2017-SEP-14
FSL version 7.5.959

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

130874 - Debian Linux 8.0, 9.0 DSA-3969-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10912, CVE-2017-10913, CVE-2017-10914, CVE-2017-10915, CVE-2017-10916, CVE-2017-10917, CVE-2017-10918, CVE-2017-10919, CVE-2017-10920, CVE-2017-10921, CVE-2017-10922, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855

Description

The scan detected that the host is missing the following update:
DSA-3969-1

Observation

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

http://www.debian.org/security/2017/dsa-3969

Debian 8.0
all
xen-system-arm64_4.4.1-9+deb8u10
libxen-4.4_4.4.1-9+deb8u10
xen-system-armhf_4.4.1-9+deb8u10
xen-system-amd64_4.4.1-9+deb8u10
xen-hypervisor-4.4-amd64_4.4.1-9+deb8u10
xen-hypervisor-4.4-armhf_4.4.1-9+deb8u10
xen-utils-4.4_4.4.1-9+deb8u10
libxenstore3.0_4.4.1-9+deb8u10
xen-utils-common_4.4.1-9+deb8u10
libxen-dev_4.4.1-9+deb8u10
xen-hypervisor-4.4-arm64_4.4.1-9+deb8u10
xenstore-utils_4.4.1-9+deb8u10

Debian 9.0
all
xen-utils-4.8_4.8.1-1+deb9u3
xen-system-amd64_4.8.1-1+deb9u3
xen-system-arm64_4.8.1-1+deb9u3
xen-system-armhf_4.8.1-1+deb9u3
xen-hypervisor-4.8-armhf_4.8.1-1+deb9u3
libxenstore3.0_4.8.1-1+deb9u3
xen-hypervisor-4.8-arm64_4.8.1-1+deb9u3
xen-utils-common_4.8.1-1+deb9u3
xenstore-utils_4.8.1-1+deb9u3
libxen-4.8_4.8.1-1+deb9u3
libxen-dev_4.8.1-1+deb9u3

xen-hypervisor-4.8-amd64_4.8.1-1+deb9u3

145906 - SuSE SLES 11 SP4 SUSE-SU-2017:2389-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9922, CVE-2016-10277, CVE-2017-1000363, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-11176, CVE-2017-11473, CVE-2017-2647, CVE-2017-6951, CVE-2017-7482, CVE-2017-7487, CVE-2017-7533, CVE-2017-7542, CVE-2017-8890, CVE-2017-8924, CVE-2017-8925, 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:
SUSE-SU-2017:2389-1

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/003193.html

SuSE SLES 11 SP4
i586
kernel-trace-devel-3.0.101-108.7.1
kernel-xen-base-3.0.101-108.7.1
cluster-network-kmp-pae-1.4_3.0.101_108.7-2.32.2.14
drbd-utils-8.4.4-0.27.2.1
kernel-trace-3.0.101-108.7.1
kernel-default-base-3.0.101-108.7.1
kernel-default-3.0.101-108.7.1
ocfs2-kmp-default-1.6_3.0.101_108.7-0.28.3.4
kernel-syms-3.0.101-108.7.1
kernel-ec2-3.0.101-108.7.1
ocfs2-kmp-trace-1.6_3.0.101_108.7-0.28.3.4
gfs2-kmp-trace-2_3.0.101_108.7-0.24.2.14
drbd-udev-8.4.4-0.27.2.1
kernel-trace-base-3.0.101-108.7.1
drbd-kmp-pae-8.4.4_3.0.101_108.7-0.27.2.13
kernel-ec2-base-3.0.101-108.7.1
cluster-network-kmp-xen-1.4_3.0.101_108.7-2.32.2.14
gfs2-kmp-xen-2_3.0.101_108.7-0.24.2.14
cluster-network-kmp-default-1.4_3.0.101_108.7-2.32.2.14
kernel-source-3.0.101-108.7.1
drbd-heartbeat-8.4.4-0.27.2.1
drbd-8.4.4-0.27.2.1
gfs2-kmp-pae-2_3.0.101_108.7-0.24.2.14
kernel-ec2-devel-3.0.101-108.7.1
gfs2-kmp-default-2_3.0.101_108.7-0.24.2.14
kernel-xen-devel-3.0.101-108.7.1
ocfs2-kmp-xen-1.6_3.0.101_108.7-0.28.3.4
drbd-bash-completion-8.4.4-0.27.2.1
kernel-pae-devel-3.0.101-108.7.1
drbd-kmp-default-8.4.4_3.0.101_108.7-0.27.2.13
kernel-pae-base-3.0.101-108.7.1
kernel-xen-3.0.101-108.7.1
drbd-pacemaker-8.4.4-0.27.2.1
cluster-network-kmp-trace-1.4_3.0.101_108.7-2.32.2.14
kernel-pae-3.0.101-108.7.1
kernel-default-devel-3.0.101-108.7.1

drbd-kmp-trace-8.4.4_3.0.101_108.7-0.27.2.13
drbd-kmp-xen-8.4.4_3.0.101_108.7-0.27.2.13
ocfs2-kmp-pae-1.6_3.0.101_108.7-0.28.3.4

x86_64
kernel-trace-devel-3.0.101-108.7.1
kernel-xen-base-3.0.101-108.7.1
drbd-utils-8.4.4-0.27.2.1
kernel-trace-3.0.101-108.7.1
kernel-default-base-3.0.101-108.7.1
drbd-kmp-xen-8.4.4_3.0.101_108.7-0.27.2.13
kernel-syms-3.0.101-108.7.1
ocfs2-kmp-default-1.6_3.0.101_108.7-0.28.3.4
gfs2-kmp-rt_trace-2_3.0.101_rt130_68-0.24.2.14
kernel-ec2-3.0.101-108.7.1
ocfs2-kmp-trace-1.6_3.0.101_108.7-0.28.3.4
gfs2-kmp-trace-2_3.0.101_108.7-0.24.2.14
gfs2-kmp-rt-2_3.0.101_rt130_68-0.24.2.14
drbd-udev-8.4.4-0.27.2.1
kernel-trace-base-3.0.101-108.7.1
kernel-ec2-base-3.0.101-108.7.1
cluster-network-kmp-xen-1.4_3.0.101_108.7-2.32.2.14
drbd-kmp-rt_trace-8.4.4_3.0.101_rt130_68-0.27.2.13
gfs2-kmp-xen-2_3.0.101_108.7-0.24.2.14
cluster-network-kmp-rt_trace-1.4_3.0.101_rt130_68-2.32.2.14
kernel-source-3.0.101-108.7.1
ocfs2-kmp-rt_trace-1.6_3.0.101_rt130_68-0.28.3.4
drbd-heartbeat-8.4.4-0.27.2.1
ocfs2-kmp-rt-1.6_3.0.101_rt130_68-0.28.3.4
drbd-8.4.4-0.27.2.1
drbd-xen-8.4.4-0.27.2.1
kernel-ec2-devel-3.0.101-108.7.1
gfs2-kmp-default-2_3.0.101_108.7-0.24.2.14
kernel-xen-devel-3.0.101-108.7.1
ocfs2-kmp-xen-1.6_3.0.101_108.7-0.28.3.4
cluster-network-kmp-default-1.4_3.0.101_108.7-2.32.2.14
drbd-kmp-default-8.4.4_3.0.101_108.7-0.27.2.13
kernel-xen-3.0.101-108.7.1
drbd-pacemaker-8.4.4-0.27.2.1
cluster-network-kmp-trace-1.4_3.0.101_108.7-2.32.2.14
cluster-network-kmp-rt-1.4_3.0.101_rt130_68-2.32.2.14
drbd-bash-completion-8.4.4-0.27.2.1
kernel-default-devel-3.0.101-108.7.1
drbd-kmp-trace-8.4.4_3.0.101_108.7-0.27.2.13
drbd-kmp-rt-8.4.4_3.0.101_rt130_68-0.27.2.13
kernel-default-3.0.101-108.7.1

22351 - (K12401251) F5 BIG-IP File Validation Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-8022

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 Configuration Utility component. Successful exploitation could allow an attacker to escalate privileges.

141704 - Red Hat Enterprise Linux RHSA-2017-2702 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11281, CVE-2017-11282

Description

The scan detected that the host is missing the following update:
RHSA-2017-2702

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/msg00029.html

RHEL6D
x86_64
flash-plugin-27.0.0.130-1.el6_9

i386
flash-plugin-27.0.0.130-1.el6_9

RHEL6S
x86_64
flash-plugin-27.0.0.130-1.el6_9

i386
flash-plugin-27.0.0.130-1.el6_9

RHEL6WS
x86_64
flash-plugin-27.0.0.130-1.el6_9

i386
flash-plugin-27.0.0.130-1.el6_9

22347 - (SB10208) McAfee ePolicy Orchestrator Multiple Java Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-10102, CVE-2017-10135, CVE-2017-10198

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 Java components. Successful exploitation could allow an attacker to compromise Java SE.

22349 - Wireshark Multiple Vulnerabilities Prior To 2.2.9

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

Risk Level: High

CVE: CVE-2017-13766, CVE-2017-13767

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

22443 - (K51390683) F5 BIG-IP PHP Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5094, CVE-2016-5095

Description

Multiple vulnerabilities are 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.

Multiple vulnerabilities are present in some versions of F5's BIG-IP Products. The flaws lie in the Configuration utility. Successful exploitation could allow an attacker to execute arbitrary code or to cause a denial of service condition.

22444 - Wireshark Multiple Vulnerabilities Prior To 2.4.1

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

Risk Level: High

CVE: CVE-2017-13764, CVE-2017-13765, CVE-2017-13766, CVE-2017-13767

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

130878 - Debian Linux 8.0, 9.0 DSA-3971-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, CVE-2017-12894, CVE-2017-

12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004, CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010, CVE-2017-13011, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016, CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022, CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028, CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034, CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040, CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046, CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052, CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689, CVE-2017-13690, CVE-2017-13725

Description

The scan detected that the host is missing the following update:
DSA-3971-1

Observation

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

http://www.debian.org/security/2017/dsa-3971

Debian 8.0
all
tcpdump_4.9.2-1~deb8u1

Debian 9.0
all
tcpdump_4.9.2-1~deb9u1

130880 - Debian Linux 9.0 DSA-3966-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-9096, CVE-2016-7798, CVE-2017-0899, CVE-2017-0900, CVE-2017-0901, CVE-2017-0902, CVE-2017-14064

Description

The scan detected that the host is missing the following update:
DSA-3966-1

Observation

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

http://www.debian.org/security/2017/dsa-3966

Debian 9.0
all
ruby2.3_2.3.3-1+deb9u1

141703 - Red Hat Enterprise Linux RHSA-2017-2681 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
RHSA-2017-2681

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/msg00027.html

RHEL6D
i386
python-perf-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-debuginfo-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6
kernel-debuginfo-common-i686-2.6.32-696.10.2.el6
kernel-2.6.32-696.10.2.el6
kernel-debug-debuginfo-2.6.32-696.10.2.el6
perf-debuginfo-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-debuginfo-2.6.32-696.10.2.el6

noarch
kernel-firmware-2.6.32-696.10.2.el6
kernel-doc-2.6.32-696.10.2.el6
kernel-abi-whitelists-2.6.32-696.10.2.el6

x86_64
kernel-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
perf-debuginfo-2.6.32-696.10.2.el6
kernel-debuginfo-common-x86_64-2.6.32-696.10.2.el6
kernel-debug-debuginfo-2.6.32-696.10.2.el6
kernel-debuginfo-common-i686-2.6.32-696.10.2.el6
python-perf-2.6.32-696.10.2.el6
python-perf-debuginfo-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
kernel-debuginfo-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6

RHEL6S
i386
python-perf-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-debuginfo-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6
kernel-debuginfo-common-i686-2.6.32-696.10.2.el6
kernel-2.6.32-696.10.2.el6
kernel-debug-debuginfo-2.6.32-696.10.2.el6
perf-debuginfo-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6

kernel-debuginfo-2.6.32-696.10.2.el6

noarch
kernel-firmware-2.6.32-696.10.2.el6
kernel-doc-2.6.32-696.10.2.el6
kernel-abi-whitelists-2.6.32-696.10.2.el6

x86_64
kernel-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
perf-debuginfo-2.6.32-696.10.2.el6
kernel-debuginfo-common-x86_64-2.6.32-696.10.2.el6
kernel-debug-debuginfo-2.6.32-696.10.2.el6
kernel-debuginfo-common-i686-2.6.32-696.10.2.el6
python-perf-2.6.32-696.10.2.el6
python-perf-debuginfo-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
kernel-debuginfo-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6

RHEL6WS
i386
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-debuginfo-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6
kernel-debuginfo-common-i686-2.6.32-696.10.2.el6
kernel-2.6.32-696.10.2.el6
kernel-debug-debuginfo-2.6.32-696.10.2.el6
perf-debuginfo-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-debuginfo-2.6.32-696.10.2.el6

noarch
kernel-firmware-2.6.32-696.10.2.el6
kernel-doc-2.6.32-696.10.2.el6
kernel-abi-whitelists-2.6.32-696.10.2.el6

x86_64
kernel-debuginfo-common-x86_64-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-debuginfo-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6
kernel-debuginfo-common-i686-2.6.32-696.10.2.el6
kernel-2.6.32-696.10.2.el6
kernel-debug-debuginfo-2.6.32-696.10.2.el6
perf-debuginfo-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-debuginfo-2.6.32-696.10.2.el6

141705 - Red Hat Enterprise Linux RHSA-2017-2678 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux 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:
RHSA-2017-2678

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/msg00018.html

RHEL6_7S
x86_64
rh-postgresql94-postgresql-server-9.4.14-1.el6
rh-postgresql94-postgresql-pltcl-9.4.14-1.el6
rh-postgresql94-postgresql-devel-9.4.14-1.el6
rh-postgresql94-postgresql-plperl-9.4.14-1.el6
rh-postgresql94-postgresql-upgrade-9.4.14-1.el6
rh-postgresql94-postgresql-debuginfo-9.4.14-1.el6
rh-postgresql94-postgresql-test-9.4.14-1.el6
rh-postgresql94-postgresql-docs-9.4.14-1.el6
rh-postgresql94-postgresql-static-9.4.14-1.el6
rh-postgresql94-postgresql-contrib-9.4.14-1.el6
rh-postgresql94-postgresql-plpython-9.4.14-1.el6
rh-postgresql94-postgresql-9.4.14-1.el6
rh-postgresql94-postgresql-libs-9.4.14-1.el6

RHEL6S
x86_64
rh-postgresql94-postgresql-server-9.4.14-1.el6
rh-postgresql94-postgresql-pltcl-9.4.14-1.el6
rh-postgresql94-postgresql-devel-9.4.14-1.el6
rh-postgresql94-postgresql-plperl-9.4.14-1.el6
rh-postgresql94-postgresql-upgrade-9.4.14-1.el6
rh-postgresql94-postgresql-debuginfo-9.4.14-1.el6
rh-postgresql94-postgresql-test-9.4.14-1.el6
rh-postgresql94-postgresql-docs-9.4.14-1.el6
rh-postgresql94-postgresql-static-9.4.14-1.el6
rh-postgresql94-postgresql-contrib-9.4.14-1.el6
rh-postgresql94-postgresql-plpython-9.4.14-1.el6
rh-postgresql94-postgresql-9.4.14-1.el6
rh-postgresql94-postgresql-libs-9.4.14-1.el6

RHEL6WS
x86_64
rh-postgresql94-postgresql-server-9.4.14-1.el6
rh-postgresql94-postgresql-pltcl-9.4.14-1.el6
rh-postgresql94-postgresql-devel-9.4.14-1.el6
rh-postgresql94-postgresql-plperl-9.4.14-1.el6
rh-postgresql94-postgresql-upgrade-9.4.14-1.el6
rh-postgresql94-postgresql-debuginfo-9.4.14-1.el6
rh-postgresql94-postgresql-test-9.4.14-1.el6
rh-postgresql94-postgresql-docs-9.4.14-1.el6
rh-postgresql94-postgresql-static-9.4.14-1.el6
rh-postgresql94-postgresql-contrib-9.4.14-1.el6
rh-postgresql94-postgresql-plpython-9.4.14-1.el6
rh-postgresql94-postgresql-9.4.14-1.el6
rh-postgresql94-postgresql-libs-9.4.14-1.el6

RHEL7S
x86_64
rh-postgresql94-postgresql-static-9.4.14-1.el7
rh-postgresql94-postgresql-docs-9.4.14-1.el7
rh-postgresql94-postgresql-plpython-9.4.14-1.el7
rh-postgresql94-postgresql-devel-9.4.14-1.el7
rh-postgresql94-postgresql-pltcl-9.4.14-1.el7
rh-postgresql94-postgresql-debuginfo-9.4.14-1.el7
rh-postgresql94-postgresql-plperl-9.4.14-1.el7
rh-postgresql94-postgresql-upgrade-9.4.14-1.el7
rh-postgresql94-postgresql-libs-9.4.14-1.el7
rh-postgresql94-postgresql-test-9.4.14-1.el7
rh-postgresql94-postgresql-server-9.4.14-1.el7
rh-postgresql94-postgresql-contrib-9.4.14-1.el7
rh-postgresql94-postgresql-9.4.14-1.el7

RHEL7WS
x86_64
rh-postgresql94-postgresql-static-9.4.14-1.el7
rh-postgresql94-postgresql-docs-9.4.14-1.el7
rh-postgresql94-postgresql-plpython-9.4.14-1.el7
rh-postgresql94-postgresql-devel-9.4.14-1.el7
rh-postgresql94-postgresql-pltcl-9.4.14-1.el7
rh-postgresql94-postgresql-debuginfo-9.4.14-1.el7
rh-postgresql94-postgresql-plperl-9.4.14-1.el7
rh-postgresql94-postgresql-upgrade-9.4.14-1.el7
rh-postgresql94-postgresql-libs-9.4.14-1.el7
rh-postgresql94-postgresql-test-9.4.14-1.el7
rh-postgresql94-postgresql-server-9.4.14-1.el7
rh-postgresql94-postgresql-contrib-9.4.14-1.el7
rh-postgresql94-postgresql-9.4.14-1.el7

141706 - Red Hat Enterprise Linux RHSA-2017-2677 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux 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:
RHSA-2017-2677

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/msg00017.html

RHEL6_7S
x86_64
rh-postgresql95-postgresql-server-9.5.9-1.el6
rh-postgresql95-postgresql-plperl-9.5.9-1.el6
rh-postgresql95-postgresql-devel-9.5.9-1.el6
rh-postgresql95-postgresql-docs-9.5.9-1.el6
rh-postgresql95-postgresql-static-9.5.9-1.el6
rh-postgresql95-postgresql-plpython-9.5.9-1.el6
rh-postgresql95-postgresql-contrib-9.5.9-1.el6
rh-postgresql95-postgresql-test-9.5.9-1.el6

rh-postgresql95-postgresql-libs-9.5.9-1.el6
rh-postgresql95-postgresql-9.5.9-1.el6
rh-postgresql95-postgresql-debuginfo-9.5.9-1.el6
rh-postgresql95-postgresql-pltcl-9.5.9-1.el6

RHEL6S
x86_64
rh-postgresql95-postgresql-server-9.5.9-1.el6
rh-postgresql95-postgresql-plperl-9.5.9-1.el6
rh-postgresql95-postgresql-devel-9.5.9-1.el6
rh-postgresql95-postgresql-docs-9.5.9-1.el6
rh-postgresql95-postgresql-static-9.5.9-1.el6
rh-postgresql95-postgresql-plpython-9.5.9-1.el6
rh-postgresql95-postgresql-contrib-9.5.9-1.el6
rh-postgresql95-postgresql-test-9.5.9-1.el6
rh-postgresql95-postgresql-libs-9.5.9-1.el6
rh-postgresql95-postgresql-9.5.9-1.el6
rh-postgresql95-postgresql-debuginfo-9.5.9-1.el6
rh-postgresql95-postgresql-pltcl-9.5.9-1.el6

RHEL6WS
x86_64
rh-postgresql95-postgresql-server-9.5.9-1.el6
rh-postgresql95-postgresql-plperl-9.5.9-1.el6
rh-postgresql95-postgresql-devel-9.5.9-1.el6
rh-postgresql95-postgresql-docs-9.5.9-1.el6
rh-postgresql95-postgresql-static-9.5.9-1.el6
rh-postgresql95-postgresql-plpython-9.5.9-1.el6
rh-postgresql95-postgresql-contrib-9.5.9-1.el6
rh-postgresql95-postgresql-test-9.5.9-1.el6
rh-postgresql95-postgresql-libs-9.5.9-1.el6
rh-postgresql95-postgresql-9.5.9-1.el6
rh-postgresql95-postgresql-debuginfo-9.5.9-1.el6
rh-postgresql95-postgresql-pltcl-9.5.9-1.el6

RHEL7S
x86_64
rh-postgresql95-postgresql-test-9.5.9-1.el7
rh-postgresql95-postgresql-static-9.5.9-1.el7
rh-postgresql95-postgresql-plperl-9.5.9-1.el7
rh-postgresql95-postgresql-pltcl-9.5.9-1.el7
rh-postgresql95-postgresql-docs-9.5.9-1.el7
rh-postgresql95-postgresql-plpython-9.5.9-1.el7
rh-postgresql95-postgresql-devel-9.5.9-1.el7
rh-postgresql95-postgresql-9.5.9-1.el7
rh-postgresql95-postgresql-debuginfo-9.5.9-1.el7
rh-postgresql95-postgresql-contrib-9.5.9-1.el7
rh-postgresql95-postgresql-libs-9.5.9-1.el7
rh-postgresql95-postgresql-server-9.5.9-1.el7

RHEL7WS
x86_64
rh-postgresql95-postgresql-test-9.5.9-1.el7
rh-postgresql95-postgresql-static-9.5.9-1.el7
rh-postgresql95-postgresql-plperl-9.5.9-1.el7
rh-postgresql95-postgresql-pltcl-9.5.9-1.el7
rh-postgresql95-postgresql-docs-9.5.9-1.el7
rh-postgresql95-postgresql-plpython-9.5.9-1.el7
rh-postgresql95-postgresql-devel-9.5.9-1.el7
rh-postgresql95-postgresql-9.5.9-1.el7

rh-postgresql95-postgresql-debuginfo-9.5.9-1.el7
rh-postgresql95-postgresql-contrib-9.5.9-1.el7
rh-postgresql95-postgresql-libs-9.5.9-1.el7
rh-postgresql95-postgresql-server-9.5.9-1.el7

141708 - Red Hat Enterprise Linux RHSA-2017-2682 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
RHSA-2017-2682

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/msg00025.html

RHEL6_7S
i386
perf-2.6.32-573.45.2.el6
perf-debuginfo-2.6.32-573.45.2.el6
kernel-devel-2.6.32-573.45.2.el6
kernel-debuginfo-2.6.32-573.45.2.el6
kernel-headers-2.6.32-573.45.2.el6
kernel-debuginfo-common-i686-2.6.32-573.45.2.el6
python-perf-2.6.32-573.45.2.el6
python-perf-debuginfo-2.6.32-573.45.2.el6
kernel-debug-devel-2.6.32-573.45.2.el6
kernel-debug-debuginfo-2.6.32-573.45.2.el6
kernel-debug-2.6.32-573.45.2.el6
kernel-2.6.32-573.45.2.el6

noarch
kernel-doc-2.6.32-573.45.2.el6
kernel-abi-whitelists-2.6.32-573.45.2.el6
kernel-firmware-2.6.32-573.45.2.el6

x86_64
kernel-2.6.32-573.45.2.el6
perf-debuginfo-2.6.32-573.45.2.el6
kernel-debug-debuginfo-2.6.32-573.45.2.el6
kernel-devel-2.6.32-573.45.2.el6
perf-2.6.32-573.45.2.el6
python-perf-debuginfo-2.6.32-573.45.2.el6
kernel-headers-2.6.32-573.45.2.el6
kernel-debuginfo-common-x86_64-2.6.32-573.45.2.el6
kernel-debug-devel-2.6.32-573.45.2.el6
kernel-debug-2.6.32-573.45.2.el6
python-perf-2.6.32-573.45.2.el6
kernel-debuginfo-common-i686-2.6.32-573.45.2.el6
kernel-debuginfo-2.6.32-573.45.2.el6

141709 - Red Hat Enterprise Linux RHSA-2017-2707 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
RHSA-2017-2707

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/msg00033.html

RHEL6_5S
x86_64
perf-debuginfo-2.6.32-431.84.1.el6
python-perf-2.6.32-431.84.1.el6
kernel-debug-2.6.32-431.84.1.el6
kernel-devel-2.6.32-431.84.1.el6
kernel-debug-debuginfo-2.6.32-431.84.1.el6
kernel-2.6.32-431.84.1.el6
perf-2.6.32-431.84.1.el6
kernel-debug-devel-2.6.32-431.84.1.el6
python-perf-debuginfo-2.6.32-431.84.1.el6
kernel-debuginfo-common-x86_64-2.6.32-431.84.1.el6
kernel-headers-2.6.32-431.84.1.el6
kernel-debuginfo-2.6.32-431.84.1.el6

noarch
kernel-doc-2.6.32-431.84.1.el6
kernel-firmware-2.6.32-431.84.1.el6
kernel-abi-whitelists-2.6.32-431.84.1.el6

141711 - Red Hat Enterprise Linux RHSA-2017-2683 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
RHSA-2017-2683

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/msg00019.html

RHEL6_4S
x86_64
python-perf-2.6.32-358.83.1.el6
python-perf-debuginfo-2.6.32-358.83.1.el6
kernel-debuginfo-2.6.32-358.83.1.el6
kernel-debuginfo-common-x86_64-2.6.32-358.83.1.el6

kernel-debug-2.6.32-358.83.1.el6
perf-debuginfo-2.6.32-358.83.1.el6
kernel-debug-devel-2.6.32-358.83.1.el6
kernel-headers-2.6.32-358.83.1.el6
kernel-debug-debuginfo-2.6.32-358.83.1.el6
kernel-2.6.32-358.83.1.el6
kernel-devel-2.6.32-358.83.1.el6
perf-2.6.32-358.83.1.el6

noarch
kernel-doc-2.6.32-358.83.1.el6
kernel-firmware-2.6.32-358.83.1.el6

141712 - Red Hat Enterprise Linux RHSA-2017-2676 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Description

The scan detected that the host is missing the following update:
RHSA-2017-2676

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/msg00016.html

RHEL6D
x86_64
chromium-browser-debuginfo-61.0.3163.79-2.el6_9
chromium-browser-61.0.3163.79-2.el6_9

i386
chromium-browser-debuginfo-61.0.3163.79-2.el6_9
chromium-browser-61.0.3163.79-2.el6_9

RHEL6S
x86_64
chromium-browser-debuginfo-61.0.3163.79-2.el6_9
chromium-browser-61.0.3163.79-2.el6_9

i386
chromium-browser-debuginfo-61.0.3163.79-2.el6_9
chromium-browser-61.0.3163.79-2.el6_9

RHEL6WS
x86_64
chromium-browser-debuginfo-61.0.3163.79-2.el6_9
chromium-browser-61.0.3163.79-2.el6_9

i386
chromium-browser-debuginfo-61.0.3163.79-2.el6_9
chromium-browser-61.0.3163.79-2.el6_9

141713 - Red Hat Enterprise Linux RHSA-2017-2706 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
RHSA-2017-2706

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/msg00032.html

RHEL7_2S
noarch
kernel-doc-3.10.0-327.59.2.el7
kernel-abi-whitelists-3.10.0-327.59.2.el7

x86_64
python-perf-debuginfo-3.10.0-327.59.2.el7
kernel-debug-debuginfo-3.10.0-327.59.2.el7
kernel-debug-3.10.0-327.59.2.el7
kernel-3.10.0-327.59.2.el7
kernel-debuginfo-common-x86_64-3.10.0-327.59.2.el7
python-perf-3.10.0-327.59.2.el7
kernel-tools-libs-3.10.0-327.59.2.el7
kernel-debug-devel-3.10.0-327.59.2.el7
kernel-debuginfo-3.10.0-327.59.2.el7
kernel-tools-3.10.0-327.59.2.el7
kernel-tools-debuginfo-3.10.0-327.59.2.el7
kernel-headers-3.10.0-327.59.2.el7
kernel-tools-libs-devel-3.10.0-327.59.2.el7
perf-debuginfo-3.10.0-327.59.2.el7
kernel-devel-3.10.0-327.59.2.el7
perf-3.10.0-327.59.2.el7

141714 - Red Hat Enterprise Linux RHSA-2017-2679 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
RHSA-2017-2679

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/msg00021.html

RHEL7D

x86_64
kernel-3.10.0-693.2.2.el7
kernel-debuginfo-3.10.0-693.2.2.el7
kernel-debug-devel-3.10.0-693.2.2.el7
kernel-tools-libs-devel-3.10.0-693.2.2.el7
kernel-devel-3.10.0-693.2.2.el7
python-perf-3.10.0-693.2.2.el7
kernel-headers-3.10.0-693.2.2.el7
perf-3.10.0-693.2.2.el7
kernel-debug-3.10.0-693.2.2.el7
kernel-tools-libs-3.10.0-693.2.2.el7
perf-debuginfo-3.10.0-693.2.2.el7
kernel-debuginfo-common-x86_64-3.10.0-693.2.2.el7
kernel-debug-debuginfo-3.10.0-693.2.2.el7
kernel-tools-debuginfo-3.10.0-693.2.2.el7
kernel-tools-3.10.0-693.2.2.el7
python-perf-debuginfo-3.10.0-693.2.2.el7

noarch
kernel-doc-3.10.0-693.2.2.el7
kernel-abi-whitelists-3.10.0-693.2.2.el7

RHEL7S
noarch
kernel-doc-3.10.0-693.2.2.el7
kernel-abi-whitelists-3.10.0-693.2.2.el7

x86_64
kernel-3.10.0-693.2.2.el7
kernel-debuginfo-3.10.0-693.2.2.el7
kernel-debug-devel-3.10.0-693.2.2.el7
kernel-tools-libs-devel-3.10.0-693.2.2.el7
kernel-devel-3.10.0-693.2.2.el7
python-perf-3.10.0-693.2.2.el7
kernel-headers-3.10.0-693.2.2.el7
perf-3.10.0-693.2.2.el7
kernel-debug-3.10.0-693.2.2.el7
kernel-tools-libs-3.10.0-693.2.2.el7
perf-debuginfo-3.10.0-693.2.2.el7
kernel-debuginfo-common-x86_64-3.10.0-693.2.2.el7
kernel-debug-debuginfo-3.10.0-693.2.2.el7
kernel-tools-debuginfo-3.10.0-693.2.2.el7
kernel-tools-3.10.0-693.2.2.el7
python-perf-debuginfo-3.10.0-693.2.2.el7

RHEL7WS
x86_64
kernel-3.10.0-693.2.2.el7
kernel-debuginfo-3.10.0-693.2.2.el7
kernel-debug-devel-3.10.0-693.2.2.el7
kernel-tools-libs-devel-3.10.0-693.2.2.el7
kernel-devel-3.10.0-693.2.2.el7
python-perf-3.10.0-693.2.2.el7
kernel-headers-3.10.0-693.2.2.el7
perf-3.10.0-693.2.2.el7
kernel-debug-3.10.0-693.2.2.el7
kernel-tools-libs-3.10.0-693.2.2.el7
perf-debuginfo-3.10.0-693.2.2.el7
kernel-debuginfo-common-x86_64-3.10.0-693.2.2.el7
kernel-debug-debuginfo-3.10.0-693.2.2.el7

kernel-tools-debuginfo-3.10.0-693.2.2.el7
kernel-tools-3.10.0-693.2.2.el7
python-perf-debuginfo-3.10.0-693.2.2.el7

noarch
kernel-doc-3.10.0-693.2.2.el7
kernel-abi-whitelists-3.10.0-693.2.2.el7

145900 - SuSE Linux 42.2 openSUSE-SU-2017:2398-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9603, CVE-2017-10664, CVE-2017-11434, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2398-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00032.html

SuSE Linux 42.2
x86_64
xen-tools-domU-debuginfo-4.7.3_03-11.12.1
xen-libs-4.7.3_03-11.12.1
xen-libs-debuginfo-4.7.3_03-11.12.1
xen-tools-4.7.3_03-11.12.1
xen-tools-domU-4.7.3_03-11.12.1
xen-tools-debuginfo-4.7.3_03-11.12.1
xen-doc-html-4.7.3_03-11.12.1
xen-4.7.3_03-11.12.1
xen-debugsource-4.7.3_03-11.12.1
xen-libs-debuginfo-32bit-4.7.3_03-11.12.1
xen-libs-32bit-4.7.3_03-11.12.1
xen-devel-4.7.3_03-11.12.1

i586
xen-tools-domU-debuginfo-4.7.3_03-11.12.1
xen-libs-4.7.3_03-11.12.1
xen-libs-debuginfo-4.7.3_03-11.12.1
xen-tools-domU-4.7.3_03-11.12.1
xen-debugsource-4.7.3_03-11.12.1
xen-devel-4.7.3_03-11.12.1

145901 - SuSE Linux 42.3 openSUSE-SU-2017:2383-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12791

Description

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

openSUSE-SU-2017:2383-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00025.html

SuSE Linux 42.3
x86_64
salt-ssh-2017.7.1-11.1
salt-2017.7.1-11.1
salt-syndic-2017.7.1-11.1
salt-cloud-2017.7.1-11.1
salt-proxy-2017.7.1-11.1
salt-api-2017.7.1-11.1
salt-master-2017.7.1-11.1
salt-minion-2017.7.1-11.1
salt-doc-2017.7.1-11.1

noarch
salt-bash-completion-2017.7.1-11.1
salt-fish-completion-2017.7.1-11.1
salt-zsh-completion-2017.7.1-11.1

145904 - SuSE Linux 42.3 openSUSE-SU-2017:2384-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12134, CVE-2017-14051

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2384-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00026.html

SuSE Linux 42.3
x86_64
kernel-vanilla-devel-4.4.85-22.1
kernel-vanilla-base-4.4.85-22.1
kernel-debug-debuginfo-4.4.85-22.1
kernel-debug-base-debuginfo-4.4.85-22.1
kernel-syms-4.4.85-22.1
kernel-vanilla-debuginfo-4.4.85-22.1
kernel-debug-debugsource-4.4.85-22.1
kernel-debug-devel-debuginfo-4.4.85-22.1
kernel-obs-qa-4.4.85-22.1
kernel-default-debugsource-4.4.85-22.1
kernel-vanilla-base-debuginfo-4.4.85-22.1
kernel-debug-4.4.85-22.1
kernel-obs-build-debugsource-4.4.85-22.1
kernel-debug-base-4.4.85-22.1

kernel-default-devel-4.4.85-22.1
kernel-default-debuginfo-4.4.85-22.1
kernel-vanilla-4.4.85-22.1
kernel-default-base-debuginfo-4.4.85-22.1
kernel-debug-devel-4.4.85-22.1
kernel-default-4.4.85-22.1
kernel-vanilla-debugsource-4.4.85-22.1
kernel-default-base-4.4.85-22.1
kernel-obs-build-4.4.85-22.1

noarch
kernel-docs-4.4.85-22.3
kernel-docs-html-4.4.85-22.3
kernel-devel-4.4.85-22.1
kernel-docs-pdf-4.4.85-22.3
kernel-macros-4.4.85-22.1
kernel-source-4.4.85-22.1
kernel-source-vanilla-4.4.85-22.1

145905 - SuSE Linux 42.2 openSUSE-SU-2017:2428-1 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-2017:2428-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00049.html

SuSE Linux 42.2
noarch
clamav-database-201709110007-54.79.1

145907 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2420-1 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:
SUSE-SU-2017:2420-1

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/003197.html

SuSE SLED 12 SP3

x86_64
xen-libs-debuginfo-4.9.0_12-3.15.1
xen-4.9.0_12-3.15.1
xen-debugsource-4.9.0_12-3.15.1
xen-libs-4.9.0_12-3.15.1
xen-libs-32bit-4.9.0_12-3.15.1
xen-libs-debuginfo-32bit-4.9.0_12-3.15.1

SuSE SLES 12 SP3
x86_64
xen-libs-debuginfo-4.9.0_12-3.15.1
xen-tools-4.9.0_12-3.15.1
xen-tools-debuginfo-4.9.0_12-3.15.1
xen-4.9.0_12-3.15.1
xen-doc-html-4.9.0_12-3.15.1
xen-tools-domU-4.9.0_12-3.15.1
xen-debugsource-4.9.0_12-3.15.1
xen-libs-4.9.0_12-3.15.1
xen-libs-32bit-4.9.0_12-3.15.1
xen-libs-debuginfo-32bit-4.9.0_12-3.15.1
xen-tools-domU-debuginfo-4.9.0_12-3.15.1

145909 - SuSE SLES 11 SP4 SUSE-SU-2017:2450-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10664, CVE-2017-10806, CVE-2017-11334, CVE-2017-11434, CVE-2017-12135, CVE-2017-12137, CVE-2017-12855, CVE-2017-14316, CVE-2017-14317, CVE-2017-14319

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2450-1

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/003213.html

SuSE SLES 11 SP4
x86_64
xen-tools-domU-4.4.4_22-61.9.2
xen-doc-html-4.4.4_22-61.9.2
xen-kmp-default-4.4.4_22_3.0.101_108.7-61.9.2
xen-4.4.4_22-61.9.2
xen-libs-4.4.4_22-61.9.2
xen-libs-32bit-4.4.4_22-61.9.2
xen-tools-4.4.4_22-61.9.2

i586
xen-tools-domU-4.4.4_22-61.9.2
xen-libs-4.4.4_22-61.9.2
xen-kmp-default-4.4.4_22_3.0.101_108.7-61.9.2
xen-kmp-pae-4.4.4_22_3.0.101_108.7-61.9.2

145913 - SuSE Linux 42.3 openSUSE-SU-2017:2410-1 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-2017:2410-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00045.html

SuSE Linux 42.3
x86_64
libidn2-tools-debuginfo-2.0.4-3.1
libidn2-0-debuginfo-2.0.4-3.1
libunistring0-debuginfo-0.9.3-25.1
libunistring-devel-0.9.3-25.1
libunistring0-32bit-0.9.3-25.1
libunistring0-debuginfo-32bit-0.9.3-25.1
libidn2-0-debuginfo-32bit-2.0.4-3.1
libidn2-0-2.0.4-3.1
libidn2-devel-2.0.4-3.1
libunistring-devel-32bit-0.9.3-25.1
libunistring-debugsource-0.9.3-25.1
libidn2-tools-2.0.4-3.1
libidn2-0-32bit-2.0.4-3.1
libunistring0-0.9.3-25.1
libidn2-debugsource-2.0.4-3.1

i586
libunistring-devel-0.9.3-25.1
libidn2-devel-2.0.4-3.1
libunistring0-debuginfo-0.9.3-25.1
libidn2-0-debuginfo-2.0.4-3.1
libunistring-debugsource-0.9.3-25.1
libunistring0-0.9.3-25.1
libidn2-tools-2.0.4-3.1
libidn2-tools-debuginfo-2.0.4-3.1
libidn2-0-2.0.4-3.1
libidn2-debugsource-2.0.4-3.1

145916 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2392-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
openSUSE-SU-2017:2392-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00029.html

SuSE Linux 42.2
i586
postgresql94-plperl-debuginfo-9.4.13-9.9.1
postgresql94-test-9.4.13-9.9.1
postgresql94-9.4.13-9.9.1
postgresql94-contrib-debuginfo-9.4.13-9.9.1
postgresql94-plpython-debuginfo-9.4.13-9.9.1
postgresql94-plperl-9.4.13-9.9.1
postgresql94-pltcl-9.4.13-9.9.1
postgresql94-libs-debugsource-9.4.13-9.9.1
postgresql94-devel-9.4.13-9.9.1
postgresql94-contrib-9.4.13-9.9.1
postgresql94-devel-debuginfo-9.4.13-9.9.1
postgresql94-pltcl-debuginfo-9.4.13-9.9.1
postgresql94-server-9.4.13-9.9.1
postgresql94-plpython-9.4.13-9.9.1
postgresql94-server-debuginfo-9.4.13-9.9.1
postgresql94-debuginfo-9.4.13-9.9.1
postgresql94-debugsource-9.4.13-9.9.1

noarch
postgresql94-docs-9.4.13-9.9.1

x86_64
postgresql94-plperl-debuginfo-9.4.13-9.9.1
postgresql94-test-9.4.13-9.9.1
postgresql94-9.4.13-9.9.1
postgresql94-contrib-debuginfo-9.4.13-9.9.1
postgresql94-plpython-debuginfo-9.4.13-9.9.1
postgresql94-plperl-9.4.13-9.9.1
postgresql94-pltcl-9.4.13-9.9.1
postgresql94-libs-debugsource-9.4.13-9.9.1
postgresql94-devel-9.4.13-9.9.1
postgresql94-contrib-9.4.13-9.9.1
postgresql94-devel-debuginfo-9.4.13-9.9.1
postgresql94-pltcl-debuginfo-9.4.13-9.9.1
postgresql94-server-9.4.13-9.9.1
postgresql94-plpython-9.4.13-9.9.1
postgresql94-server-debuginfo-9.4.13-9.9.1
postgresql94-debuginfo-9.4.13-9.9.1
postgresql94-debugsource-9.4.13-9.9.1

SuSE Linux 42.3
i586
postgresql94-9.4.13-12.1
postgresql94-contrib-debuginfo-9.4.13-12.1
postgresql94-plpython-9.4.13-12.1
postgresql94-debugsource-9.4.13-12.1
postgresql94-test-9.4.13-12.1
postgresql94-libs-debugsource-9.4.13-12.1
postgresql94-server-debuginfo-9.4.13-12.1
postgresql94-plperl-9.4.13-12.1
postgresql94-server-9.4.13-12.1
postgresql94-pltcl-9.4.13-12.1
postgresql94-devel-9.4.13-12.1
postgresql94-contrib-9.4.13-12.1
postgresql94-devel-debuginfo-9.4.13-12.1
postgresql94-debuginfo-9.4.13-12.1

postgresql94-pltcl-debuginfo-9.4.13-12.1
postgresql94-plperl-debuginfo-9.4.13-12.1
postgresql94-plpython-debuginfo-9.4.13-12.1

noarch
postgresql94-docs-9.4.13-12.1

x86_64
postgresql94-9.4.13-12.1
postgresql94-contrib-debuginfo-9.4.13-12.1
postgresql94-plpython-9.4.13-12.1
postgresql94-debugsource-9.4.13-12.1
postgresql94-test-9.4.13-12.1
postgresql94-libs-debugsource-9.4.13-12.1
postgresql94-server-debuginfo-9.4.13-12.1
postgresql94-plperl-9.4.13-12.1
postgresql94-server-9.4.13-12.1
postgresql94-pltcl-9.4.13-12.1
postgresql94-devel-9.4.13-12.1
postgresql94-contrib-9.4.13-12.1
postgresql94-devel-debuginfo-9.4.13-12.1
postgresql94-debuginfo-9.4.13-12.1
postgresql94-pltcl-debuginfo-9.4.13-12.1
postgresql94-plperl-debuginfo-9.4.13-12.1
postgresql94-plpython-debuginfo-9.4.13-12.1

145917 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2391-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
openSUSE-SU-2017:2391-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00030.html

SuSE Linux 42.2
i586
postgresql96-debugsource-9.6.4-5.1
postgresql96-devel-9.6.4-5.1
libecpg6-debuginfo-9.6.4-5.1
libpq5-debuginfo-9.6.4-5.1
postgresql96-pltcl-debuginfo-9.6.4-5.1
postgresql96-plpython-9.6.4-5.1
postgresql96-devel-debuginfo-9.6.4-5.1
libecpg6-9.6.4-5.1
postgresql96-server-9.6.4-5.1
postgresql96-libs-debugsource-9.6.4-5.1
postgresql96-plperl-9.6.4-5.1
postgresql96-plperl-debuginfo-9.6.4-5.1
postgresql96-test-9.6.4-5.1
postgresql96-contrib-debuginfo-9.6.4-5.1

postgresql96-pltcl-9.6.4-5.1
libpq5-9.6.4-5.1
postgresql96-plpython-debuginfo-9.6.4-5.1
postgresql96-contrib-9.6.4-5.1
postgresql96-9.6.4-5.1
postgresql96-server-debuginfo-9.6.4-5.1
postgresql96-debuginfo-9.6.4-5.1

noarch
postgresql96-docs-9.6.4-5.1

x86_64
postgresql96-debugsource-9.6.4-5.1
postgresql96-devel-9.6.4-5.1
libecpg6-32bit-9.6.4-5.1
libecpg6-debuginfo-9.6.4-5.1
libpq5-debuginfo-9.6.4-5.1
libecpg6-debuginfo-32bit-9.6.4-5.1
libpq5-32bit-9.6.4-5.1
postgresql96-pltcl-debuginfo-9.6.4-5.1
postgresql96-plpython-9.6.4-5.1
postgresql96-devel-debuginfo-9.6.4-5.1
libecpg6-9.6.4-5.1
postgresql96-server-9.6.4-5.1
postgresql96-libs-debugsource-9.6.4-5.1
libpq5-debuginfo-32bit-9.6.4-5.1
postgresql96-plperl-9.6.4-5.1
postgresql96-plperl-debuginfo-9.6.4-5.1
postgresql96-test-9.6.4-5.1
postgresql96-contrib-debuginfo-9.6.4-5.1
postgresql96-pltcl-9.6.4-5.1
libpq5-9.6.4-5.1
postgresql96-plpython-debuginfo-9.6.4-5.1
postgresql96-contrib-9.6.4-5.1
postgresql96-9.6.4-5.1
postgresql96-server-debuginfo-9.6.4-5.1
postgresql96-debuginfo-9.6.4-5.1

SuSE Linux 42.3
i586
postgresql96-pltcl-debuginfo-9.6.4-6.1
postgresql96-server-debuginfo-9.6.4-6.1
postgresql96-server-9.6.4-6.1
postgresql96-devel-debuginfo-9.6.4-6.1
libecpg6-9.6.4-6.1
postgresql96-contrib-9.6.4-6.1
postgresql96-plperl-debuginfo-9.6.4-6.1
postgresql96-debuginfo-9.6.4-6.1
postgresql96-devel-9.6.4-6.1
postgresql96-plpython-debuginfo-9.6.4-6.1
postgresql96-pltcl-9.6.4-6.1
postgresql96-plpython-9.6.4-6.1
libecpg6-debuginfo-9.6.4-6.1
postgresql96-9.6.4-6.1
libpq5-9.6.4-6.1
postgresql96-libs-debugsource-9.6.4-6.1
libpq5-debuginfo-9.6.4-6.1
postgresql96-test-9.6.4-6.1
postgresql96-plperl-9.6.4-6.1
postgresql96-contrib-debuginfo-9.6.4-6.1

postgresql96-debugsource-9.6.4-6.1

noarch
postgresql96-docs-9.6.4-6.1

x86_64
libpq5-32bit-9.6.4-6.1
postgresql96-pltcl-debuginfo-9.6.4-6.1
postgresql96-server-debuginfo-9.6.4-6.1
libecpg6-32bit-9.6.4-6.1
postgresql96-server-9.6.4-6.1
postgresql96-devel-debuginfo-9.6.4-6.1
libecpg6-9.6.4-6.1
postgresql96-contrib-9.6.4-6.1
postgresql96-plperl-debuginfo-9.6.4-6.1
postgresql96-debuginfo-9.6.4-6.1
postgresql96-devel-9.6.4-6.1
postgresql96-plpython-debuginfo-9.6.4-6.1
postgresql96-pltcl-9.6.4-6.1
postgresql96-plpython-9.6.4-6.1
libecpg6-debuginfo-9.6.4-6.1
postgresql96-9.6.4-6.1
libpq5-9.6.4-6.1
postgresql96-libs-debugsource-9.6.4-6.1
libpq5-debuginfo-9.6.4-6.1
postgresql96-test-9.6.4-6.1
postgresql96-plperl-9.6.4-6.1
libecpg6-debuginfo-32bit-9.6.4-6.1
libpq5-debuginfo-32bit-9.6.4-6.1
postgresql96-contrib-debuginfo-9.6.4-6.1
postgresql96-debugsource-9.6.4-6.1

145918 - SuSE Linux 42.3 openSUSE-SU-2017:2394-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10664, CVE-2017-11434, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2394-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00033.html

SuSE Linux 42.3
x86_64
xen-tools-debuginfo-4.9.0_11-4.1
xen-libs-4.9.0_11-4.1
xen-libs-debuginfo-4.9.0_11-4.1
xen-tools-domU-4.9.0_11-4.1
xen-devel-4.9.0_11-4.1
xen-doc-html-4.9.0_11-4.1
xen-tools-4.9.0_11-4.1
xen-4.9.0_11-4.1

xen-debugsource-4.9.0_11-4.1
xen-tools-domU-debuginfo-4.9.0_11-4.1

160296 - CentOS 6 CESA-2017-2681 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
CESA-2017-2681

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/022530.html

CentOS 6
i686
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6

noarch
kernel-firmware-2.6.32-696.10.2.el6
kernel-doc-2.6.32-696.10.2.el6
kernel-abi-whitelists-2.6.32-696.10.2.el6

x86_64
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6

160297 - CentOS 7 CESA-2017-2679 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-2017-2679

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/022536.html

CentOS 7
x86_64
kernel-devel-3.10.0-693.2.2.el7
kernel-debug-devel-3.10.0-693.2.2.el7
perf-3.10.0-693.2.2.el7
kernel-debug-3.10.0-693.2.2.el7
kernel-3.10.0-693.2.2.el7
python-perf-3.10.0-693.2.2.el7
kernel-headers-3.10.0-693.2.2.el7
kernel-tools-3.10.0-693.2.2.el7
kernel-tools-libs-3.10.0-693.2.2.el7
kernel-tools-libs-devel-3.10.0-693.2.2.el7

noarch
kernel-doc-3.10.0-693.2.2.el7
kernel-abi-whitelists-3.10.0-693.2.2.el7

163453 - Oracle Enterprise Linux ELSA-2017-2681 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
ELSA-2017-2681

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/007203.html

OEL6
x86_64
perf-2.6.32-696.10.2.el6
kernel-abi-whitelists-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
kernel-doc-2.6.32-696.10.2.el6
kernel-firmware-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6

i386
perf-2.6.32-696.10.2.el6
kernel-abi-whitelists-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
kernel-doc-2.6.32-696.10.2.el6
kernel-firmware-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6

kernel-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6

163455 - Oracle Enterprise Linux ELSA-2017-2679 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
ELSA-2017-2679

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/007201.html
http://oss.oracle.com/pipermail/el-errata/2017-September/007205.html

OEL7
x86_64
kernel-3.10.0-693.2.2.el7
perf-3.10.0-693.2.2.0.1.el7
kernel-abi-whitelists-3.10.0-693.2.2.0.1.el7
kernel-headers-3.10.0-693.2.2.0.1.el7
kernel-3.10.0-693.2.2.0.1.el7
kernel-debug-devel-3.10.0-693.2.2.el7
kernel-devel-3.10.0-693.2.2.el7
kernel-debug-3.10.0-693.2.2.0.1.el7
python-perf-3.10.0-693.2.2.0.1.el7
kernel-tools-libs-devel-3.10.0-693.2.2.el7
kernel-doc-3.10.0-693.2.2.el7
kernel-tools-libs-devel-3.10.0-693.2.2.0.1.el7
kernel-devel-3.10.0-693.2.2.0.1.el7
python-perf-3.10.0-693.2.2.el7
kernel-doc-3.10.0-693.2.2.0.1.el7
perf-3.10.0-693.2.2.el7
kernel-debug-3.10.0-693.2.2.el7
kernel-headers-3.10.0-693.2.2.el7
kernel-abi-whitelists-3.10.0-693.2.2.el7
kernel-debug-devel-3.10.0-693.2.2.0.1.el7
kernel-tools-3.10.0-693.2.2.el7
kernel-tools-libs-3.10.0-693.2.2.el7
kernel-tools-libs-3.10.0-693.2.2.0.1.el7
kernel-tools-3.10.0-693.2.2.0.1.el7

175258 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1709-1083)

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1709-1083)

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=1083

SL6
i386
python-perf-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6
python-perf-debuginfo-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6
kernel-debuginfo-common-i686-2.6.32-696.10.2.el6
kernel-2.6.32-696.10.2.el6
kernel-debug-debuginfo-2.6.32-696.10.2.el6
perf-debuginfo-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-debuginfo-2.6.32-696.10.2.el6

noarch
kernel-firmware-2.6.32-696.10.2.el6
kernel-doc-2.6.32-696.10.2.el6
kernel-abi-whitelists-2.6.32-696.10.2.el6

x86_64
kernel-2.6.32-696.10.2.el6
perf-2.6.32-696.10.2.el6
perf-debuginfo-2.6.32-696.10.2.el6
kernel-debuginfo-common-x86_64-2.6.32-696.10.2.el6
kernel-debug-debuginfo-2.6.32-696.10.2.el6
kernel-debuginfo-common-i686-2.6.32-696.10.2.el6
python-perf-2.6.32-696.10.2.el6
python-perf-debuginfo-2.6.32-696.10.2.el6
kernel-debug-2.6.32-696.10.2.el6
kernel-debuginfo-2.6.32-696.10.2.el6
kernel-headers-2.6.32-696.10.2.el6
kernel-devel-2.6.32-696.10.2.el6
kernel-debug-devel-2.6.32-696.10.2.el6

175259 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1709-756)

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

Risk Level: High

CVE: CVE-2017-1000251

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1709-756)

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=756

SL7
x86_64
kernel-3.10.0-693.2.2.el7
kernel-debuginfo-3.10.0-693.2.2.el7
kernel-debug-devel-3.10.0-693.2.2.el7
kernel-tools-libs-devel-3.10.0-693.2.2.el7
kernel-devel-3.10.0-693.2.2.el7
python-perf-3.10.0-693.2.2.el7
kernel-headers-3.10.0-693.2.2.el7
perf-3.10.0-693.2.2.el7
kernel-debug-3.10.0-693.2.2.el7
kernel-tools-libs-3.10.0-693.2.2.el7
perf-debuginfo-3.10.0-693.2.2.el7
kernel-debuginfo-common-x86_64-3.10.0-693.2.2.el7
kernel-debug-debuginfo-3.10.0-693.2.2.el7
kernel-tools-debuginfo-3.10.0-693.2.2.el7
kernel-tools-3.10.0-693.2.2.el7
python-perf-debuginfo-3.10.0-693.2.2.el7

noarch
kernel-doc-3.10.0-693.2.2.el7
kernel-abi-whitelists-3.10.0-693.2.2.el7

185870 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3414-1 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-3414-1

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/004041.html

Ubuntu 16.04

qemu-system-s390x_2.5+dfsg-5ubuntu10.15
qemu-system-arm_2.5+dfsg-5ubuntu10.15
qemu-system-ppc_2.5+dfsg-5ubuntu10.15
qemu-system-misc_2.5+dfsg-5ubuntu10.15
qemu-system-mips_2.5+dfsg-5ubuntu10.15
qemu-system-x86_2.5+dfsg-5ubuntu10.15
qemu-system-aarch64_2.5+dfsg-5ubuntu10.15
qemu-system_2.5+dfsg-5ubuntu10.15
qemu-system-sparc_2.5+dfsg-5ubuntu10.15

Ubuntu 14.04

qemu-system-misc_2.0.0+dfsg-2ubuntu1.35
qemu-system-aarch64_2.0.0+dfsg-2ubuntu1.35
qemu-system-sparc_2.0.0+dfsg-2ubuntu1.35

qemu-system-mips_2.0.0+dfsg-2ubuntu1.35
qemu-system-ppc_2.0.0+dfsg-2ubuntu1.35
qemu-system-x86_2.0.0+dfsg-2ubuntu1.35
qemu-system-arm_2.0.0+dfsg-2ubuntu1.35
qemu-system_2.0.0+dfsg-2ubuntu1.35

Ubuntu 17.04

qemu-system-misc_2.8+dfsg-3ubuntu2.4
qemu-system-ppc_2.8+dfsg-3ubuntu2.4
qemu-system-s390x_2.8+dfsg-3ubuntu2.4
qemu-system-aarch64_2.8+dfsg-3ubuntu2.4
qemu-system-arm_2.8+dfsg-3ubuntu2.4
qemu-system-mips_2.8+dfsg-3ubuntu2.4
qemu-system-x86_2.8+dfsg-3ubuntu2.4
qemu-system_2.8+dfsg-3ubuntu2.4
qemu-system-sparc_2.8+dfsg-3ubuntu2.4

192607 - Fedora Linux 25 FEDORA-2017-86cfcbbae8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9432

Description

The scan detected that the host is missing the following update:
FEDORA-2017-86cfcbbae8

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=2

Fedora Core 25

libstaroffice-0.0.4-1.fc25

192608 - Fedora Linux 26 FEDORA-2017-20214ad330 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0899, CVE-2017-0900, CVE-2017-0901, CVE-2017-0902

Description

The scan detected that the host is missing the following update:
FEDORA-2017-20214ad330

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=2

Fedora Core 26

rubygems-2.6.13-100.fc26

192619 - Fedora Linux 26 FEDORA-2017-fe4f93fde4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14061, CVE-2017-14062

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fe4f93fde4

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=2

Fedora Core 26

mingw-libidn2-2.0.4-1.fc26

192620 - Fedora Linux 26 FEDORA-2017-840db88351 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12858, CVE-2017-14107

Description

The scan detected that the host is missing the following update:
FEDORA-2017-840db88351

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=3

Fedora Core 26

libzip-1.3.0-1.fc26

192625 - Fedora Linux 25 FEDORA-2017-f0b31bc9c5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12858

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f0b31bc9c5

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=2

Fedora Core 25

mingw-libzip-1.1.3-2.fc25

130881 - Debian Linux 9.0 DSA-3967-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14032

Description

The scan detected that the host is missing the following update:
DSA-3967-1

Observation

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

http://www.debian.org/security/2017/dsa-3967

Debian 9.0
all
libmbedtls-dev_2.4.2-1+deb9u1
libmbedtls-doc_2.4.2-1+deb9u1
libmbedx509-0_2.4.2-1+deb9u1
libmbedtls10_2.4.2-1+deb9u1
libmbedcrypto0_2.4.2-1+deb9u1

145902 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2390-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000083

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2390-1

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/003194.html

SuSE SLED 12 SP2
x86_64
evince-plugin-tiffdocument-debuginfo-3.20.1-6.16.1
evince-plugin-psdocument-debuginfo-3.20.1-6.16.1
evince-debugsource-3.20.1-6.16.1
evince-plugin-pdfdocument-debuginfo-3.20.1-6.16.1
evince-plugin-xpsdocument-3.20.1-6.16.1

libevdocument3-4-debuginfo-3.20.1-6.16.1
libevview3-3-debuginfo-3.20.1-6.16.1
evince-browser-plugin-debuginfo-3.20.1-6.16.1
evince-plugin-djvudocument-3.20.1-6.16.1
evince-plugin-psdocument-3.20.1-6.16.1
evince-plugin-dvidocument-debuginfo-3.20.1-6.16.1
typelib-1_0-EvinceView-3_0-3.20.1-6.16.1
evince-plugin-xpsdocument-debuginfo-3.20.1-6.16.1
libevdocument3-4-3.20.1-6.16.1
evince-plugin-tiffdocument-3.20.1-6.16.1
nautilus-evince-3.20.1-6.16.1
evince-debuginfo-3.20.1-6.16.1
nautilus-evince-debuginfo-3.20.1-6.16.1
evince-plugin-pdfdocument-3.20.1-6.16.1
evince-plugin-dvidocument-3.20.1-6.16.1
evince-plugin-djvudocument-debuginfo-3.20.1-6.16.1
evince-3.20.1-6.16.1
typelib-1_0-EvinceDocument-3_0-3.20.1-6.16.1
evince-browser-plugin-3.20.1-6.16.1
libevview3-3-3.20.1-6.16.1

noarch
evince-lang-3.20.1-6.16.1

SuSE SLES 12 SP3
noarch
evince-lang-3.20.1-6.16.1

x86_64
evince-plugin-tiffdocument-debuginfo-3.20.1-6.16.1
evince-plugin-psdocument-debuginfo-3.20.1-6.16.1
evince-debugsource-3.20.1-6.16.1
evince-plugin-xpsdocument-3.20.1-6.16.1
libevdocument3-4-debuginfo-3.20.1-6.16.1
libevview3-3-debuginfo-3.20.1-6.16.1
evince-browser-plugin-debuginfo-3.20.1-6.16.1
evince-plugin-djvudocument-3.20.1-6.16.1
evince-plugin-psdocument-3.20.1-6.16.1
evince-plugin-dvidocument-debuginfo-3.20.1-6.16.1
evince-plugin-pdfdocument-debuginfo-3.20.1-6.16.1
evince-plugin-xpsdocument-debuginfo-3.20.1-6.16.1
libevdocument3-4-3.20.1-6.16.1
evince-plugin-tiffdocument-3.20.1-6.16.1
nautilus-evince-3.20.1-6.16.1
evince-debuginfo-3.20.1-6.16.1
nautilus-evince-debuginfo-3.20.1-6.16.1
evince-plugin-pdfdocument-3.20.1-6.16.1
evince-plugin-dvidocument-3.20.1-6.16.1
evince-3.20.1-6.16.1
evince-plugin-djvudocument-debuginfo-3.20.1-6.16.1
evince-browser-plugin-3.20.1-6.16.1
libevview3-3-3.20.1-6.16.1

SuSE SLES 12 SP2
noarch
evince-lang-3.20.1-6.16.1

x86_64
evince-plugin-tiffdocument-debuginfo-3.20.1-6.16.1
evince-plugin-psdocument-debuginfo-3.20.1-6.16.1

evince-debugsource-3.20.1-6.16.1
evince-plugin-xpsdocument-3.20.1-6.16.1
libevdocument3-4-debuginfo-3.20.1-6.16.1
libevview3-3-debuginfo-3.20.1-6.16.1
evince-browser-plugin-debuginfo-3.20.1-6.16.1
evince-plugin-djvudocument-3.20.1-6.16.1
evince-plugin-psdocument-3.20.1-6.16.1
evince-plugin-dvidocument-debuginfo-3.20.1-6.16.1
evince-plugin-pdfdocument-debuginfo-3.20.1-6.16.1
evince-plugin-xpsdocument-debuginfo-3.20.1-6.16.1
libevdocument3-4-3.20.1-6.16.1
evince-plugin-tiffdocument-3.20.1-6.16.1
nautilus-evince-3.20.1-6.16.1
evince-debuginfo-3.20.1-6.16.1
nautilus-evince-debuginfo-3.20.1-6.16.1
evince-plugin-pdfdocument-3.20.1-6.16.1
evince-plugin-dvidocument-3.20.1-6.16.1
evince-3.20.1-6.16.1
evince-plugin-djvudocument-debuginfo-3.20.1-6.16.1
evince-browser-plugin-3.20.1-6.16.1
libevview3-3-3.20.1-6.16.1

SuSE SLED 12 SP3
x86_64
evince-plugin-tiffdocument-debuginfo-3.20.1-6.16.1
evince-plugin-psdocument-debuginfo-3.20.1-6.16.1
evince-debugsource-3.20.1-6.16.1
evince-plugin-pdfdocument-debuginfo-3.20.1-6.16.1
evince-plugin-xpsdocument-3.20.1-6.16.1
libevdocument3-4-debuginfo-3.20.1-6.16.1
libevview3-3-debuginfo-3.20.1-6.16.1
evince-browser-plugin-debuginfo-3.20.1-6.16.1
evince-plugin-djvudocument-3.20.1-6.16.1
evince-plugin-psdocument-3.20.1-6.16.1
evince-plugin-dvidocument-debuginfo-3.20.1-6.16.1
typelib-1_0-EvinceView-3_0-3.20.1-6.16.1
evince-plugin-xpsdocument-debuginfo-3.20.1-6.16.1
libevdocument3-4-3.20.1-6.16.1
evince-plugin-tiffdocument-3.20.1-6.16.1
nautilus-evince-3.20.1-6.16.1
evince-debuginfo-3.20.1-6.16.1
nautilus-evince-debuginfo-3.20.1-6.16.1
evince-plugin-pdfdocument-3.20.1-6.16.1
evince-plugin-dvidocument-3.20.1-6.16.1
evince-plugin-djvudocument-debuginfo-3.20.1-6.16.1
evince-3.20.1-6.16.1
typelib-1_0-EvinceDocument-3_0-3.20.1-6.16.1
evince-browser-plugin-3.20.1-6.16.1
libevview3-3-3.20.1-6.16.1

noarch
evince-lang-3.20.1-6.16.1

145908 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2381-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2862, CVE-2017-2870, CVE-2017-6312, CVE-2017-6313, CVE-2017-6314

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2381-1

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/003191.html

SuSE SLES 12 SP2
noarch
gdk-pixbuf-lang-2.34.0-19.5.1

x86_64
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-19.5.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-19.5.1
gdk-pixbuf-query-loaders-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-19.5.1
gdk-pixbuf-debugsource-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-19.5.1

SuSE SLED 12 SP3
x86_64
libgdk_pixbuf-2_0-0-2.34.0-19.5.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-19.5.1
gdk-pixbuf-query-loaders-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-19.5.1
gdk-pixbuf-query-loaders-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-19.5.1
gdk-pixbuf-debugsource-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-19.5.1

noarch
gdk-pixbuf-lang-2.34.0-19.5.1

SuSE SLED 12 SP2
x86_64
libgdk_pixbuf-2_0-0-2.34.0-19.5.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-19.5.1
gdk-pixbuf-query-loaders-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-19.5.1
gdk-pixbuf-query-loaders-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-19.5.1
gdk-pixbuf-debugsource-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-19.5.1

noarch
gdk-pixbuf-lang-2.34.0-19.5.1

SuSE SLES 12 SP3

noarch
gdk-pixbuf-lang-2.34.0-19.5.1

x86_64
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-19.5.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-19.5.1
gdk-pixbuf-query-loaders-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-19.5.1
gdk-pixbuf-debugsource-2.34.0-19.5.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-19.5.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-19.5.1

145915 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2393-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2862, CVE-2017-2870, CVE-2017-6312, CVE-2017-6313, CVE-2017-6314

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2393-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00031.html

SuSE Linux 42.2
i586
libgdk_pixbuf-2_0-0-2.34.0-7.3.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-7.3.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-7.3.1
gdk-pixbuf-debugsource-2.34.0-7.3.1
gdk-pixbuf-devel-2.34.0-7.3.1
gdk-pixbuf-query-loaders-2.34.0-7.3.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-7.3.1
gdk-pixbuf-devel-debuginfo-2.34.0-7.3.1

noarch
gdk-pixbuf-lang-2.34.0-7.3.1

x86_64
typelib-1_0-GdkPixbuf-2_0-2.34.0-7.3.1
gdk-pixbuf-devel-debuginfo-32bit-2.34.0-7.3.1
gdk-pixbuf-debugsource-2.34.0-7.3.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-7.3.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-7.3.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-7.3.1
gdk-pixbuf-query-loaders-32bit-2.34.0-7.3.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-7.3.1
gdk-pixbuf-query-loaders-2.34.0-7.3.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-7.3.1
gdk-pixbuf-devel-32bit-2.34.0-7.3.1
gdk-pixbuf-devel-debuginfo-2.34.0-7.3.1

gdk-pixbuf-devel-2.34.0-7.3.1
libgdk_pixbuf-2_0-0-2.34.0-7.3.1

SuSE Linux 42.3
i586
gdk-pixbuf-devel-debuginfo-2.34.0-10.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-10.1
gdk-pixbuf-debugsource-2.34.0-10.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-10.1
gdk-pixbuf-devel-2.34.0-10.1
gdk-pixbuf-query-loaders-2.34.0-10.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-10.1
libgdk_pixbuf-2_0-0-2.34.0-10.1

noarch
gdk-pixbuf-lang-2.34.0-10.1

x86_64
gdk-pixbuf-query-loaders-debuginfo-2.34.0-10.1
gdk-pixbuf-devel-2.34.0-10.1
gdk-pixbuf-devel-debuginfo-32bit-2.34.0-10.1
gdk-pixbuf-query-loaders-32bit-2.34.0-10.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-10.1
libgdk_pixbuf-2_0-0-2.34.0-10.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-10.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-10.1
gdk-pixbuf-devel-32bit-2.34.0-10.1
gdk-pixbuf-devel-debuginfo-2.34.0-10.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-10.1
gdk-pixbuf-debugsource-2.34.0-10.1
gdk-pixbuf-query-loaders-2.34.0-10.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-10.1

192609 - Fedora Linux 25 FEDORA-2017-f7a73de98d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14040, CVE-2017-14041, CVE-2017-14151, CVE-2017-14152

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f7a73de98d

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=2

Fedora Core 25

mingw-openjpeg2-2.2.0-3.fc25

192613 - Fedora Linux 25 FEDORA-2017-3abea58794 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14032

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3abea58794

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=2

Fedora Core 25

mbedtls-2.6.0-1.fc25

192614 - Fedora Linux 25 FEDORA-2017-f285db3668 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14040, CVE-2017-14041, CVE-2017-14151, CVE-2017-14152

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f285db3668

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=2

Fedora Core 25

openjpeg2-2.2.0-3.fc25

192615 - Fedora Linux 26 FEDORA-2017-5a3cd21cee Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14040, CVE-2017-14041, CVE-2017-14151, CVE-2017-14152

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5a3cd21cee

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=3

Fedora Core 26

openjpeg2-2.2.0-3.fc26

192622 - Fedora Linux 26 FEDORA-2017-43390e73b1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14040, CVE-2017-14041, CVE-2017-14151, CVE-2017-14152

Description

The scan detected that the host is missing the following update:
FEDORA-2017-43390e73b1

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-openjpeg2-2.2.0-3.fc26

22387 - (K10133477) F5 BIG-IP IPsec IKE Peer Listener Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-5736

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 IPsec IKE peer listener. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

22449 - (K44942017) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-5209

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 NTP component. Successful exploitation could allow attacker to cause a disclosure of information.

141707 - Red Hat Enterprise Linux RHSA-2017-2672 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000048

Description

The scan detected that the host is missing the following update:
RHSA-2017-2672

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/msg00015.html

RHEL6_7S
noarch
rh-nodejs6-nodejs-qs-6.2.3-1.el6

RHEL6S
noarch
rh-nodejs6-nodejs-qs-6.2.3-1.el6

RHEL6WS
noarch
rh-nodejs6-nodejs-qs-6.2.3-1.el6

RHEL7S
noarch
rh-nodejs6-nodejs-qs-6.2.3-1.el7

RHEL7WS
noarch
rh-nodejs6-nodejs-qs-6.2.3-1.el7

141710 - Red Hat Enterprise Linux RHSA-2017-2685 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000250

Description

The scan detected that the host is missing the following update:
RHSA-2017-2685

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/msg00028.html

RHEL7S
x86_64
bluez-cups-5.44-4.el7_4
bluez-5.44-4.el7_4
bluez-libs-devel-5.44-4.el7_4
bluez-libs-5.44-4.el7_4

bluez-debuginfo-5.44-4.el7_4
bluez-hid2hci-5.44-4.el7_4

RHEL6S
i386
bluez-libs-devel-4.66-2.el6_9
bluez-debuginfo-4.66-2.el6_9
bluez-cups-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-libs-4.66-2.el6_9

x86_64
bluez-libs-devel-4.66-2.el6_9
bluez-debuginfo-4.66-2.el6_9
bluez-cups-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-libs-4.66-2.el6_9

RHEL6WS
x86_64
bluez-debuginfo-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-libs-4.66-2.el6_9

i386
bluez-debuginfo-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-libs-4.66-2.el6_9

RHEL7D
x86_64
bluez-cups-5.44-4.el7_4
bluez-5.44-4.el7_4
bluez-libs-devel-5.44-4.el7_4
bluez-libs-5.44-4.el7_4
bluez-debuginfo-5.44-4.el7_4
bluez-hid2hci-5.44-4.el7_4

RHEL6D
x86_64
bluez-libs-devel-4.66-2.el6_9
bluez-debuginfo-4.66-2.el6_9
bluez-cups-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-libs-4.66-2.el6_9

i386
bluez-libs-devel-4.66-2.el6_9
bluez-debuginfo-4.66-2.el6_9
bluez-cups-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9

bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-libs-4.66-2.el6_9

RHEL7WS
x86_64
bluez-cups-5.44-4.el7_4
bluez-5.44-4.el7_4
bluez-libs-devel-5.44-4.el7_4
bluez-libs-5.44-4.el7_4
bluez-debuginfo-5.44-4.el7_4
bluez-hid2hci-5.44-4.el7_4

145910 - SuSE SLES 11 SP4 SUSE-SU-2017:2422-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12836

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2422-1

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/003198.html

SuSE SLES 11 SP4
i586
cvs-1.12.12-144.23.5.3.1
cvs-doc-1.12.12-144.23.5.3.1

x86_64
cvs-1.12.12-144.23.5.3.1
cvs-doc-1.12.12-144.23.5.3.1

145911 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2419-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12836

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2419-1

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/003196.html

SuSE SLES 12 SP2

noarch
cvs-doc-1.12.12-182.3.1

x86_64
cvs-1.12.12-182.3.1
cvs-debuginfo-1.12.12-182.3.1
cvs-debugsource-1.12.12-182.3.1

SuSE SLED 12 SP3
x86_64
cvs-1.12.12-182.3.1
cvs-debuginfo-1.12.12-182.3.1
cvs-debugsource-1.12.12-182.3.1

SuSE SLED 12 SP2
x86_64
cvs-1.12.12-182.3.1
cvs-debuginfo-1.12.12-182.3.1
cvs-debugsource-1.12.12-182.3.1

SuSE SLES 12 SP3
noarch
cvs-doc-1.12.12-182.3.1

x86_64
cvs-1.12.12-182.3.1
cvs-debuginfo-1.12.12-182.3.1
cvs-debugsource-1.12.12-182.3.1

145912 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2416-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10664, CVE-2017-10806, CVE-2017-11334, CVE-2017-11434

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2416-1

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/003195.html

SuSE SLED 12 SP3
x86_64
qemu-tools-2.9.0-6.3.1
qemu-block-curl-2.9.0-6.3.1
qemu-x86-2.9.0-6.3.1
qemu-block-curl-debuginfo-2.9.0-6.3.1
qemu-kvm-2.9.0-6.3.1
qemu-tools-debuginfo-2.9.0-6.3.1
qemu-2.9.0-6.3.1
qemu-debugsource-2.9.0-6.3.1

noarch
qemu-ipxe-1.0.0-6.3.1

qemu-vgabios-1.10.2-6.3.1
qemu-sgabios-8-6.3.1
qemu-seabios-1.10.2-6.3.1

SuSE SLES 12 SP3
noarch
qemu-ipxe-1.0.0-6.3.1
qemu-vgabios-1.10.2-6.3.1
qemu-sgabios-8-6.3.1
qemu-seabios-1.10.2-6.3.1

x86_64
qemu-block-ssh-debuginfo-2.9.0-6.3.1
qemu-2.9.0-6.3.1
qemu-block-rbd-debuginfo-2.9.0-6.3.1
qemu-tools-debuginfo-2.9.0-6.3.1
qemu-block-curl-2.9.0-6.3.1
qemu-block-ssh-2.9.0-6.3.1
qemu-kvm-2.9.0-6.3.1
qemu-debugsource-2.9.0-6.3.1
qemu-block-rbd-2.9.0-6.3.1
qemu-guest-agent-2.9.0-6.3.1
qemu-tools-2.9.0-6.3.1
qemu-lang-2.9.0-6.3.1
qemu-guest-agent-debuginfo-2.9.0-6.3.1
qemu-block-curl-debuginfo-2.9.0-6.3.1
qemu-x86-2.9.0-6.3.1

145914 - SuSE SLES 11 SP4 SUSE-SU-2017:2375-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9063, CVE-2017-9233

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2375-1

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/003189.html

SuSE SLES 11 SP4
i586
libexpat1-2.0.1-88.42.3.2
expat-2.0.1-88.42.3.2

x86_64
libexpat1-32bit-2.0.1-88.42.3.2
libexpat1-2.0.1-88.42.3.2
expat-2.0.1-88.42.3.2

160295 - CentOS 6, 7 CESA-2017-2685 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-2017-2685

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/022531.html
http://lists.centos.org/pipermail/centos-announce/2017-September/022535.html

CentOS 7
x86_64
bluez-5.44-4.el7_4
bluez-libs-5.44-4.el7_4
bluez-hid2hci-5.44-4.el7_4
bluez-cups-5.44-4.el7_4
bluez-libs-devel-5.44-4.el7_4

i686
bluez-libs-5.44-4.el7_4
bluez-libs-devel-5.44-4.el7_4

CentOS 6
x86_64
bluez-libs-devel-4.66-2.el6_9
bluez-libs-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-cups-4.66-2.el6_9

i686
bluez-libs-devel-4.66-2.el6_9
bluez-libs-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-cups-4.66-2.el6_9

163454 - Oracle Enterprise Linux ELSA-2017-2685 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000250

Description

The scan detected that the host is missing the following update:
ELSA-2017-2685

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/007202.html
http://oss.oracle.com/pipermail/el-errata/2017-September/007204.html

OEL7
x86_64
bluez-5.44-4.el7_4
bluez-libs-5.44-4.el7_4
bluez-hid2hci-5.44-4.el7_4
bluez-cups-5.44-4.el7_4
bluez-libs-devel-5.44-4.el7_4

OEL6
x86_64
bluez-libs-devel-4.66-2.el6_9
bluez-libs-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-cups-4.66-2.el6_9

i386
bluez-libs-devel-4.66-2.el6_9
bluez-libs-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-cups-4.66-2.el6_9

175257 - Scientific Linux Security ERRATA Moderate: bluez on SL6.x, SL7.x i386/x86_64 (1709-422)

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

Risk Level: Medium

CVE: CVE-2017-1000250

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: bluez on SL6.x, SL7.x i386/x86_64 (1709-422)

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=422

SL7
x86_64
bluez-libs-devel-5.44-4.el7_4
bluez-libs-5.44-4.el7_4
bluez-hid2hci-5.44-4.el7_4
bluez-5.44-4.el7_4
bluez-cups-5.44-4.el7_4

SL6
x86_64

bluez-libs-devel-4.66-2.el6_9
bluez-cups-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-libs-4.66-2.el6_9

i386
bluez-libs-devel-4.66-2.el6_9
bluez-debuginfo-4.66-2.el6_9
bluez-libs-4.66-2.el6_9
bluez-alsa-4.66-2.el6_9
bluez-gstreamer-4.66-2.el6_9
bluez-compat-4.66-2.el6_9
bluez-4.66-2.el6_9
bluez-cups-4.66-2.el6_9

192624 - Fedora Linux 25 FEDORA-2017-a69b0bb52d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6362, CVE-2017-7890

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a69b0bb52d

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=2

Fedora Core 25

gd-2.2.5-1.fc25

192627 - Fedora Linux 26 FEDORA-2017-c98c2e8e7a 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-c98c2e8e7a

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

libwmf-0.2.8.4-53.fc26

145903 - SuSE Linux 42.3 openSUSE-SU-2017:2409-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12797

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2409-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-09/msg00044.html

SuSE Linux 42.3
x86_64
mpg123-pulse-debuginfo-1.25.6-7.1
mpg123-openal-debuginfo-1.25.6-7.1
mpg123-devel-32bit-1.25.6-7.1
libmpg123-0-1.25.6-7.1
mpg123-esound-debuginfo-1.25.6-7.1
mpg123-jack-debuginfo-1.25.6-7.1
mpg123-esound-1.25.6-7.1
libout123-0-32bit-1.25.6-7.1
mpg123-openal-debuginfo-32bit-1.25.6-7.1
mpg123-sdl-debuginfo-32bit-1.25.6-7.1
mpg123-esound-32bit-1.25.6-7.1
libout123-0-debuginfo-32bit-1.25.6-7.1
mpg123-sdl-32bit-1.25.6-7.1
mpg123-pulse-1.25.6-7.1
libout123-0-debuginfo-1.25.6-7.1
mpg123-jack-1.25.6-7.1
mpg123-esound-debuginfo-32bit-1.25.6-7.1
libmpg123-0-debuginfo-32bit-1.25.6-7.1
mpg123-portaudio-debuginfo-32bit-1.25.6-7.1
mpg123-debuginfo-1.25.6-7.1
mpg123-devel-1.25.6-7.1
mpg123-pulse-debuginfo-32bit-1.25.6-7.1
mpg123-jack-32bit-1.25.6-7.1
libmpg123-0-32bit-1.25.6-7.1
libmpg123-0-debuginfo-1.25.6-7.1
mpg123-pulse-32bit-1.25.6-7.1
mpg123-sdl-1.25.6-7.1
mpg123-debugsource-1.25.6-7.1
mpg123-jack-debuginfo-32bit-1.25.6-7.1
mpg123-openal-32bit-1.25.6-7.1
mpg123-openal-1.25.6-7.1
mpg123-portaudio-32bit-1.25.6-7.1
mpg123-portaudio-debuginfo-1.25.6-7.1
mpg123-1.25.6-7.1
libout123-0-1.25.6-7.1
mpg123-portaudio-1.25.6-7.1
mpg123-sdl-debuginfo-1.25.6-7.1

i586
mpg123-jack-debuginfo-1.25.6-7.1
mpg123-pulse-debuginfo-1.25.6-7.1
mpg123-esound-debuginfo-1.25.6-7.1
libout123-0-debuginfo-1.25.6-7.1
mpg123-portaudio-debuginfo-1.25.6-7.1
mpg123-openal-1.25.6-7.1
mpg123-jack-1.25.6-7.1
mpg123-pulse-1.25.6-7.1
libmpg123-0-debuginfo-1.25.6-7.1
mpg123-debuginfo-1.25.6-7.1
libmpg123-0-1.25.6-7.1
mpg123-sdl-1.25.6-7.1
mpg123-openal-debuginfo-1.25.6-7.1
libout123-0-1.25.6-7.1
mpg123-portaudio-1.25.6-7.1
mpg123-debugsource-1.25.6-7.1
mpg123-1.25.6-7.1
mpg123-esound-1.25.6-7.1
mpg123-sdl-debuginfo-1.25.6-7.1
mpg123-devel-1.25.6-7.1

192606 - Fedora Linux 25 FEDORA-2017-a3a8638a60 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13693, CVE-2017-13694, CVE-2017-13695, CVE-2017-14051

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a3a8638a60

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-4.12.11-200.fc25

192616 - Fedora Linux 25 FEDORA-2017-deefb26e8b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12982

Description

The scan detected that the host is missing the following update:
FEDORA-2017-deefb26e8b

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=2

Fedora Core 25

openjpeg2-2.2.0-2.fc25
mingw-openjpeg2-2.2.0-2.fc25

192617 - Fedora Linux 26 FEDORA-2017-77e8bc720a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14102

Description

The scan detected that the host is missing the following update:
FEDORA-2017-77e8bc720a

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

mimedefang-2.81-1.fc26

192623 - Fedora Linux 25 FEDORA-2017-15ad4721e3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14102

Description

The scan detected that the host is missing the following update:
FEDORA-2017-15ad4721e3

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

mimedefang-2.81-1.fc25

192626 - Fedora Linux 26 FEDORA-2017-6764d16965 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13693, CVE-2017-13694, CVE-2017-13695, CVE-2017-14051

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6764d16965

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

kernel-4.12.11-300.fc26

130875 - Debian Linux 8.0, 9.0 DSA-3970-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-3970-1

Observation

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

http://www.debian.org/security/2017/dsa-3970

Debian 8.0
all
emacs24_24.4+1-5+deb8u1

Debian 9.0
all
emacs24_24.5+1-11+deb9u1

130876 - Debian Linux 8.0, 9.0 DSA-3968-1 Update Is Not Installed

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

Risk Level: Low

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-2017-7800, 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:
DSA-3968-1

Observation

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

http://www.debian.org/security/2017/dsa-3968

Debian 8.0

all
icedove_52.3.0-4~deb8u2

Debian 9.0
all
icedove_52.3.0-4~deb9u1

130877 - Debian Linux 9.0 DSA-3965-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000249

Description

The scan detected that the host is missing the following update:
DSA-3965-1

Observation

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

http://www.debian.org/security/2017/dsa-3965

Debian 9.0
all
file_1:5.30-1+deb9u1

130879 - Debian Linux 8.0, 9.0 DSA-3972-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000250

Description

The scan detected that the host is missing the following update:
DSA-3972-1

Observation

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

http://www.debian.org/security/2017/dsa-3972

Debian 8.0
all
bluez_5.23-2+deb8u1

Debian 9.0
all
bluez_5.43-2+deb9u1

182436 - FreeBSD Django Possible XSS In Traceback Section Of Technical 500 Debug Page (aaab03be-932d-11e7-92d8-4b26fc968492)

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

Risk Level: Low

CVE: CVE-2017-12794

Description

The scan detected that the host is missing the following update:
Django -- possible XSS in traceback section of technical 500 debug page (aaab03be-932d-11e7-92d8-4b26fc968492)

Observation

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

http://www.vuxml.org/freebsd/aaab03be-932d-11e7-92d8-4b26fc968492.html

Affected packages:
py27-django110 < 1.10.8
py34-django110 < 1.10.8
py35-django110 < 1.10.8
py36-django110 < 1.10.8
py27-django111 < 1.11.5
py34-django111 < 1.11.5
py35-django111 < 1.11.5
py36-django111 < 1.11.5

182437 - FreeBSD chromium Multiple Vulnerabilities (e1100e63-92f7-11e7-bd95-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (e1100e63-92f7-11e7-bd95-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/e1100e63-92f7-11e7-bd95-e8e0b747a45a.html

Affected packages:
chromium < 61.0.3163.79

182438 - FreeBSD emacs Enriched Text Remote Code Execution Vulnerability (47e2e52c-975c-11e7-942d-5404a68a61a2)

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:
emacs -- enriched text remote code execution vulnerability (47e2e52c-975c-11e7-942d-5404a68a61a2)

Observation

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

http://www.vuxml.org/freebsd/47e2e52c-975c-11e7-942d-5404a68a61a2.html

Affected packages:
emacs25 < 25.3,3
emacs-nox11 < 25.3,3
emacs-devel < 26.0.50.20170912,2

182439 - FreeBSD Flash Player Multiple Vulnerabilities (531aae08-97f0-11e7-aadd-6451062f0f7a)

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

Risk Level: Low

CVE: CVE-2017-11281, CVE-2017-11282

Description

The scan detected that the host is missing the following update:
Flash Player -- multiple vulnerabilities (531aae08-97f0-11e7-aadd-6451062f0f7a)

Observation

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

http://www.vuxml.org/freebsd/531aae08-97f0-11e7-aadd-6451062f0f7a.html

Affected packages:
linux-flashplayer < 27.0.0.130

182440 - FreeBSD cyrus-imapd Broken "other Users" Behaviour (f9f76a50-9642-11e7-ab09-080027b00c2e)

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

Risk Level: Low

CVE: CVE-2017-14230

Description

The scan detected that the host is missing the following update:
cyrus-imapd -- broken "other users" behaviour (f9f76a50-9642-11e7-ab09-080027b00c2e)

Observation

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

http://www.vuxml.org/freebsd/f9f76a50-9642-11e7-ab09-080027b00c2e.html

Affected packages:
3.0.0 <= cyrus-imapd30 < 3.0.4

185868 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3411-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3411-1

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/004038.html

Ubuntu 16.04

python-bzrlib_2.7.0-2ubuntu3.1
bzr_2.7.0-2ubuntu3.1

Ubuntu 14.04

python-bzrlib_2.6.0+bzr6593-1ubuntu1.6
bzr_2.6.0+bzr6593-1ubuntu1.6

Ubuntu 17.04

bzr_2.7.0+bzr6619-7ubuntu0.1
python-bzrlib_2.7.0+bzr6619-7ubuntu0.1

185869 - Ubuntu Linux 17.04 USN-3412-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000249

Description

The scan detected that the host is missing the following update:
USN-3412-1

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/004039.html

Ubuntu 17.04

libmagic1_5.29-3ubuntu0.1
file_5.29-3ubuntu0.1

185871 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3413-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000250

Description

The scan detected that the host is missing the following update:
USN-3413-1

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/004040.html

Ubuntu 16.04

bluez_5.37-0ubuntu5.1
libbluetooth3_5.37-0ubuntu5.1

Ubuntu 14.04

libbluetooth3_4.101-0ubuntu13.3
bluez_4.101-0ubuntu13.3

Ubuntu 17.04

bluez_5.43-0ubuntu1.1
libbluetooth3_5.43-0ubuntu1.1

192610 - Fedora Linux 25 FEDORA-2017-bdd0b565ef 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-bdd0b565ef

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=2

Fedora Core 25

thunderbird-52.3.0-1.fc25

192611 - Fedora Linux 26 FEDORA-2017-fe95a5b88b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000250

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fe95a5b88b

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

bluez-5.46-6.fc26

192612 - Fedora Linux 26 FEDORA-2017-a1dc0ef38c 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-a1dc0ef38c

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

emacs-25.3-1.fc26

192618 - Fedora Linux 25 FEDORA-2017-902970c18f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora 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:
FEDORA-2017-902970c18f

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=2

Fedora Core 25

drupal8-8.3.7-1.fc25

192621 - Fedora Linux 25 FEDORA-2017-c708c044e3 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-c708c044e3

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=2

Fedora Core 25

chromium-60.0.3112.113-1.fc25

192628 - Fedora Linux 26 FEDORA-2017-0fbd57c134 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora 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:
FEDORA-2017-0fbd57c134

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=2

Fedora Core 26

drupal8-8.3.7-1.fc26

192629 - Fedora Linux 26 FEDORA-2017-10c74147f9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-11462

Description

The scan detected that the host is missing the following update:
FEDORA-2017-10c74147f9

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=2

Fedora Core 26

krb5-1.15.1-28.fc26

192630 - Fedora Linux 26 FEDORA-2017-bb4c07b01a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000249

Description

The scan detected that the host is missing the following update:
FEDORA-2017-bb4c07b01a

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

file-5.30-11.fc26

22454 - Microsoft Office 2016 Click-To-Run September 2017 Updates

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

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

Observation

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

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

ENHANCED CHECKS

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

33152 - Oracle Solaris 119758-42 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-0452, CVE-2007-2444, CVE-2007-2446, CVE-2007-2447, CVE-2007-4138, CVE-2007-4572, CVE-2007-5398, CVE-2007-6015, CVE-2008-4314, CVE-2010-2063, CVE-2010-3069, CVE-2011-0719, CVE-2011-2522, CVE-2011-2694, CVE-2012-1182, CVE-2012-2111, CVE-2012-6150, CVE-2013-0213, CVE-2013-0214, CVE-2013-4124, CVE-2013-4408, CVE-2013-4475, CVE-2013-4496, CVE-2014-0178, CVE-2014-0244, CVE-2014-3493

Update Details

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

33154 - Oracle Solaris 119757-42 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-0452, CVE-2007-2444, CVE-2007-2446, CVE-2007-2447, CVE-2007-4138, CVE-2007-4572, CVE-2007-5398, CVE-2007-6015, CVE-2008-4314, CVE-2010-2063, CVE-2010-3069, CVE-2011-0719, CVE-2011-2522, CVE-2011-2694, CVE-2012-1182, CVE-2012-2111, CVE-2012-6150, CVE-2013-0213, CVE-2013-0214, CVE-2013-4124, CVE-2013-4408, CVE-2013-4475, CVE-2013-4496, CVE-2014-0178, CVE-2014-0244, CVE-2014-3493

Update Details

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

22367 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8748)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-8748

Update Details

Risk is updated

22369 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8741)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-8741

Update Details

Risk is updated

22371 - (MSPT-Sept2017) Microsoft Internet Explorer Memory Corruption Remote Code Execution (CVE-2017-8747)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-8747

Update Details

Risk is updated

22401 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8738)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-8738

Update Details

Risk is updated

22375 - (MSPT-Sept2017) Microsoft Windows Remote Desktop Protocol Remote Code Execution (CVE-2017-8714)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-8714

Update Details

Recommendation is updated

22380 - (MSPT-Sept2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-8719)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-8719

Update Details

Recommendation is updated

32172 - Oracle Solaris 137080-11 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-5266, CVE-2007-5267, CVE-2007-5268, CVE-2007-5269, CVE-2008-1382, CVE-2008-3964, CVE-2009-0040, CVE-2009-2042, CVE-2010-0205, CVE-2010-1205, CVE-2010-2249, CVE-2011-2690, CVE-2011-2691, CVE-2011-2692, CVE-2011-3026, CVE-2011-3048

Update Details

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

32179 - Oracle Solaris 137081-11 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-5266, CVE-2007-5267, CVE-2007-5268, CVE-2007-5269, CVE-2008-1382, CVE-2008-3964, CVE-2009-0040, CVE-2009-2042, CVE-2010-0205, CVE-2010-1205, CVE-2010-2249, CVE-2011-2690, CVE-2011-2691, CVE-2011-2692, CVE-2011-3026, CVE-2011-3048

Update Details

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

33040 - Oracle Solaris 148310-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-5365, CVE-2015-2662

Update Details

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

33060 - Oracle Solaris 148309-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-5365, CVE-2015-2662

Update Details

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

33145 - Oracle Solaris 150401-55 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5544, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122

Update Details

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

181439 - FreeBSD security/ossec-hids-* Root Escalation Via Syscheck Feature (c470db07-1098-11e5-b6a8-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-3222

Update Details

Risk is updated

22360 - (MSPT-Sept2017) Microsoft Windows Security Security Bypass (CVE-2017-8716)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8716

Update Details

Recommendation is updated

22361 - (MSPT-Sept2017) Microsoft Windows Hyper-V Information Disclosure (CVE-2017-8713)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8713

Update Details

Observation is updated Recommendation is updated

22362 - (MSPT-Sept2017) Microsoft Windows Hyper-V Information Disclosure (CVE-2017-8712)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8712

Update Details

Observation is updated Recommendation is updated

22363 - (MSPT-Sept2017) Microsoft Windows Hyper-V Information Disclosure (CVE-2017-8711)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8711

Update Details

Observation is updated Recommendation is updated

22376 - (MSPT-Sept2017) Microsoft Windows Device Guard Security Bypass (CVE-2017-8746)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8746

Update Details

Risk is updated

22410 - (MSPT-Sept2017) Microsoft Office PowerPoint Remote Code Execution (CVE-2017-8743)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8743

Update Details

Risk is updated

22417 - (MSPT-Sept2017) Microsoft Windows System Information Console Information Disclosure (CVE-2017-8710)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8710

Update Details

Recommendation is updated

22425 - (MSPT-Sept2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-8709)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8709

Update Details

Observation is updated Recommendation is updated

189632 - Fedora Linux 21 FEDORA-2015-12716 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5704, CVE-2015-5705

Update Details

Risk is updated

189648 - Fedora Linux 21 FEDORA-2015-13471 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5186

Update Details

Risk is updated

189663 - Fedora Linux 22 FEDORA-2015-12699 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5704, CVE-2015-5705

Update Details

Risk is updated

189676 - Fedora Linux 22 FEDORA-2015-13526 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5186

Update Details

Risk is updated

22433 - (MSPT-Sept2017) Microsoft Edge Security Security Bypass (CVE-2017-8723)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-8723

Update Details

Observation is updated

33162 - Oracle Solaris 150400-55 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122

Update Details

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

33360 - Oracle Solaris 152510-06 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33364 - Oracle Solaris 152511-06 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33365 - Oracle Solaris 152644-05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33366 - Oracle Solaris 152643-05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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