devel-docs-1.10.4-1.el7
gstreamer-plugins-good-devel-docs-0.10.31-13.el7
gnome-video-effects-0.4.3-1.el7

175229 - Scientific Linux Security ERRATA Moderate: xmlsec1 on SL7.x x86_64 (1708-1471)

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

Risk Level: Medium

CVE: CVE-2017-1000061

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: xmlsec1 on SL7.x x86_64 (1708-1471)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=1471

SL7
x86_64
xmlsec1-nss-devel-1.2.20-7.el7_4
xmlsec1-1.2.20-7.el7_4
xmlsec1-openssl-1.2.20-7.el7_4
xmlsec1-gnutls-1.2.20-7.el7_4
xmlsec1-debuginfo-1.2.20-7.el7_4
xmlsec1-nss-1.2.20-7.el7_4
xmlsec1-gcrypt-1.2.20-7.el7_4
xmlsec1-gcrypt-devel-1.2.20-7.el7_4
xmlsec1-openssl-devel-1.2.20-7.el7_4
xmlsec1-devel-1.2.20-7.el7_4
xmlsec1-gnutls-devel-1.2.20-7.el7_4

175237 - Scientific Linux Security ERRATA Moderate: python on SL7.x x86_64 (1708-15573)

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

Risk Level: Medium

CVE: CVE-2014-9365

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: python on SL7.x x86_64 (1708-15573)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=15573

SL7
x86_64
python-2.7.5-58.el7
python-tools-2.7.5-58.el7
python-devel-2.7.5-58.el7
python-debuginfo-2.7.5-58.el7
python-test-2.7.5-58.el7
python-debug-2.7.5-58.el7
tkinter-2.7.5-58.el7
python-libs-2.7.5-58.el7

175246 - Scientific Linux Security ERRATA Moderate: pki-core on SL7.x x86_64 (1708-10705)

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

Risk Level: Medium

CVE: CVE-2017-7537

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: pki-core on SL7.x x86_64 (1708-10705)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=10705

SL7
x86_64
pki-tools-10.4.1-11.el7
pki-symkey-10.4.1-11.el7
pki-core-debuginfo-10.4.1-11.el7

noarch
pki-javadoc-10.4.1-11.el7
pki-server-10.4.1-11.el7
pki-base-java-10.4.1-11.el7
pki-base-10.4.1-11.el7
pki-ca-10.4.1-11.el7
pki-kra-10.4.1-11.el7

175250 - Scientific Linux Security ERRATA Moderate: postgresql on SL7.x x86_64 (1708-17812)

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

Risk Level: Medium

CVE: CVE-2017-7484, CVE-2017-7486

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: postgresql on SL7.x x86_64 (1708-17812)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=17812

SL7
x86_64
postgresql-plpython-9.2.21-1.el7
postgresql-contrib-9.2.21-1.el7
postgresql-9.2.21-1.el7
postgresql-pltcl-9.2.21-1.el7
postgresql-plperl-9.2.21-1.el7
postgresql-libs-9.2.21-1.el7
postgresql-test-9.2.21-1.el7
postgresql-docs-9.2.21-1.el7

postgresql-devel-9.2.21-1.el7
postgresql-debuginfo-9.2.21-1.el7
postgresql-server-9.2.21-1.el7
postgresql-static-9.2.21-1.el7
postgresql-upgrade-9.2.21-1.el7

178480 - Gentoo Linux GLSA-201708-07 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201708-07

Observation

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

https://security.gentoo.org/glsa/201708-07

Affected packages:
x11-terms/evilvte < 0.5.1

178481 - Gentoo Linux GLSA-201708-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2016-9778, CVE-2017-3135, CVE-2017-3136, CVE-2017-3137, CVE-2017-3138, CVE-2017-3140, CVE-2017-3141

Description

The scan detected that the host is missing the following update:
GLSA-201708-01

Observation

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

https://security.gentoo.org/glsa/201708-01

Affected packages:
net-dns/bind < 9.11.1_p1

178485 - Gentoo Linux GLSA-201708-04 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8296

Description

The scan detected that the host is missing the following update:
GLSA-201708-04

Observation

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

https://security.gentoo.org/glsa/201708-04

Affected packages:
app-admin/kedpm < 0.4.0-r2

182422 - FreeBSD pspp Multiple Vulnerabilities (6876b163-8708-11e7-8568-e8e0b747a45a)

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

Risk Level: Medium

CVE: CVE-2017-10791, CVE-2017-10792, CVE-2017-12958, CVE-2017-12959, CVE-2017-12960, CVE-2017-12961

Description

The scan detected that the host is missing the following update:
pspp -- multiple vulnerabilities (6876b163-8708-11e7-8568-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/6876b163-8708-11e7-8568-e8e0b747a45a.html

Affected packages:
pspp < 1.0.0

185853 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3395-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000381

Description

The scan detected that the host is missing the following update:
USN-3395-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004013.html

Ubuntu 16.04

libc-ares2_1.10.0-3ubuntu0.2

Ubuntu 14.04

libc-ares2_1.10.0-2ubuntu0.2

Ubuntu 17.04

libc-ares2_1.12.0-1ubuntu0.1

192551 - Fedora Linux 25 FEDORA-2017-f6e3215f2b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9112, CVE-2016-9113, CVE-2016-9114, CVE-2016-9115, CVE-2016-9116, CVE-2016-9117, CVE-2016-9118

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f6e3215f2b

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/2017/8/?count=200&page=1

Fedora Core 25

mingw-openjpeg2-2.2.0-1.fc25

192561 - Fedora Linux 25 FEDORA-2017-82b5035f76 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11343

Description

The scan detected that the host is missing the following update:
FEDORA-2017-82b5035f76

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/2017/8/?count=200&page=1

Fedora Core 25

chicken-4.12.0-3.fc25

192562 - Fedora Linux 26 FEDORA-2017-76ce091a43 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11343

Description

The scan detected that the host is missing the following update:
FEDORA-2017-76ce091a43

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/2017/8/?count=200&page=2

Fedora Core 26

chicken-4.12.0-3.fc26

22302 - IBM WebSphere Application Server Weaker Than Expected Security Vulnerability (swg22006803)

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

Risk Level: Medium

CVE: CVE-2017-1504

Description

A vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a server engine for Java EE Web applications.

A vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in the PasswordUtil component. Successful exploitation could allow the system to not encrypt passwords as expected.

22321 - (VMSA-2017-0014) VMware NSX-V Edge OSPF Protocol LSA DoS Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4920

Description

A vulnerability is present in some versions of VMware NSX-V Edge.

Observation

VMware NSX-V Edge is a virtual networking and security software product.

A vulnerability is present in some versions of VMware NSX-V Edge. The implementation of the OSPF protocol in VMware NSX-V doesn't correctly handle the link-state advertisement. Successful exploitation could allow an attacker to cause a denial of service.

130853 - Debian Linux 8.0 DSA-3944-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3308, CVE-2017-3309, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3636, CVE-2017-3641, CVE-2017-3653

Description

The scan detected that the host is missing the following update:
DSA-3944-1

Observation

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

http://www.debian.org/security/2017/dsa-3944

Debian 8.0
all
mariadb-client-core-10.0_10.0.32-0+deb8u1
mariadb-server_10.0.32-0+deb8u1
mariadb-common_10.0.32-0+deb8u1
mariadb-server-core-10.0_10.0.32-0+deb8u1
libmariadbd-dev_10.0.32-0+deb8u1
mariadb-client_10.0.32-0+deb8u1
mariadb-test-10.0_10.0.32-0+deb8u1
mariadb-connect-engine-10.0_10.0.32-0+deb8u1
mariadb-client-10.0_10.0.32-0+deb8u1
mariadb-server-10.0_10.0.32-0+deb8u1
mariadb-test_10.0.32-0+deb8u1
mariadb-oqgraph-engine-10.0_10.0.32-0+deb8u1

145483 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2201-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6435, CVE-2017-6436, CVE-2017-6437, CVE-2017-6438, CVE-2017-6439

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2201-1

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-August/003143.html

SuSE SLED 12 SP2
x86_64
libplist3-1.12-20.3.2
libplist++3-debuginfo-1.12-20.3.2
libplist-debugsource-1.12-20.3.2
libplist++3-1.12-20.3.2
libplist3-debuginfo-1.12-20.3.2

SuSE SLES 12 SP3
x86_64
libplist-debugsource-1.12-20.3.2
libplist3-1.12-20.3.2
libplist3-debuginfo-1.12-20.3.2

SuSE SLES 12 SP2
x86_64
libplist-debugsource-1.12-20.3.2
libplist3-1.12-20.3.2
libplist3-debuginfo-1.12-20.3.2

SuSE SLED 12 SP3
x86_64
libplist3-1.12-20.3.2
libplist++3-debuginfo-1.12-20.3.2
libplist-debugsource-1.12-20.3.2

libplist++3-1.12-20.3.2
libplist3-debuginfo-1.12-20.3.2

145487 - SuSE SLES 11 SP4 SUSE-SU-2017:2173-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11171

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2173-1

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-August/003137.html

SuSE SLES 11 SP4
i586
gnome-session-lang-2.28.0-3.11.12.2
gnome-session-2.28.0-3.11.12.2

x86_64
gnome-session-lang-2.28.0-3.11.12.2
gnome-session-2.28.0-3.11.12.2

175208 - Scientific Linux Security ERRATA Moderate: openldap on SL7.x x86_64 (1708-16237)

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

Risk Level: Medium

CVE: CVE-2017-9287

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openldap on SL7.x x86_64 (1708-16237)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=16237

SL7
x86_64
openldap-servers-sql-2.4.44-5.el7
openldap-servers-2.4.44-5.el7
openldap-devel-2.4.44-5.el7
openldap-debuginfo-2.4.44-5.el7
openldap-2.4.44-5.el7
openldap-clients-2.4.44-5.el7

175209 - Scientific Linux Security ERRATA Low: ghostscript on SL7.x x86_64 (1708-6749)

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

Risk Level: Medium

CVE: CVE-2017-7207

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: ghostscript on SL7.x x86_64 (1708-6749)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=6749

SL7
x86_64
ghostscript-devel-9.07-28.el7
ghostscript-gtk-9.07-28.el7
ghostscript-9.07-28.el7
ghostscript-cups-9.07-28.el7
ghostscript-debuginfo-9.07-28.el7

noarch
ghostscript-doc-9.07-28.el7

175221 - Scientific Linux Security ERRATA Moderate: golang on (1708-15908)

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

Risk Level: Medium

CVE: CVE-2017-8932

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: golang on (1708-15908)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=15908

SL7
x86_64
golang-misc-1.8.3-1.el7
golang-src-1.8.3-1.el7
golang-bin-1.8.3-1.el7
golang-docs-1.8.3-1.el7
golang-1.8.3-1.el7
golang-tests-1.8.3-1.el7

175236 - Scientific Linux Security ERRATA Moderate: authconfig on SL7.x x86_64 (1708-8819)

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

Risk Level: Medium

CVE: CVE-2017-7488

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: authconfig on SL7.x x86_64 (1708-8819)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=8819

SL7
x86_64
authconfig-gtk-6.2.8-30.el7
authconfig-debuginfo-6.2.8-30.el7
authconfig-6.2.8-30.el7

178483 - Gentoo Linux GLSA-201708-08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3189

Description

The scan detected that the host is missing the following update:
GLSA-201708-08

Observation

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

https://security.gentoo.org/glsa/201708-08

Affected packages:
app-arch/bzip2 < 1.0.6-r8

192548 - Fedora Linux 25 FEDORA-2017-f318871e3b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-9096

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f318871e3b

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/2017/8/?count=200&page=1

Fedora Core 25

ruby-2.3.4-63.fc25

192549 - Fedora Linux 25 FEDORA-2017-a05e2b8545 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9208, CVE-2017-9209, CVE-2017-9210

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a05e2b8545

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/2017/8/?count=200&page=2

Fedora Core 25

cups-filters-1.10.0-4.fc25
qpdf-6.0.0-6.fc25

192559 - Fedora Linux 26 FEDORA-2017-92f8958310 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12132

Description

The scan detected that the host is missing the following update:
FEDORA-2017-92f8958310

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/2017/8/?count=200&page=1

Fedora Core 26

glibc-2.25-8.fc26

192567 - Fedora Linux 26 FEDORA-2017-f336ba205d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855, CVE-2017-5579, CVE-2017-7718

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f336ba205d

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/2017/8/?count=200&page=1

Fedora Core 26

xen-4.8.1-6.fc26

130854 - Debian Linux 8.0, 9.0 DSA-3949-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7555

Description

The scan detected that the host is missing the following update:
DSA-3949-1

Observation

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

http://www.debian.org/security/2017/dsa-3949

Debian 8.0
all
augeas-lenses_1.2.0-0.2+deb8u2
libaugeas-dev_1.2.0-0.2+deb8u2
libaugeas0_1.2.0-0.2+deb8u2
augeas-tools_1.2.0-0.2+deb8u2
augeas-dbg_1.2.0-0.2+deb8u2
augeas-doc_1.2.0-0.2+deb8u2

Debian 9.0
all
augeas-tools_1.8.0-1+deb9u1
augeas-lenses_1.8.0-1+deb9u1
libaugeas0_1.8.0-1+deb9u1
augeas-doc_1.8.0-1+deb9u1
augeas-dbg_1.8.0-1+deb9u1
libaugeas-dev_1.8.0-1+deb9u1

130857 - Debian Linux 8.0, 9.0 DSA-3947-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12904

Description

The scan detected that the host is missing the following update:
DSA-3947-1

Observation

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

http://www.debian.org/security/2017/dsa-3947

Debian 8.0
all
newsbeuter_2.8-2+deb8u1

Debian 9.0
all
newsbeuter_2.9-5+deb9u1

175212 - Scientific Linux Security ERRATA Low: tomcat on SL7.x (noarch) (1708-8410)

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

Risk Level: Low

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: tomcat on SL7.x (noarch) (1708-8410)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=8410

SL7
noarch
tomcat-docs-webapp-7.0.76-2.el7
tomcat-servlet-3.0-api-7.0.76-2.el7
tomcat-javadoc-7.0.76-2.el7
tomcat-jsp-2.2-api-7.0.76-2.el7
tomcat-7.0.76-2.el7
tomcat-el-2.2-api-7.0.76-2.el7
tomcat-jsvc-7.0.76-2.el7
tomcat-webapps-7.0.76-2.el7
tomcat-lib-7.0.76-2.el7
tomcat-admin-webapps-7.0.76-2.el7

182420 - FreeBSD salt Maliciously Crafted Minion IDs Can Cause Unwanted Directory Traversals On The Salt-master (3531141d-a708-477c-954a-

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

Risk Level: Low

CVE: CVE-2017-12791

Description

The scan detected that the host is missing the following update:
salt -- Maliciously crafted minion IDs can cause unwanted directory traversals on the Salt-master (3531141d-a708-477c-954a-2a0549e49ca9)

Observation

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

http://www.vuxml.org/freebsd/3531141d-a708-477c-954a-2a0549e49ca9.html

Affected packages:
py27-salt < 2016.11.7
py32-salt < 2016.11.7
py33-salt < 2016.11.7
py34-salt < 2016.11.7
py35-salt < 2016.11.7
py36-salt < 2016.11.7
2017.7.0 <= py27-salt < 2017.7.1
2017.7.0 <= py32-salt < 2017.7.1
2017.7.0 <= py33-salt < 2017.7.1
2017.7.0 <= py34-salt < 2017.7.1
2017.7.0 <= py35-salt < 2017.7.1
2017.7.0 <= py36-salt < 2017.7.1

182421 - FreeBSD drupal Drupal Core - Multiple Vulnerabilities (473b6a9e-8493-11e7-b24b-6cf0497db129)

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

Risk Level: Low

CVE: CVE-2017-6923, CVE-2017-6924, CVE-2017-6925

Description

The scan detected that the host is missing the following update:
drupal -- Drupal Core - Multiple Vulnerabilities (473b6a9e-8493-11e7-b24b-6cf0497db129)

Observation

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

http://www.vuxml.org/freebsd/473b6a9e-8493-11e7-b24b-6cf0497db129.html

Affected packages:
drupal8 < 8.3.7

182423 - FreeBSD libsoup Stack Based Buffer Overflow (8e7bbddd-8338-11e7-867f-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-2885

Description

The scan detected that the host is missing the following update:
libsoup -- stack based buffer overflow (8e7bbddd-8338-11e7-867f-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/8e7bbddd-8338-11e7-867f-b499baebfeaf.html

Affected packages:
libsoup < 2.52.2_1

182424 - FreeBSD SquirrelMail Post-authentication Remote Code Execution (e1de77e8-c45e-48d7-8866-5a6f943046de)

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:
SquirrelMail -- post-authentication remote code execution (e1de77e8-c45e-48d7-8866-5a6f943046de)

Observation

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

http://www.vuxml.org/freebsd/e1de77e8-c45e-48d7-8866-5a6f943046de.html

Affected packages:
squirrelmail < 20170705

182425 - FreeBSD evince and atril Command Injection Vulnerability In CBT Handler (01a197ca-67f1-11e7-a266-28924a333806)

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

Risk Level: Low

CVE: CVE-2017-1000083

Description

The scan detected that the host is missing the following update:
evince and atril -- command injection vulnerability in CBT handler (01a197ca-67f1-11e7-a266-28924a333806)

Observation

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

http://www.vuxml.org/freebsd/01a197ca-67f1-11e7-a266-28924a333806.html

Affected packages:
evince <= 3.24.0
evince-lite <= 3.24.0
atril <= 1.19.0
atril-lite <= 1.19.0

182427 - FreeBSD dnsdist Multiple Vulnerabilities (198d82f3-8777-11e7-950a-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2016-7069, CVE-2017-7557

Description

The scan detected that the host is missing the following update:
dnsdist -- multiple vulnerabilities (198d82f3-8777-11e7-950a-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/198d82f3-8777-11e7-950a-e8e0b747a45a.html

Affected packages:
dnsdist < 1.2.0

185840 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3391-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7780, CVE-2017-7781, CVE-2017-7783, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7788, CVE-2017-7789, CVE-2017-7791, CVE-2017-7792, CVE-2017-7794, CVE-2017-7797, CVE-2017-7798, CVE-2017-7799, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7806, CVE-2017-7807, CVE-2017-7808, CVE-2017-7809

Description

The scan detected that the host is missing the following update:
USN-3391-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004010.html

Ubuntu 16.04

xul-ext-ubufox_3.4-0ubuntu0.16.04.1

Ubuntu 14.04

xul-ext-ubufox_3.4-0ubuntu0.14.04.1

Ubuntu 17.04

xul-ext-ubufox_3.4-0ubuntu0.17.04.1

185842 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3397-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-11185

Description

The scan detected that the host is missing the following update:
USN-3397-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004018.html

Ubuntu 16.04

strongswan_5.3.5-1ubuntu3.4
libstrongswan_5.3.5-1ubuntu3.4

Ubuntu 14.04

strongswan_5.1.2-0ubuntu2.7
libstrongswan_5.1.2-0ubuntu2.7

Ubuntu 17.04

libstrongswan_5.5.1-1ubuntu3.2
strongswan_5.5.1-1ubuntu3.2

185843 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3398-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778

Description

The scan detected that the host is missing the following update:
USN-3398-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004019.html

Ubuntu 16.04

libgraphite2-3_1.3.10-0ubuntu0.16.04.1

Ubuntu 14.04

libgraphite2-3_1.3.10-0ubuntu0.14.04.1

Ubuntu 17.04

libgraphite2-3_1.3.10-0ubuntu0.17.04.1

185847 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3399-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12836

Description

The scan detected that the host is missing the following update:
USN-3399-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004020.html

Ubuntu 16.04

cvs_1.12.13+real-15ubuntu0.1

Ubuntu 14.04

cvs_1.12.13+real-12ubuntu0.1

Ubuntu 17.04

cvs_1.12.13+real-22ubuntu0.1

185848 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3391-3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7780, CVE-2017-7781, CVE-2017-7783, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7788, CVE-2017-7789, CVE-2017-7791, CVE-2017-7792, CVE-2017-7794, CVE-2017-7797, CVE-2017-7798, CVE-2017-7799, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7806, CVE-2017-7807, CVE-2017-7808, CVE-2017-7809

Description

The scan detected that the host is missing the following update:
USN-3391-3

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004016.html

Ubuntu 16.04

firefox_55.0.2+build1-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_55.0.2+build1-0ubuntu0.14.04.1

Ubuntu 17.04

firefox_55.0.2+build1-0ubuntu0.17.04.1

185851 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3400-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7555

Description

The scan detected that the host is missing the following update:
USN-3400-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004021.html

Ubuntu 16.04

augeas-tools_1.4.0-0ubuntu1.1
libaugeas0_1.4.0-0ubuntu1.1

Ubuntu 14.04

libaugeas0_1.2.0-0ubuntu1.3
augeas-tools_1.2.0-0ubuntu1.3

Ubuntu 17.04

libaugeas0_1.6.0-0ubuntu3.1
augeas-tools_1.6.0-0ubuntu3.1

192546 - Fedora Linux 25 FEDORA-2017-c9d8011d69 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2885

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c9d8011d69

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/2017/8/?count=200&page=1

Fedora Core 25

mingw-libsoup-2.56.1-1.fc25

192547 - Fedora Linux 26 FEDORA-2017-1f4c82d73e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2885

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1f4c82d73e

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/2017/8/?count=200&page=1

Fedora Core 26

mingw-libsoup-2.58.2-1.fc26

192550 - Fedora Linux 26 FEDORA-2017-aab5f759f5 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-aab5f759f5

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/2017/8/?count=200&page=1

Fedora Core 26

cryptlib-3.4.3.1-7.fc26

192553 - Fedora Linux 25 FEDORA-2017-1d1a38bdd1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-9800

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1d1a38bdd1

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/2017/8/?count=200&page=1

Fedora Core 25

subversion-1.9.7-1.fc25

192554 - Fedora Linux 26 FEDORA-2017-f8f4cd5b67 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12843

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f8f4cd5b67

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/2017/8/?count=200&page=1

Fedora Core 26

cyrus-imapd-3.0.3-1.fc26

192556 - Fedora Linux 25 FEDORA-2017-866fc566e0 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-2017-866fc566e0

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/2017/8/?count=200&page=1

Fedora Core 25

torbrowser-launcher-0.2.8-1.fc25

192558 - Fedora Linux 26 FEDORA-2017-f79ae2b96f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5091, CVE-2017-5092, CVE-2017-5093, CVE-2017-5094, CVE-2017-5095, CVE-2017-5096, CVE-2017-5097, CVE-2017-5098, CVE-2017-5099, CVE-2017-5100, CVE-2017-5101, CVE-2017-5102, CVE-2017-5103, CVE-2017-5104, CVE-2017-5105, CVE-2017-5106, CVE-2017-5107, CVE-2017-5108, CVE-2017-5109, CVE-2017-5110, CVE-2017-7000

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f79ae2b96f

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/2017/8/?count=200&page=2

Fedora Core 26

chromium-60.0.3112.90-1.fc26

192560 - Fedora Linux 25 FEDORA-2017-33c8085c5d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6814

Description

The scan detected that the host is missing the following update:
FEDORA-2017-33c8085c5d

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/2017/8/?count=200&page=2

Fedora Core 25

groovy18-1.8.9-28.fc25

192563 - Fedora Linux 26 FEDORA-2017-48f0384090 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1002152

Description

The scan detected that the host is missing the following update:
FEDORA-2017-48f0384090

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/2017/8/?count=200&page=1

Fedora Core 26

bodhi-2.9.1-1.fc26

192565 - Fedora Linux 26 FEDORA-2017-661dddc462 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6814

Description

The scan detected that the host is missing the following update:
FEDORA-2017-661dddc462

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/2017/8/?count=200&page=2

Fedora Core 26

groovy18-1.8.9-28.fc26

192566 - Fedora Linux 26 FEDORA-2017-c535f23493 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-c535f23493

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/2017/8/?count=200&page=2

Fedora Core 26

torbrowser-launcher-0.2.8-1.fc26

175218 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1708-12131)

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

Risk Level: Low

CVE: CVE-2016-4020, CVE-2017-2633, CVE-2017-5898

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1708-12131)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=12131

SL7
x86_64
qemu-kvm-common-1.5.3-141.el7
qemu-kvm-1.5.3-141.el7
qemu-img-1.5.3-141.el7
qemu-kvm-tools-1.5.3-141.el7
qemu-kvm-debuginfo-1.5.3-141.el7

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.

135184 - Oracle Solaris 11.3.22.3.0 Update Is Not Installed (CVE-2017-3632)

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

Risk Level: High

CVE: CVE-2017-3632

Update Details

Risk is updated

130838 - Debian Linux 8.0 DSA-3935-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Update Details

Risk is updated

130844 - Debian Linux 9.0 DSA-3936-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Update Details

Risk is updated

181424 - FreeBSD rest-client Session Fixation Vulnerability (83a7a720-07d8-11e5-9a28-001e67150279)

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

Risk Level: High

CVE: CVE-2015-1820

Update Details

Risk is updated

181589 - FreeBSD ganglia-webfrontend Auth Bypass (d68df01b-564e-11e5-9ad8-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2015-6816

Update Details

Risk is updated

182417 - FreeBSD PostgreSQL Vulnerabilities (982872f1-7dd3-11e7-9736-6cc21735f730)

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Update Details

Risk is updated

185832 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3390-1 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Update Details
Risk is updated

189824 - Fedora Linux 21 FEDORA-2015-accdc7ebfc Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-6816

Update Details
Risk is updated

189844 - Fedora Linux 22 FEDORA-2015-ee7a2b5844 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-6816

Update Details
Risk is updated

189902 - Fedora Linux 23 FEDORA-2015-de8ba28354 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-6816

Update Details
Risk is updated

192511 - Fedora Linux 26 FEDORA-2017-d9cac37bd8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Update Details
Risk is updated

163424 - Oracle Enterprise Linux ELSA-2017-2473 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7533

Update Details
FASLScript is updated

145165 - SuSE Linux 13.2 openSUSE-SU-2017:0158-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3462

Update Details

Risk is updated

181634 - FreeBSD Salt Multiple Vulnerabilities (3934cc60-f0fa-4eca-be09-c8bd7ae42871)

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

Risk Level: Medium

CVE: CVE-2015-6918, CVE-2015-6941

Update Details

Risk is updated

182399 - FreeBSD MySQL Multiple Vulnerabilities (cda2f3c2-6c8b-11e7-867f-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-3529, CVE-2017-3633, CVE-2017-3634, CVE-2017-3635, CVE-2017-3636, CVE-2017-3637, CVE-2017-3638, CVE-2017-3639, CVE-2017-3640, CVE-2017-3641, CVE-2017-3642, CVE-2017-3643, CVE-2017-3644, CVE-2017-3645, CVE-2017-3646, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3650, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Update Details

Risk is updated

185784 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3357-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3529, CVE-2017-3633, CVE-2017-3634, CVE-2017-3635, CVE-2017-3636, CVE-2017-3637, CVE-2017-3638, CVE-2017-3639, CVE-2017-3640, CVE-2017-3641, CVE-2017-3642, CVE-2017-3643, CVE-2017-3644, CVE-2017-3645, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3650, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Update Details

Risk is updated

189901 - Fedora Linux 22 FEDORA-2015-13616 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3277

Update Details

Risk is updated

192522 - Fedora Linux 25 FEDORA-2017-7c039552fa Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3633, CVE-2017-3634, CVE-2017-3635, CVE-2017-3636, CVE-2017-3641, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Update Details

Risk is updated

192539 - Fedora Linux 26 FEDORA-2017-ee93493bea Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3633, CVE-2017-3634, CVE-2017-3635, CVE-2017-3636, CVE-2017-3641, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Update Details

Risk is updated

130832 - Debian Linux 8.0 DSA-3922-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3635, CVE-2017-3636, CVE-2017-3641, CVE-2017-3648, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Update Details

Risk is updated

192528 - Fedora Linux 25 FEDORA-2017-571e659c85 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000100, CVE-2017-1000101, CVE-2017-7000

Update Details

CVE is updated

45000 - ShellLogon.fasl3

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

45001 - ShellInitialize.fasl3

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.