2017-SEP-22
FSL version 7.5.961

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

22462 - (CTX227185) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-14316, CVE-2017-14318, CVE-2017-14319

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.

22324 - (K06045217) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5022

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 BIG-IP systems. The flaw lies in Virtual servers and self IP addresses. Successful exploitation could allow a remote attacker to cause a denial of service condition.

22458 - Delta Industrial Automation Products Multiple File Parsing Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Delta Electronics ISPSoft, PMSoft and WPLSoft.

Observation

Delta Electronics ISPSoft, PMSoft and WPLSoft are part of a suite of platforms used for control software edition of Delta DVP Series Programable Logic Controllers (PLCs).

Multiple vulnerabilities are present in some versions of Delta Electronics ISPSoft, PMSoft and WPLSoft. The flaws are related with bad parsing of DVP files. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

22459 - Delta Industrial Automation Products Multiple File Parsing Vulnerabilities II

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Delta Electronics ISPSoft, PMSoft and WPLSoft.

Observation

Delta Electronics ISPSoft, PMSoft and WPLSoft are part of a suite of platforms used for control software edition of Delta DVP Series Programable Logic Controllers (PLCs).

Multiple vulnerabilities are present in some versions of Delta Electronics ISPSoft, PMSoft and WPLSoft. The flaws are related with bad parsing of DVP files. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

22460 - Delta Industrial Automation Products Multiple File Parsing Vulnerabilities III

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Delta Electronics ISPSoft, PMSoft and WPLSoft.

Observation

Delta Electronics ISPSoft, PMSoft and WPLSoft are part of a suite of platforms used for control software edition of Delta DVP Series Programable Logic Controllers (PLCs).

Multiple vulnerabilities are present in some versions of Delta Electronics ISPSoft, PMSoft and WPLSoft. The flaws are related with bad parsing of DVP files. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

22472 - (VMSA-2017-0015) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4924, CVE-2017-4925

Description

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

Observation

VMware Workstation is a virtualization software.

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

130890 - Debian Linux 8.0, 9.0 DSA-3981-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112, CVE-2017-1000251, CVE-2017-1000252, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-1000380, CVE-2017-10661, CVE-2017-11600, CVE-2017-12134, CVE-2017-12146, CVE-2017-12153, CVE-2017-12154, CVE-2017-14106, CVE-2017-14140, CVE-2017-14156, CVE-2017-14340, CVE-2017-14489, CVE-2017-14497, CVE-2017-7518, CVE-2017-7558

Description

The scan detected that the host is missing the following update:
DSA-3981-1

Observation

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

http://www.debian.org/security/2017/dsa-3981

Debian 8.0
all
squashfs-modules-3.16.0-4-r4k-ip22-di_3.16.43-2+deb8u5
isofs-modules-3.16.0-4-loongson-3-di_3.16.43-2+deb8u5
isofs-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u5
nic-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
usb-serial-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u5
nbd-modules-3.16.0-4-r4k-ip22-di_3.16.43-2+deb8u5
virtio-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u5
ppp-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u5
scsi-core-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
linux-image-3.16.0-4-arm64-dbg_3.16.43-2+deb8u5
sata-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u5
nic-usb-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u5
linux-image-3.16.0-4-versatile_3.16.43-2+deb8u5
uinput-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u5
sound-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u5
squashfs-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u5
kernel-image-3.16.0-4-armmp-di_3.16.43-2+deb8u5
nic-shared-modules-3.16.0-4-loongson-3-di_3.16.43-2+deb8u5
fat-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u5
scsi-extra-modules-3.16.0-4-loongson-3-di_3.16.43-2+deb8u5
nic-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u5
crc-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
crc-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u5
i2c-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u5
ata-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u5
btrfs-modules-3.16.0-4-r5k-ip32-di_3.16.43-2+deb8u5
nic-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u5
linux-headers-3.16.0-4-all_3.16.43-2+deb8u5
nbd-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u5
zlib-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u5
loop-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u5
isofs-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u5
loop-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
hyperv-modules-3.16.0-4-586-di_3.16.43-2+deb8u5

udf-modules-3.16.0-4-r4k-ip22-di_3.16.43-2+deb8u5
multipath-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
fuse-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u5
scsi-core-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u5
nic-shared-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u5
scsi-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u5
jfs-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u5
crypto-dm-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
scsi-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
crypto-dm-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u5
sata-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u5
firewire-core-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u5
scsi-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u5
virtio-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u5
fuse-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u5
fat-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u5
ata-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u5
crypto-dm-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
usb-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u5
fat-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
pata-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
loop-modules-3.16.0-4-versatile-di_3.16.43-2+deb8u5
crc-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u5
nic-pcmcia-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u5
speakup-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u5
scsi-common-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u5
acpi-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u5
scsi-modules-3.16.0-4-octeon-di_3.16.43-2+deb8u5
md-modules-3.16.0-4-octeon-di_3.16.43-2+deb8u5
jffs2-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u5
nic-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u5
loop-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u5
linux-image-3.16.0-4-arm64_3.16.43-2+deb8u5
xfs-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
isofs-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u5
event-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u5
cdrom-core-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
cdrom-core-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u5
ext4-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u5
pcmcia-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u5
multipath-modules-3.16.0-4-s390x-di_3.16.43-2+deb8u5
crc-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u5
linux-headers-3.16.0-4-all-arm64_3.16.43-2+deb8u5
isofs-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u5
xfs-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u5
hypervisor-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u5
jfs-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
nic-usb-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u5
minix-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
dasd-modules-3.16.0-4-s390x-di_3.16.43-2+deb8u5
linux-headers-3.16.0-4-ixp4xx_3.16.43-2+deb8u5
ata-modules-3.16.0-4-686-pae-di_3.16.43-2+deb8u5
fuse-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u5
input-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u5
minix-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u5
fuse-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u5
md-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
nic-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u5
virtio-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u5
crypto-dm-modules-3.16.0-4-r5k-ip32-di_3.16.43-2+deb8u5

fuse-modules-3.16.0-4-loongson-3-di_3.16.43-2+deb8u5
ppp-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u5
loop-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u5
linux-headers-3.16.0-4-versatile_3.16.43-2+deb8u5
firewire-core-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u5
md-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u5
crc-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u5
core-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u5
input-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u5
zlib-modules-3.16.0-4-orion5x-di_3.16.43-2+deb8u5
crypto-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u5
linux-image-3.16.0-4-4kc-malta_3.16.43-2+deb8u5
loop-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u5
firewire-core-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
cdrom-core-modules-3.16.0-4-sb1-bcm91250a-di_3.16.43-2+deb8u5
ext4-modules-3.16.0-4-arm64-di_3.16.43-2+deb8u5
crypto-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
usb-storage-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u5
nic-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u5
sata-modules-3.16.0-4-octeon-di_3.16.43-2+deb8u5
linux-headers-3.16.0-4-r5k-ip32_3.16.43-2+deb8u5
firewire-core-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u5
scsi-core-modules-3.16.0-4-s390x-di_3.16.43-2+deb8u5
event-modules-3.16.0-4-powerpc-di_3.16.43-2+deb8u5
isofs-modules-3.16.0-4-powerpc64le-di_3.16.43-2+deb8u5
pcmcia-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
scsi-extra-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
nic-modules-3.16.0-4-amd64-di_3.16.43-2+deb8u5
nic-wireless-modules-3.16.0-4-loongson-2e-di_3.16.43-2+deb8u5
nic-usb-modules-3.16.0-4-4kc-malta-di_3.16.43-2+deb8u5
crypto-dm-modules-3.16.0-4-octeon-di_3.16.43-2+deb8u5
scsi-core-modules-3.16.0-4-powerpc64-di_3.16.43-2+deb8u5
nic-wireless-modules-3.16.0-4-loongson-2f-di_3.16.43-2+deb8u5
uinput-modules-3.16.0-4-kirkwood-di_3.16.43-2+deb8u5
linux-headers-3.16.0-4-all-ppc64el_3.16.43-2+deb8u5
nic-modules-3.16.0-4-586-di_3.16.43-2+deb8u5
event-modules-3.16.0-4-armmp-di_3.16.43-2+deb8u5
crypto-modules-3.16.0-4-s390x-di_3.16.43-2+deb8u5

Debian 9.0
all
multipath-modules-4.9.0-3-4kc-malta-di_4.9.30-2+deb9u5

132399 - Oracle VM OVMSA-2017-0152 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-1000365, CVE-2017-12134

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0152

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-September/000781.html

OVM3.3
x86_64
kernel-uek-firmware-3.8.13-118.19.7.el6uek
kernel-uek-3.8.13-118.19.7.el6uek

132400 - Oracle VM OVMSA-2017-0151 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0151

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-September/000780.html

OVM3.4
x86_64
kernel-uek-4.1.12-103.3.8.1.el6uek
kernel-uek-firmware-4.1.12-103.3.8.1.el6uek

141721 - Red Hat Enterprise Linux RHSA-2017-2788 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7555

Description

The scan detected that the host is missing the following update:
RHSA-2017-2788

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00049.html

RHEL7D
x86_64
augeas-debuginfo-1.4.0-2.el7_4.1
augeas-1.4.0-2.el7_4.1
augeas-libs-1.4.0-2.el7_4.1
augeas-devel-1.4.0-2.el7_4.1

RHEL7S
x86_64
augeas-debuginfo-1.4.0-2.el7_4.1
augeas-1.4.0-2.el7_4.1
augeas-libs-1.4.0-2.el7_4.1
augeas-devel-1.4.0-2.el7_4.1

RHEL7WS
x86_64
augeas-debuginfo-1.4.0-2.el7_4.1
augeas-1.4.0-2.el7_4.1
augeas-libs-1.4.0-2.el7_4.1
augeas-devel-1.4.0-2.el7_4.1

141723 - Red Hat Enterprise Linux RHSA-2017-2787 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5483, CVE-2016-6664, CVE-2016-8327, CVE-2017-3238, CVE-2017-3244, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-2017-3273, CVE-2017-3291, CVE-2017-3302, CVE-2017-3305, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3450, CVE-2017-3452, CVE-2017-3453, CVE-2017-3456, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3599, CVE-2017-3600, CVE-2017-3633, CVE-2017-3634, CVE-2017-3636, CVE-2017-3641, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Description

The scan detected that the host is missing the following update:
RHSA-2017-2787

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00048.html

RHEL6_7S
x86_64
rh-mysql56-mysql-bench-5.6.37-5.el6
rh-mysql56-mysql-config-5.6.37-5.el6
rh-mysql56-mysql-errmsg-5.6.37-5.el6
rh-mysql56-mysql-devel-5.6.37-5.el6
rh-mysql56-mysql-5.6.37-5.el6
rh-mysql56-mysql-server-5.6.37-5.el6
rh-mysql56-mysql-debuginfo-5.6.37-5.el6
rh-mysql56-mysql-test-5.6.37-5.el6
rh-mysql56-mysql-common-5.6.37-5.el6

RHEL6S
x86_64
rh-mysql56-mysql-bench-5.6.37-5.el6
rh-mysql56-mysql-config-5.6.37-5.el6
rh-mysql56-mysql-errmsg-5.6.37-5.el6
rh-mysql56-mysql-devel-5.6.37-5.el6
rh-mysql56-mysql-5.6.37-5.el6
rh-mysql56-mysql-server-5.6.37-5.el6
rh-mysql56-mysql-debuginfo-5.6.37-5.el6
rh-mysql56-mysql-test-5.6.37-5.el6
rh-mysql56-mysql-common-5.6.37-5.el6

RHEL6WS
x86_64
rh-mysql56-mysql-bench-5.6.37-5.el6
rh-mysql56-mysql-config-5.6.37-5.el6
rh-mysql56-mysql-errmsg-5.6.37-5.el6
rh-mysql56-mysql-devel-5.6.37-5.el6
rh-mysql56-mysql-5.6.37-5.el6

rh-mysql56-mysql-server-5.6.37-5.el6
rh-mysql56-mysql-debuginfo-5.6.37-5.el6
rh-mysql56-mysql-test-5.6.37-5.el6
rh-mysql56-mysql-common-5.6.37-5.el6

RHEL7S
x86_64
rh-mysql56-mysql-bench-5.6.37-5.el7
rh-mysql56-mysql-common-5.6.37-5.el7
rh-mysql56-mysql-server-5.6.37-5.el7
rh-mysql56-mysql-config-5.6.37-5.el7
rh-mysql56-mysql-5.6.37-5.el7
rh-mysql56-mysql-debuginfo-5.6.37-5.el7
rh-mysql56-mysql-test-5.6.37-5.el7
rh-mysql56-mysql-errmsg-5.6.37-5.el7
rh-mysql56-mysql-devel-5.6.37-5.el7

RHEL7WS
x86_64
rh-mysql56-mysql-bench-5.6.37-5.el7
rh-mysql56-mysql-common-5.6.37-5.el7
rh-mysql56-mysql-server-5.6.37-5.el7
rh-mysql56-mysql-config-5.6.37-5.el7
rh-mysql56-mysql-5.6.37-5.el7
rh-mysql56-mysql-debuginfo-5.6.37-5.el7
rh-mysql56-mysql-test-5.6.37-5.el7
rh-mysql56-mysql-errmsg-5.6.37-5.el7
rh-mysql56-mysql-devel-5.6.37-5.el7

145933 - SuSE SLES 11 SP4 SUSE-SU-2017:2532-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2532-1

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-September/003251.html

SuSE SLES 11 SP4
i586
emacs-info-22.3-42.3.1
emacs-el-22.3-42.3.1
emacs-22.3-42.3.1
emacs-x11-22.3-42.3.1
emacs-nox-22.3-42.3.1

x86_64
emacs-info-22.3-42.3.1
emacs-el-22.3-42.3.1
emacs-22.3-42.3.1
emacs-x11-22.3-42.3.1

emacs-nox-22.3-42.3.1

145934 - SuSE SLES 11 SP4 SUSE-SU-2017:2548-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2548-1

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-September/003256.html

SuSE SLES 11 SP4
i586
kernel-xen-base-3.0.101-108.10.1
kernel-default-3.0.101-108.10.1
kernel-xen-3.0.101-108.10.1
kernel-ec2-3.0.101-108.10.1
kernel-ec2-base-3.0.101-108.10.1
kernel-default-base-3.0.101-108.10.1
kernel-pae-base-3.0.101-108.10.1
kernel-ec2-devel-3.0.101-108.10.1
kernel-syms-3.0.101-108.10.1
kernel-pae-3.0.101-108.10.1
kernel-trace-devel-3.0.101-108.10.1
kernel-trace-base-3.0.101-108.10.1
kernel-trace-3.0.101-108.10.1
kernel-xen-devel-3.0.101-108.10.1
kernel-source-3.0.101-108.10.1
kernel-pae-devel-3.0.101-108.10.1
kernel-default-devel-3.0.101-108.10.1

x86_64
kernel-xen-base-3.0.101-108.10.1
kernel-default-3.0.101-108.10.1
kernel-xen-3.0.101-108.10.1
kernel-ec2-3.0.101-108.10.1
kernel-ec2-base-3.0.101-108.10.1
kernel-default-base-3.0.101-108.10.1
kernel-ec2-devel-3.0.101-108.10.1
kernel-syms-3.0.101-108.10.1
kernel-trace-devel-3.0.101-108.10.1
kernel-trace-base-3.0.101-108.10.1
kernel-trace-3.0.101-108.10.1
kernel-xen-devel-3.0.101-108.10.1
kernel-source-3.0.101-108.10.1
kernel-default-devel-3.0.101-108.10.1

145936 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:2542-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2542-1

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-September/003254.html

SuSE SLES 12 SP3
noarch
apache2-doc-2.4.23-29.6.1

x86_64
apache2-debuginfo-2.4.23-29.6.1
apache2-2.4.23-29.6.1
apache2-utils-debuginfo-2.4.23-29.6.1
apache2-prefork-debuginfo-2.4.23-29.6.1
apache2-debugsource-2.4.23-29.6.1
apache2-worker-debuginfo-2.4.23-29.6.1
apache2-prefork-2.4.23-29.6.1
apache2-example-pages-2.4.23-29.6.1
apache2-utils-2.4.23-29.6.1
apache2-worker-2.4.23-29.6.1

SuSE SLES 12 SP2
noarch
apache2-doc-2.4.23-29.6.1

x86_64
apache2-debuginfo-2.4.23-29.6.1
apache2-2.4.23-29.6.1
apache2-utils-debuginfo-2.4.23-29.6.1
apache2-prefork-debuginfo-2.4.23-29.6.1
apache2-debugsource-2.4.23-29.6.1
apache2-worker-debuginfo-2.4.23-29.6.1
apache2-prefork-2.4.23-29.6.1
apache2-example-pages-2.4.23-29.6.1
apache2-utils-2.4.23-29.6.1
apache2-worker-2.4.23-29.6.1

145937 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2549-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2549-1

Observation

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

For more information see:

http://lists.opensuse.org/opensuse-updates/2017-09/msg00095.html

SuSE Linux 42.2
i586
apache2-prefork-debuginfo-2.4.23-8.12.1
apache2-2.4.23-8.12.1
apache2-devel-2.4.23-8.12.1
apache2-prefork-2.4.23-8.12.1
apache2-utils-2.4.23-8.12.1
apache2-event-debuginfo-2.4.23-8.12.1
apache2-example-pages-2.4.23-8.12.1
apache2-utils-debuginfo-2.4.23-8.12.1
apache2-event-2.4.23-8.12.1
apache2-debugsource-2.4.23-8.12.1
apache2-worker-2.4.23-8.12.1
apache2-debuginfo-2.4.23-8.12.1
apache2-worker-debuginfo-2.4.23-8.12.1

noarch
apache2-doc-2.4.23-8.12.1

x86_64
apache2-prefork-debuginfo-2.4.23-8.12.1
apache2-2.4.23-8.12.1
apache2-devel-2.4.23-8.12.1
apache2-prefork-2.4.23-8.12.1
apache2-utils-2.4.23-8.12.1
apache2-event-debuginfo-2.4.23-8.12.1
apache2-example-pages-2.4.23-8.12.1
apache2-utils-debuginfo-2.4.23-8.12.1
apache2-event-2.4.23-8.12.1
apache2-debugsource-2.4.23-8.12.1
apache2-worker-2.4.23-8.12.1
apache2-debuginfo-2.4.23-8.12.1
apache2-worker-debuginfo-2.4.23-8.12.1

SuSE Linux 42.3
i586
apache2-event-debuginfo-2.4.23-16.1
apache2-worker-debuginfo-2.4.23-16.1
apache2-utils-2.4.23-16.1
apache2-utils-debuginfo-2.4.23-16.1
apache2-2.4.23-16.1
apache2-debugsource-2.4.23-16.1
apache2-prefork-debuginfo-2.4.23-16.1
apache2-devel-2.4.23-16.1
apache2-worker-2.4.23-16.1
apache2-example-pages-2.4.23-16.1
apache2-debuginfo-2.4.23-16.1
apache2-prefork-2.4.23-16.1
apache2-event-2.4.23-16.1

noarch
apache2-doc-2.4.23-16.1

x86_64
apache2-event-debuginfo-2.4.23-16.1
apache2-worker-debuginfo-2.4.23-16.1

apache2-utils-2.4.23-16.1
apache2-utils-debuginfo-2.4.23-16.1
apache2-2.4.23-16.1
apache2-debugsource-2.4.23-16.1
apache2-prefork-debuginfo-2.4.23-16.1
apache2-devel-2.4.23-16.1
apache2-worker-2.4.23-16.1
apache2-example-pages-2.4.23-16.1
apache2-debuginfo-2.4.23-16.1
apache2-prefork-2.4.23-16.1
apache2-event-2.4.23-16.1

145939 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2535-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2535-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00089.html

SuSE Linux 42.2
i586
emacs-debugsource-24.3-24.6.1
emacs-x11-24.3-24.6.1
emacs-nox-debuginfo-24.3-24.6.1
emacs-x11-debuginfo-24.3-24.6.1
emacs-nox-24.3-24.6.1
emacs-24.3-24.6.1
emacs-debuginfo-24.3-24.6.1
etags-debuginfo-24.3-24.6.1
etags-24.3-24.6.1

noarch
emacs-info-24.3-24.6.1
emacs-el-24.3-24.6.1

x86_64
emacs-debugsource-24.3-24.6.1
emacs-x11-24.3-24.6.1
emacs-nox-debuginfo-24.3-24.6.1
emacs-x11-debuginfo-24.3-24.6.1
emacs-nox-24.3-24.6.1
emacs-24.3-24.6.1
emacs-debuginfo-24.3-24.6.1
etags-debuginfo-24.3-24.6.1
etags-24.3-24.6.1

SuSE Linux 42.3
i586
emacs-x11-24.3-28.1

etags-debuginfo-24.3-28.1
etags-24.3-28.1
emacs-debuginfo-24.3-28.1
emacs-x11-debuginfo-24.3-28.1
emacs-debugsource-24.3-28.1
emacs-24.3-28.1
emacs-nox-24.3-28.1
emacs-nox-debuginfo-24.3-28.1

noarch
emacs-el-24.3-28.1
emacs-info-24.3-28.1

x86_64
emacs-x11-24.3-28.1
etags-debuginfo-24.3-28.1
etags-24.3-28.1
emacs-debuginfo-24.3-28.1
emacs-x11-debuginfo-24.3-28.1
emacs-debugsource-24.3-28.1
emacs-24.3-28.1
emacs-nox-24.3-28.1
emacs-nox-debuginfo-24.3-28.1

145941 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2536-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12933

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2536-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00090.html

SuSE Linux 42.2
i586
php5-snmp-debuginfo-5.5.14-77.12.1
php5-ctype-debuginfo-5.5.14-77.12.1
php5-bcmath-5.5.14-77.12.1
php5-shmop-5.5.14-77.12.1
php5-ctype-5.5.14-77.12.1
apache2-mod_php5-5.5.14-77.12.1
php5-calendar-5.5.14-77.12.1
php5-sqlite-debuginfo-5.5.14-77.12.1
php5-curl-debuginfo-5.5.14-77.12.1
php5-firebird-5.5.14-77.12.1
php5-wddx-5.5.14-77.12.1
php5-soap-5.5.14-77.12.1
php5-fpm-5.5.14-77.12.1
php5-mcrypt-5.5.14-77.12.1
php5-sysvshm-debuginfo-5.5.14-77.12.1
php5-fpm-debuginfo-5.5.14-77.12.1

apache2-mod_php5-debuginfo-5.5.14-77.12.1
php5-pspell-debuginfo-5.5.14-77.12.1
php5-xmlwriter-5.5.14-77.12.1
php5-posix-debuginfo-5.5.14-77.12.1
php5-sysvshm-5.5.14-77.12.1
php5-pcntl-debuginfo-5.5.14-77.12.1
php5-gd-debuginfo-5.5.14-77.12.1
php5-odbc-debuginfo-5.5.14-77.12.1
php5-soap-debuginfo-5.5.14-77.12.1
php5-zlib-5.5.14-77.12.1
php5-mysql-5.5.14-77.12.1
php5-sockets-5.5.14-77.12.1
php5-mbstring-5.5.14-77.12.1
php5-ftp-debuginfo-5.5.14-77.12.1
php5-dom-debuginfo-5.5.14-77.12.1
php5-wddx-debuginfo-5.5.14-77.12.1
php5-pspell-5.5.14-77.12.1
php5-pgsql-5.5.14-77.12.1
php5-zip-5.5.14-77.12.1
php5-ldap-debuginfo-5.5.14-77.12.1
php5-iconv-debuginfo-5.5.14-77.12.1
php5-tokenizer-5.5.14-77.12.1
php5-suhosin-5.5.14-77.12.1
php5-bz2-5.5.14-77.12.1
php5-mysql-debuginfo-5.5.14-77.12.1
php5-mssql-5.5.14-77.12.1
php5-xmlrpc-5.5.14-77.12.1
php5-bz2-debuginfo-5.5.14-77.12.1
php5-pcntl-5.5.14-77.12.1
php5-fileinfo-debuginfo-5.5.14-77.12.1
php5-sysvsem-5.5.14-77.12.1
php5-tidy-debuginfo-5.5.14-77.12.1
php5-zlib-debuginfo-5.5.14-77.12.1
php5-ftp-5.5.14-77.12.1
php5-pdo-debuginfo-5.5.14-77.12.1
php5-intl-5.5.14-77.12.1
php5-gettext-debuginfo-5.5.14-77.12.1
php5-calendar-debuginfo-5.5.14-77.12.1
php5-opcache-5.5.14-77.12.1
php5-odbc-5.5.14-77.12.1
php5-sockets-debuginfo-5.5.14-77.12.1
php5-openssl-5.5.14-77.12.1
php5-gd-5.5.14-77.12.1
php5-phar-5.5.14-77.12.1
php5-bcmath-debuginfo-5.5.14-77.12.1
php5-sqlite-5.5.14-77.12.1
php5-debuginfo-5.5.14-77.12.1
php5-imap-5.5.14-77.12.1
php5-openssl-debuginfo-5.5.14-77.12.1
php5-readline-5.5.14-77.12.1
php5-posix-5.5.14-77.12.1
php5-devel-5.5.14-77.12.1
php5-iconv-5.5.14-77.12.1
php5-imap-debuginfo-5.5.14-77.12.1
php5-exif-debuginfo-5.5.14-77.12.1
php5-tidy-5.5.14-77.12.1
php5-sysvmsg-debuginfo-5.5.14-77.12.1
php5-opcache-debuginfo-5.5.14-77.12.1
php5-fastcgi-debuginfo-5.5.14-77.12.1
php5-mssql-debuginfo-5.5.14-77.12.1

php5-xmlreader-5.5.14-77.12.1
php5-xsl-debuginfo-5.5.14-77.12.1
php5-ldap-5.5.14-77.12.1
php5-zip-debuginfo-5.5.14-77.12.1
php5-pgsql-debuginfo-5.5.14-77.12.1
php5-sysvsem-debuginfo-5.5.14-77.12.1
php5-snmp-5.5.14-77.12.1
php5-shmop-debuginfo-5.5.14-77.12.1
php5-pdo-5.5.14-77.12.1
php5-phar-debuginfo-5.5.14-77.12.1
php5-tokenizer-debuginfo-5.5.14-77.12.1
php5-intl-debuginfo-5.5.14-77.12.1
php5-mbstring-debuginfo-5.5.14-77.12.1
php5-dba-debuginfo-5.5.14-77.12.1
php5-dom-5.5.14-77.12.1
php5-xmlwriter-debuginfo-5.5.14-77.12.1
php5-gettext-5.5.14-77.12.1
php5-sysvmsg-5.5.14-77.12.1
php5-mcrypt-debuginfo-5.5.14-77.12.1
php5-suhosin-debuginfo-5.5.14-77.12.1
php5-json-debuginfo-5.5.14-77.12.1
php5-exif-5.5.14-77.12.1
php5-gmp-debuginfo-5.5.14-77.12.1
php5-firebird-debuginfo-5.5.14-77.12.1
php5-enchant-5.5.14-77.12.1
php5-curl-5.5.14-77.12.1
php5-5.5.14-77.12.1
php5-enchant-debuginfo-5.5.14-77.12.1
php5-debugsource-5.5.14-77.12.1
php5-fileinfo-5.5.14-77.12.1
php5-fastcgi-5.5.14-77.12.1
php5-dba-5.5.14-77.12.1
php5-readline-debuginfo-5.5.14-77.12.1
php5-json-5.5.14-77.12.1
php5-xmlrpc-debuginfo-5.5.14-77.12.1
php5-xsl-5.5.14-77.12.1
php5-gmp-5.5.14-77.12.1
php5-xmlreader-debuginfo-5.5.14-77.12.1

noarch
php5-pear-5.5.14-77.12.1

x86_64
php5-snmp-debuginfo-5.5.14-77.12.1
php5-ctype-debuginfo-5.5.14-77.12.1
php5-bcmath-5.5.14-77.12.1
php5-shmop-5.5.14-77.12.1
php5-ctype-5.5.14-77.12.1
apache2-mod_php5-5.5.14-77.12.1
php5-calendar-5.5.14-77.12.1
php5-sqlite-debuginfo-5.5.14-77.12.1
php5-curl-debuginfo-5.5.14-77.12.1
php5-firebird-5.5.14-77.12.1
php5-wddx-5.5.14-77.12.1
php5-soap-5.5.14-77.12.1
php5-fpm-5.5.14-77.12.1
php5-mcrypt-5.5.14-77.12.1
php5-sysvshm-debuginfo-5.5.14-77.12.1
php5-fpm-debuginfo-5.5.14-77.12.1
apache2-mod_php5-debuginfo-5.5.14-77.12.1

php5-pspell-debuginfo-5.5.14-77.12.1
php5-xmlwriter-5.5.14-77.12.1
php5-posix-debuginfo-5.5.14-77.12.1
php5-sysvshm-5.5.14-77.12.1
php5-pcntl-debuginfo-5.5.14-77.12.1
php5-gd-debuginfo-5.5.14-77.12.1
php5-odbc-debuginfo-5.5.14-77.12.1
php5-soap-debuginfo-5.5.14-77.12.1
php5-zlib-5.5.14-77.12.1
php5-mysql-5.5.14-77.12.1
php5-sockets-5.5.14-77.12.1
php5-mbstring-5.5.14-77.12.1
php5-ftp-debuginfo-5.5.14-77.12.1
php5-dom-debuginfo-5.5.14-77.12.1
php5-wddx-debuginfo-5.5.14-77.12.1
php5-pspell-5.5.14-77.12.1
php5-pgsql-5.5.14-77.12.1
php5-zip-5.5.14-77.12.1
php5-ldap-debuginfo-5.5.14-77.12.1
php5-iconv-debuginfo-5.5.14-77.12.1
php5-tokenizer-5.5.14-77.12.1
php5-suhosin-5.5.14-77.12.1
php5-bz2-5.5.14-77.12.1
php5-mysql-debuginfo-5.5.14-77.12.1
php5-mssql-5.5.14-77.12.1
php5-xmlrpc-5.5.14-77.12.1
php5-bz2-debuginfo-5.5.14-77.12.1
php5-pcntl-5.5.14-77.12.1
php5-fileinfo-debuginfo-5.5.14-77.12.1
php5-sysvsem-5.5.14-77.12.1
php5-tidy-debuginfo-5.5.14-77.12.1
php5-zlib-debuginfo-5.5.14-77.12.1
php5-ftp-5.5.14-77.12.1
php5-pdo-debuginfo-5.5.14-77.12.1
php5-intl-5.5.14-77.12.1
php5-gettext-debuginfo-5.5.14-77.12.1
php5-calendar-debuginfo-5.5.14-77.12.1
php5-opcache-5.5.14-77.12.1
php5-odbc-5.5.14-77.12.1
php5-sockets-debuginfo-5.5.14-77.12.1
php5-openssl-5.5.14-77.12.1
php5-gd-5.5.14-77.12.1
php5-phar-5.5.14-77.12.1
php5-bcmath-debuginfo-5.5.14-77.12.1
php5-sqlite-5.5.14-77.12.1
php5-debuginfo-5.5.14-77.12.1
php5-imap-5.5.14-77.12.1
php5-openssl-debuginfo-5.5.14-77.12.1
php5-readline-5.5.14-77.12.1
php5-posix-5.5.14-77.12.1
php5-devel-5.5.14-77.12.1
php5-iconv-5.5.14-77.12.1
php5-imap-debuginfo-5.5.14-77.12.1
php5-exif-debuginfo-5.5.14-77.12.1
php5-tidy-5.5.14-77.12.1
php5-sysvmsg-debuginfo-5.5.14-77.12.1
php5-opcache-debuginfo-5.5.14-77.12.1
php5-fastcgi-debuginfo-5.5.14-77.12.1
php5-mssql-debuginfo-5.5.14-77.12.1
php5-xmlreader-5.5.14-77.12.1

php5-xsl-debuginfo-5.5.14-77.12.1
php5-ldap-5.5.14-77.12.1
php5-zip-debuginfo-5.5.14-77.12.1
php5-pgsql-debuginfo-5.5.14-77.12.1
php5-sysvsem-debuginfo-5.5.14-77.12.1
php5-snmp-5.5.14-77.12.1
php5-shmop-debuginfo-5.5.14-77.12.1
php5-pdo-5.5.14-77.12.1
php5-phar-debuginfo-5.5.14-77.12.1
php5-tokenizer-debuginfo-5.5.14-77.12.1
php5-intl-debuginfo-5.5.14-77.12.1
php5-mbstring-debuginfo-5.5.14-77.12.1
php5-dba-debuginfo-5.5.14-77.12.1
php5-dom-5.5.14-77.12.1
php5-xmlwriter-debuginfo-5.5.14-77.12.1
php5-gettext-5.5.14-77.12.1
php5-sysvmsg-5.5.14-77.12.1
php5-mcrypt-debuginfo-5.5.14-77.12.1
php5-suhosin-debuginfo-5.5.14-77.12.1
php5-json-debuginfo-5.5.14-77.12.1
php5-exif-5.5.14-77.12.1
php5-gmp-debuginfo-5.5.14-77.12.1
php5-firebird-debuginfo-5.5.14-77.12.1

SuSE Linux 42.3
i586
php5-pdo-5.5.14-85.1

145942 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2529-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14482

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2529-1

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-September/003250.html

SuSE SLES 12 SP2
noarch
emacs-info-24.3-25.3.1
emacs-el-24.3-25.3.1

x86_64
emacs-debuginfo-24.3-25.3.1
emacs-nox-debuginfo-24.3-25.3.1
etags-24.3-25.3.1
emacs-nox-24.3-25.3.1
emacs-x11-debuginfo-24.3-25.3.1
emacs-debugsource-24.3-25.3.1
emacs-x11-24.3-25.3.1
etags-debuginfo-24.3-25.3.1

emacs-24.3-25.3.1

SuSE SLED 12 SP3
x86_64
emacs-x11-debuginfo-24.3-25.3.1
emacs-debuginfo-24.3-25.3.1
emacs-debugsource-24.3-25.3.1
emacs-x11-24.3-25.3.1
etags-24.3-25.3.1
etags-debuginfo-24.3-25.3.1
emacs-24.3-25.3.1

noarch
emacs-info-24.3-25.3.1

SuSE SLED 12 SP2
x86_64
emacs-x11-debuginfo-24.3-25.3.1
emacs-debuginfo-24.3-25.3.1
emacs-debugsource-24.3-25.3.1
emacs-x11-24.3-25.3.1
etags-24.3-25.3.1
etags-debuginfo-24.3-25.3.1
emacs-24.3-25.3.1

noarch
emacs-info-24.3-25.3.1

SuSE SLES 12 SP3
noarch
emacs-info-24.3-25.3.1
emacs-el-24.3-25.3.1

x86_64
emacs-debuginfo-24.3-25.3.1
emacs-nox-debuginfo-24.3-25.3.1
etags-24.3-25.3.1
emacs-nox-24.3-25.3.1
emacs-x11-debuginfo-24.3-25.3.1
emacs-debugsource-24.3-25.3.1
emacs-x11-24.3-25.3.1
etags-debuginfo-24.3-25.3.1
emacs-24.3-25.3.1

145943 - SuSE Linux 42.2 openSUSE-SU-2017:2538-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2538-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00092.html

SuSE Linux 42.2
x86_64
fossil-debugsource-2.3-5.3.1
fossil-2.3-5.3.1
fossil-debuginfo-2.3-5.3.1

i586
fossil-debugsource-2.3-5.3.1
fossil-2.3-5.3.1
fossil-debuginfo-2.3-5.3.1

145944 - SuSE Linux 42.2 openSUSE-SU-2017:2540-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14316, CVE-2017-14317, CVE-2017-14318, CVE-2017-14319

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2540-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00094.html

SuSE Linux 42.2
x86_64
xen-tools-domU-4.7.3_04-11.15.1
xen-4.7.3_04-11.15.1
xen-libs-debuginfo-32bit-4.7.3_04-11.15.1
xen-libs-32bit-4.7.3_04-11.15.1
xen-debugsource-4.7.3_04-11.15.1
xen-tools-debuginfo-4.7.3_04-11.15.1
xen-doc-html-4.7.3_04-11.15.1
xen-libs-debuginfo-4.7.3_04-11.15.1
xen-devel-4.7.3_04-11.15.1
xen-tools-4.7.3_04-11.15.1
xen-tools-domU-debuginfo-4.7.3_04-11.15.1
xen-libs-4.7.3_04-11.15.1

i586
xen-tools-domU-4.7.3_04-11.15.1
xen-debugsource-4.7.3_04-11.15.1
xen-libs-debuginfo-4.7.3_04-11.15.1
xen-devel-4.7.3_04-11.15.1
xen-tools-domU-debuginfo-4.7.3_04-11.15.1
xen-libs-4.7.3_04-11.15.1

160300 - CentOS 7 CESA-2017-2788 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-2017-2788

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-September/022545.html

CentOS 7
x86_64
augeas-1.4.0-2.el7_4.1
augeas-libs-1.4.0-2.el7_4.1
augeas-devel-1.4.0-2.el7_4.1

i686
augeas-libs-1.4.0-2.el7_4.1
augeas-devel-1.4.0-2.el7_4.1

160301 - CentOS 7 CESA-2017-2771 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-2017-2771

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-September/022541.html

CentOS 7
x86_64
emacs-nox-24.3-20.el7_4
emacs-common-24.3-20.el7_4
emacs-24.3-20.el7_4

noarch
emacs-el-24.3-20.el7_4
emacs-filesystem-24.3-20.el7_4
emacs-terminal-24.3-20.el7_4

163459 - Oracle Enterprise Linux ELSA-2017-3621 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-1000365, CVE-2017-12134

Description

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

ELSA-2017-3621

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007216.html
http://oss.oracle.com/pipermail/el-errata/2017-September/007217.html

OEL7
x86_64
kernel-uek-doc-3.8.13-118.19.7.el7uek
kernel-uek-debug-3.8.13-118.19.7.el7uek
kernel-uek-devel-3.8.13-118.19.7.el7uek
dtrace-modules-3.8.13-118.19.7.el7uek-0.4.5-3.el7
kernel-uek-3.8.13-118.19.7.el7uek
kernel-uek-firmware-3.8.13-118.19.7.el7uek
kernel-uek-debug-devel-3.8.13-118.19.7.el7uek

OEL6
x86_64
kernel-uek-debug-devel-3.8.13-118.19.7.el6uek
kernel-uek-3.8.13-118.19.7.el6uek
kernel-uek-doc-3.8.13-118.19.7.el6uek
kernel-uek-debug-3.8.13-118.19.7.el6uek
dtrace-modules-3.8.13-118.19.7.el6uek-0.4.5-3.el6
kernel-uek-firmware-3.8.13-118.19.7.el6uek
kernel-uek-devel-3.8.13-118.19.7.el6uek

163460 - Oracle Enterprise Linux ELSA-2017-3622 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251, CVE-2017-1000365, CVE-2017-12134

Description

The scan detected that the host is missing the following update:
ELSA-2017-3622

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-September/007219.html
http://oss.oracle.com/pipermail/el-errata/2017-September/007218.html

OEL5
x86_64
kernel-uek-debug-devel-2.6.39-400.297.8.el5uek
kernel-uek-doc-2.6.39-400.297.8.el5uek
kernel-uek-firmware-2.6.39-400.297.8.el5uek
kernel-uek-2.6.39-400.297.8.el5uek
kernel-uek-debug-2.6.39-400.297.8.el5uek
kernel-uek-devel-2.6.39-400.297.8.el5uek

i386
kernel-uek-debug-devel-2.6.39-400.297.8.el5uek

kernel-uek-doc-2.6.39-400.297.8.el5uek
kernel-uek-debug-2.6.39-400.297.8.el5uek
kernel-uek-2.6.39-400.297.8.el5uek
kernel-uek-firmware-2.6.39-400.297.8.el5uek
kernel-uek-devel-2.6.39-400.297.8.el5uek

OEL6
x86_64
kernel-uek-firmware-2.6.39-400.297.8.el6uek
kernel-uek-doc-2.6.39-400.297.8.el6uek
kernel-uek-devel-2.6.39-400.297.8.el6uek
kernel-uek-debug-devel-2.6.39-400.297.8.el6uek
kernel-uek-2.6.39-400.297.8.el6uek
kernel-uek-debug-2.6.39-400.297.8.el6uek

i386
kernel-uek-firmware-2.6.39-400.297.8.el6uek
kernel-uek-doc-2.6.39-400.297.8.el6uek
kernel-uek-devel-2.6.39-400.297.8.el6uek
kernel-uek-debug-devel-2.6.39-400.297.8.el6uek
kernel-uek-2.6.39-400.297.8.el6uek
kernel-uek-debug-2.6.39-400.297.8.el6uek

175263 - Scientific Linux Security ERRATA Important: augeas on SL7.x x86_64 (1709-2086)

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

Risk Level: High

CVE: CVE-2017-7555

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: augeas on SL7.x x86_64 (1709-2086)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1709&L=scientific-linux-errata&F=&S=&P=2086

SL7
x86_64
augeas-debuginfo-1.4.0-2.el7_4.1
augeas-1.4.0-2.el7_4.1
augeas-libs-1.4.0-2.el7_4.1
augeas-devel-1.4.0-2.el7_4.1

185890 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3414-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10664, CVE-2017-10806, CVE-2017-10911, CVE-2017-11434, CVE-2017-12809, CVE-2017-7493, CVE-2017-8112, CVE-2017-8380, CVE-2017-9060, CVE-2017-9310, CVE-2017-9330, CVE-2017-9373, CVE-2017-9374, CVE-2017-9375, CVE-2017-9503, CVE-2017-9524

Description

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

USN-3414-2

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-September/004059.html

Ubuntu 16.04

qemu-system_2.5+dfsg-5ubuntu10.16
qemu-system-misc_2.5+dfsg-5ubuntu10.16
qemu-system-ppc_2.5+dfsg-5ubuntu10.16
qemu-system-x86_2.5+dfsg-5ubuntu10.16
qemu-system-mips_2.5+dfsg-5ubuntu10.16
qemu-system-aarch64_2.5+dfsg-5ubuntu10.16
qemu-system-arm_2.5+dfsg-5ubuntu10.16
qemu-system-sparc_2.5+dfsg-5ubuntu10.16
qemu-system-s390x_2.5+dfsg-5ubuntu10.16

Ubuntu 14.04

qemu-system-arm_2.0.0+dfsg-2ubuntu1.36
qemu-system_2.0.0+dfsg-2ubuntu1.36
qemu-system-mips_2.0.0+dfsg-2ubuntu1.36
qemu-system-ppc_2.0.0+dfsg-2ubuntu1.36
qemu-system-misc_2.0.0+dfsg-2ubuntu1.36
qemu-system-x86_2.0.0+dfsg-2ubuntu1.36
qemu-system-sparc_2.0.0+dfsg-2ubuntu1.36
qemu-system-aarch64_2.0.0+dfsg-2ubuntu1.36

Ubuntu 17.04

qemu-system-ppc_2.8+dfsg-3ubuntu2.5
qemu-system-s390x_2.8+dfsg-3ubuntu2.5
qemu-system-mips_2.8+dfsg-3ubuntu2.5
qemu-system-misc_2.8+dfsg-3ubuntu2.5
qemu-system-aarch64_2.8+dfsg-3ubuntu2.5
qemu-system-sparc_2.8+dfsg-3ubuntu2.5
qemu-system-x86_2.8+dfsg-3ubuntu2.5
qemu-system_2.8+dfsg-3ubuntu2.5
qemu-system-arm_2.8+dfsg-3ubuntu2.5

22455 - Cisco IOS Software UDP Packet Processing Denial of Service Vulnerability (CSCva95506)

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6627

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw lies in UDP processing code. Successful exploitation could allow an attacker to cause a denial of service condition.

22467 - (K11220361) F5 BIG-IP LibTIFF Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-1547

Description

A denial of service 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 denial of service vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the LibTIFF component. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

141720 - Red Hat Enterprise Linux RHSA-2017-2791 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12150, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
RHSA-2017-2791

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00050.html

RHEL6D
x86_64
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-debuginfo-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

i386
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-debuginfo-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9

samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

RHEL6S
i386
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-debuginfo-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

x86_64
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-debuginfo-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

RHEL6WS
x86_64
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-debuginfo-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

i386
samba4-4.2.10-11.el6_9

samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-debuginfo-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

141722 - Red Hat Enterprise Linux RHSA-2017-2790 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12150, CVE-2017-12151, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
RHSA-2017-2790

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00051.html

RHEL7D
x86_64
samba-test-4.6.2-11.el7_4
samba-krb5-printing-4.6.2-11.el7_4
samba-python-4.6.2-11.el7_4
samba-winbind-modules-4.6.2-11.el7_4
samba-common-libs-4.6.2-11.el7_4
samba-winbind-4.6.2-11.el7_4
libwbclient-4.6.2-11.el7_4
samba-libs-4.6.2-11.el7_4
libsmbclient-4.6.2-11.el7_4
samba-winbind-clients-4.6.2-11.el7_4
libsmbclient-devel-4.6.2-11.el7_4
samba-debuginfo-4.6.2-11.el7_4
samba-client-4.6.2-11.el7_4
libwbclient-devel-4.6.2-11.el7_4
samba-client-libs-4.6.2-11.el7_4
samba-dc-4.6.2-11.el7_4
samba-devel-4.6.2-11.el7_4
samba-winbind-krb5-locator-4.6.2-11.el7_4
samba-test-libs-4.6.2-11.el7_4
samba-common-tools-4.6.2-11.el7_4
samba-4.6.2-11.el7_4
samba-vfs-glusterfs-4.6.2-11.el7_4
samba-dc-libs-4.6.2-11.el7_4

noarch
samba-common-4.6.2-11.el7_4

samba-pidl-4.6.2-11.el7_4

RHEL7S
noarch
samba-common-4.6.2-11.el7_4
samba-pidl-4.6.2-11.el7_4

x86_64
samba-test-4.6.2-11.el7_4
samba-krb5-printing-4.6.2-11.el7_4
samba-winbind-krb5-locator-4.6.2-11.el7_4
samba-winbind-modules-4.6.2-11.el7_4
samba-common-libs-4.6.2-11.el7_4
samba-winbind-4.6.2-11.el7_4
libwbclient-4.6.2-11.el7_4
samba-python-4.6.2-11.el7_4
libsmbclient-4.6.2-11.el7_4
samba-winbind-clients-4.6.2-11.el7_4
libsmbclient-devel-4.6.2-11.el7_4
samba-debuginfo-4.6.2-11.el7_4
samba-client-4.6.2-11.el7_4
libwbclient-devel-4.6.2-11.el7_4
samba-client-libs-4.6.2-11.el7_4
samba-dc-4.6.2-11.el7_4
samba-devel-4.6.2-11.el7_4
samba-test-libs-4.6.2-11.el7_4
samba-common-tools-4.6.2-11.el7_4
samba-4.6.2-11.el7_4
samba-vfs-glusterfs-4.6.2-11.el7_4
samba-libs-4.6.2-11.el7_4
samba-dc-libs-4.6.2-11.el7_4

RHEL7WS
x86_64
samba-test-4.6.2-11.el7_4
samba-krb5-printing-4.6.2-11.el7_4
samba-winbind-krb5-locator-4.6.2-11.el7_4
samba-winbind-modules-4.6.2-11.el7_4
samba-common-libs-4.6.2-11.el7_4
samba-winbind-4.6.2-11.el7_4
libwbclient-4.6.2-11.el7_4
samba-python-4.6.2-11.el7_4
libsmbclient-4.6.2-11.el7_4
samba-winbind-clients-4.6.2-11.el7_4
libsmbclient-devel-4.6.2-11.el7_4
samba-debuginfo-4.6.2-11.el7_4
samba-client-4.6.2-11.el7_4
libwbclient-devel-4.6.2-11.el7_4
samba-client-libs-4.6.2-11.el7_4
samba-dc-4.6.2-11.el7_4
samba-devel-4.6.2-11.el7_4
samba-test-libs-4.6.2-11.el7_4
samba-common-tools-4.6.2-11.el7_4
samba-4.6.2-11.el7_4
samba-vfs-glusterfs-4.6.2-11.el7_4
samba-libs-4.6.2-11.el7_4
samba-dc-libs-4.6.2-11.el7_4

noarch
samba-common-4.6.2-11.el7_4

samba-pidl-4.6.2-11.el7_4

141724 - Red Hat Enterprise Linux RHSA-2017-2789 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12150, CVE-2017-12163, CVE-2017-2619

Description

The scan detected that the host is missing the following update:
RHSA-2017-2789

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-September/msg00052.html

RHEL6D
x86_64
samba-debuginfo-3.6.23-45.el6_9
samba-3.6.23-45.el6_9
samba-glusterfs-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9
libsmbclient-devel-3.6.23-45.el6_9
samba-swat-3.6.23-45.el6_9
samba-doc-3.6.23-45.el6_9
samba-winbind-devel-3.6.23-45.el6_9
samba-domainjoin-gui-3.6.23-45.el6_9
samba-winbind-krb5-locator-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9

i386
samba-3.6.23-45.el6_9
samba-debuginfo-3.6.23-45.el6_9
samba-winbind-devel-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9
libsmbclient-devel-3.6.23-45.el6_9
samba-swat-3.6.23-45.el6_9
samba-doc-3.6.23-45.el6_9
samba-domainjoin-gui-3.6.23-45.el6_9
samba-winbind-krb5-locator-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9

RHEL6S
i386
samba-3.6.23-45.el6_9
samba-debuginfo-3.6.23-45.el6_9
samba-winbind-devel-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9
libsmbclient-devel-3.6.23-45.el6_9

samba-swat-3.6.23-45.el6_9
samba-doc-3.6.23-45.el6_9
samba-domainjoin-gui-3.6.23-45.el6_9
samba-winbind-krb5-locator-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9

x86_64
samba-debuginfo-3.6.23-45.el6_9
samba-3.6.23-45.el6_9
samba-glusterfs-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9
libsmbclient-devel-3.6.23-45.el6_9
samba-swat-3.6.23-45.el6_9
samba-doc-3.6.23-45.el6_9
samba-winbind-devel-3.6.23-45.el6_9
samba-domainjoin-gui-3.6.23-45.el6_9
samba-winbind-krb5-locator-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9

RHEL6WS
x86_64
samba-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-debuginfo-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9

i386
samba-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-debuginfo-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9

160299 - CentOS 7 CESA-2017-2790 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2790

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-September/022546.html

CentOS 7
i686
libwbclient-devel-4.6.2-11.el7_4
samba-devel-4.6.2-11.el7_4
samba-winbind-modules-4.6.2-11.el7_4
libwbclient-4.6.2-11.el7_4
samba-client-libs-4.6.2-11.el7_4
libsmbclient-4.6.2-11.el7_4
samba-libs-4.6.2-11.el7_4
libsmbclient-devel-4.6.2-11.el7_4
samba-test-libs-4.6.2-11.el7_4

noarch
samba-common-4.6.2-11.el7_4
samba-pidl-4.6.2-11.el7_4

x86_64
samba-test-4.6.2-11.el7_4
samba-krb5-printing-4.6.2-11.el7_4
samba-python-4.6.2-11.el7_4
samba-winbind-modules-4.6.2-11.el7_4
samba-common-libs-4.6.2-11.el7_4
samba-winbind-4.6.2-11.el7_4
libwbclient-4.6.2-11.el7_4
samba-libs-4.6.2-11.el7_4
libsmbclient-4.6.2-11.el7_4
samba-winbind-clients-4.6.2-11.el7_4
libsmbclient-devel-4.6.2-11.el7_4
samba-devel-4.6.2-11.el7_4
ctdb-4.6.2-11.el7_4
samba-client-4.6.2-11.el7_4
libwbclient-devel-4.6.2-11.el7_4
samba-client-libs-4.6.2-11.el7_4
samba-dc-4.6.2-11.el7_4
samba-winbind-krb5-locator-4.6.2-11.el7_4
samba-test-libs-4.6.2-11.el7_4
ctdb-tests-4.6.2-11.el7_4
samba-common-tools-4.6.2-11.el7_4
samba-4.6.2-11.el7_4
samba-vfs-glusterfs-4.6.2-11.el7_4
samba-dc-libs-4.6.2-11.el7_4

160302 - CentOS 6 CESA-2017-2791 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2791

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-September/022544.html

CentOS 6
x86_64
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

i686
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

160303 - CentOS 6 CESA-2017-2789 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2789

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-September/022543.html

CentOS 6
x86_64
samba-3.6.23-45.el6_9
samba-winbind-devel-3.6.23-45.el6_9
samba-glusterfs-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9
libsmbclient-devel-3.6.23-45.el6_9
samba-swat-3.6.23-45.el6_9
samba-doc-3.6.23-45.el6_9
samba-domainjoin-gui-3.6.23-45.el6_9

samba-winbind-krb5-locator-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9

i686
samba-3.6.23-45.el6_9
samba-client-3.6.23-45.el6_9
samba-winbind-3.6.23-45.el6_9
samba-doc-3.6.23-45.el6_9
samba-common-3.6.23-45.el6_9
samba-winbind-krb5-locator-3.6.23-45.el6_9
samba-winbind-devel-3.6.23-45.el6_9
samba-swat-3.6.23-45.el6_9
libsmbclient-3.6.23-45.el6_9
samba-domainjoin-gui-3.6.23-45.el6_9
samba-winbind-clients-3.6.23-45.el6_9
libsmbclient-devel-3.6.23-45.el6_9

175262 - Scientific Linux Security ERRATA Moderate: samba on SL7.x x86_64 (1709-2758)

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

Risk Level: Medium

CVE: CVE-2017-12150, CVE-2017-12151, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: samba on SL7.x x86_64 (1709-2758)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1709&L=scientific-linux-errata&F=&S=&P=2758

SL7
x86_64
samba-test-4.6.2-11.el7_4
samba-krb5-printing-4.6.2-11.el7_4
samba-python-4.6.2-11.el7_4
samba-winbind-modules-4.6.2-11.el7_4
samba-common-libs-4.6.2-11.el7_4
samba-winbind-4.6.2-11.el7_4
libwbclient-4.6.2-11.el7_4
samba-libs-4.6.2-11.el7_4
libsmbclient-4.6.2-11.el7_4
samba-winbind-clients-4.6.2-11.el7_4
libsmbclient-devel-4.6.2-11.el7_4
samba-debuginfo-4.6.2-11.el7_4
samba-client-4.6.2-11.el7_4
libwbclient-devel-4.6.2-11.el7_4
samba-client-libs-4.6.2-11.el7_4
samba-dc-4.6.2-11.el7_4
samba-devel-4.6.2-11.el7_4
samba-winbind-krb5-locator-4.6.2-11.el7_4
samba-test-libs-4.6.2-11.el7_4
samba-common-tools-4.6.2-11.el7_4
samba-4.6.2-11.el7_4

samba-vfs-glusterfs-4.6.2-11.el7_4
samba-dc-libs-4.6.2-11.el7_4

noarch
samba-common-4.6.2-11.el7_4
samba-pidl-4.6.2-11.el7_4

175264 - Scientific Linux Security ERRATA Moderate: samba4 on SL6.x i386/x86_64 (1709-2411)

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

Risk Level: Medium

CVE: CVE-2017-12150, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: samba4 on SL6.x i386/x86_64 (1709-2411)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1709&L=scientific-linux-errata&F=&S=&P=2411

SL6
x86_64
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-debuginfo-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

i386
samba4-4.2.10-11.el6_9
samba4-libs-4.2.10-11.el6_9
samba4-pidl-4.2.10-11.el6_9
samba4-debuginfo-4.2.10-11.el6_9
samba4-common-4.2.10-11.el6_9
samba4-winbind-krb5-locator-4.2.10-11.el6_9
samba4-devel-4.2.10-11.el6_9
samba4-winbind-clients-4.2.10-11.el6_9
samba4-python-4.2.10-11.el6_9
samba4-client-4.2.10-11.el6_9
samba4-dc-libs-4.2.10-11.el6_9
samba4-dc-4.2.10-11.el6_9
samba4-winbind-4.2.10-11.el6_9
samba4-test-4.2.10-11.el6_9

192656 - Fedora Linux 26 FEDORA-2017-7699952c1b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13735

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7699952c1b

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/2017/9/?count=200&page=1

Fedora Core 26

mingw-LibRaw-0.18.4-1.fc26

192658 - Fedora Linux 26 FEDORA-2017-c89d94d812 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10683, CVE-2017-11126, CVE-2017-12797, CVE-2017-9545

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c89d94d812

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/2017/9/?count=200&page=1

Fedora Core 26

mpg123-1.25.6-1.fc26

192659 - Fedora Linux 25 FEDORA-2017-d361de1a65 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6362

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d361de1a65

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/2017/9/?count=200&page=1

Fedora Core 25

libwmf-0.2.8.4-53.fc25

22465 - IBM DB2 Sensitive Information Exposure In Error Log Vulnerability (swg22005740)

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

Risk Level: Medium

CVE: CVE-2017-1434

Description

An information disclosure vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

An information disclosure vulnerability is present in some versions of IBM DB2. The flaw lies in error logging. Successful exploitation could allow an attacker to retrieve sensitive data.

145935 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2546-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14107

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2546-1

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-September/003255.html

SuSE SLES 12 SP2
x86_64
libzip2-0.11.1-13.3.1
libzip-debugsource-0.11.1-13.3.1
libzip-debuginfo-0.11.1-13.3.1
libzip2-debuginfo-0.11.1-13.3.1

SuSE SLED 12 SP3
x86_64
libzip2-0.11.1-13.3.1
libzip-debugsource-0.11.1-13.3.1
libzip-debuginfo-0.11.1-13.3.1
libzip2-debuginfo-0.11.1-13.3.1

SuSE SLED 12 SP2
x86_64
libzip2-0.11.1-13.3.1
libzip-debugsource-0.11.1-13.3.1
libzip-debuginfo-0.11.1-13.3.1
libzip2-debuginfo-0.11.1-13.3.1

SuSE SLES 12 SP3
x86_64
libzip2-0.11.1-13.3.1
libzip-debugsource-0.11.1-13.3.1
libzip-debuginfo-0.11.1-13.3.1
libzip2-debuginfo-0.11.1-13.3.1

145938 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2550-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14107

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2550-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00096.html

SuSE Linux 42.2
x86_64
libzip-0.11.1-6.3.1
libzip2-debuginfo-32bit-0.11.1-6.3.1
libzip2-32bit-0.11.1-6.3.1
libzip-debugsource-0.11.1-6.3.1
libzip2-debuginfo-0.11.1-6.3.1
libzip-devel-0.11.1-6.3.1
libzip2-0.11.1-6.3.1
libzip-debuginfo-0.11.1-6.3.1

i586
libzip-0.11.1-6.3.1
libzip-debugsource-0.11.1-6.3.1
libzip2-debuginfo-0.11.1-6.3.1
libzip-devel-0.11.1-6.3.1
libzip2-0.11.1-6.3.1
libzip-debuginfo-0.11.1-6.3.1

SuSE Linux 42.3
x86_64
libzip-debugsource-0.11.1-9.1
libzip2-0.11.1-9.1
libzip-devel-0.11.1-9.1
libzip-0.11.1-9.1
libzip2-debuginfo-32bit-0.11.1-9.1
libzip2-32bit-0.11.1-9.1
libzip2-debuginfo-0.11.1-9.1
libzip-debuginfo-0.11.1-9.1

i586
libzip-debugsource-0.11.1-9.1
libzip2-0.11.1-9.1
libzip-devel-0.11.1-9.1

libzip-0.11.1-9.1
libzip2-debuginfo-0.11.1-9.1
libzip-debuginfo-0.11.1-9.1

130889 - Debian Linux 8.0, 9.0 DSA-3982-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12837, CVE-2017-12883

Description

The scan detected that the host is missing the following update:
DSA-3982-1

Observation

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

http://www.debian.org/security/2017/dsa-3982

Debian 8.0
all
perl_5.20.2-3+deb8u9

Debian 9.0
all
perl_5.24.1-3+deb9u2

130891 - Debian Linux 8.0, 9.0 DSA-3980-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-9798

Description

The scan detected that the host is missing the following update:
DSA-3980-1

Observation

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

http://www.debian.org/security/2017/dsa-3980

Debian 8.0
all
apache2_2.4.10-10+deb8u11

Debian 9.0
all
apache2_2.4.25-3+deb9u3

145940 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2537-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2923, CVE-2017-2924

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2537-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00091.html

SuSE Linux 42.2
x86_64
libfreexl1-debuginfo-1.0.4-2.3.1
freexl-debugsource-1.0.4-2.3.1
libfreexl1-1.0.4-2.3.1
freexl-devel-1.0.4-2.3.1

i586
libfreexl1-debuginfo-1.0.4-2.3.1
freexl-debugsource-1.0.4-2.3.1
libfreexl1-1.0.4-2.3.1
freexl-devel-1.0.4-2.3.1

SuSE Linux 42.3
x86_64
libfreexl1-1.0.4-5.1
libfreexl1-debuginfo-1.0.4-5.1
freexl-debugsource-1.0.4-5.1
freexl-devel-1.0.4-5.1

i586
libfreexl1-1.0.4-5.1
libfreexl1-debuginfo-1.0.4-5.1
freexl-debugsource-1.0.4-5.1
freexl-devel-1.0.4-5.1

185889 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3426-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12150, CVE-2017-12151, CVE-2017-12163

Description

The scan detected that the host is missing the following update:
USN-3426-1

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-September/004060.html

Ubuntu 16.04

samba_4.3.11+dfsg-0ubuntu0.16.04.11

Ubuntu 14.04

samba_4.3.11+dfsg-0ubuntu0.14.04.12

Ubuntu 17.04

samba_4.5.8+dfsg-0ubuntu0.17.04.7

192657 - Fedora Linux 25 FEDORA-2017-e07d7fb18e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000251, CVE-2017-12153, CVE-2017-12154

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e07d7fb18e

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/2017/9/?count=200&page=1

Fedora Core 25

kernel-4.12.13-200.fc25

22466 - (K04253390) F5 BIG-IP Apache Xerces Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Informational

CVE: CVE-2016-2099

Description

A vulnerability is present in some versions of F5's 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's BIG-IP Products. The flaw lies in the Apache Xerces. Successful exploitation could allow an attacker to cause a denial-of-service condition, retrieve sensitive data or other unspecified impact on target system.

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.