

MCAFFEE 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

141444 - Red Hat Enterprise Linux RHSA-2017-0196 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

The scan detected that the host is missing the following update:
RHSA-2017-0196

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0196.html>

RHEL6_4S

x86_64

kernel-headers-2.6.32-358.76.1.el6

kernel-debug-2.6.32-358.76.1.el6

kernel-2.6.32-358.76.1.el6

perf-2.6.32-358.76.1.el6

kernel-debug-devel-2.6.32-358.76.1.el6

python-perf-debuginfo-2.6.32-358.76.1.el6

python-perf-2.6.32-358.76.1.el6

kernel-debuginfo-2.6.32-358.76.1.el6

kernel-debuginfo-common-x86_64-2.6.32-358.76.1.el6

kernel-devel-2.6.32-358.76.1.el6

kernel-debug-debuginfo-2.6.32-358.76.1.el6

perf-debuginfo-2.6.32-358.76.1.el6

noarch

kernel-firmware-2.6.32-358.76.1.el6

kernel-doc-2.6.32-358.76.1.el6

141445 - Red Hat Enterprise Linux RHSA-2017-0031 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

The scan detected that the host is missing the following update:
RHSA-2017-0031

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0031.html>

RHEL6_7S

i386

kernel-devel-2.6.32-573.38.1.el6

kernel-headers-2.6.32-573.38.1.el6

perf-debuginfo-2.6.32-573.38.1.el6

kernel-debuginfo-common-i686-2.6.32-573.38.1.el6

python-perf-2.6.32-573.38.1.el6

kernel-debuginfo-2.6.32-573.38.1.el6

kernel-debug-debuginfo-2.6.32-573.38.1.el6

kernel-2.6.32-573.38.1.el6

python-perf-debuginfo-2.6.32-573.38.1.el6

kernel-debug-devel-2.6.32-573.38.1.el6

kernel-debug-2.6.32-573.38.1.el6

perf-2.6.32-573.38.1.el6

noarch

kernel-firmware-2.6.32-573.38.1.el6

kernel-abi-whitelists-2.6.32-573.38.1.el6

kernel-doc-2.6.32-573.38.1.el6

x86_64

python-perf-debuginfo-2.6.32-573.38.1.el6

kernel-2.6.32-573.38.1.el6

kernel-debuginfo-2.6.32-573.38.1.el6

python-perf-2.6.32-573.38.1.el6

kernel-debuginfo-common-x86_64-2.6.32-573.38.1.el6

kernel-debug-2.6.32-573.38.1.el6

kernel-debug-debuginfo-2.6.32-573.38.1.el6

perf-2.6.32-573.38.1.el6

kernel-debug-devel-2.6.32-573.38.1.el6

kernel-headers-2.6.32-573.38.1.el6

kernel-debuginfo-common-i686-2.6.32-573.38.1.el6

kernel-devel-2.6.32-573.38.1.el6

perf-debuginfo-2.6.32-573.38.1.el6

141447 - Red Hat Enterprise Linux RHSA-2017-0065 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

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

RHSA-2017-0065

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0065.html>

RHEL6_5S
x86_64
perf-debuginfo-2.6.32-431.77.1.el6
kernel-debuginfo-2.6.32-431.77.1.el6
kernel-2.6.32-431.77.1.el6
python-perf-debuginfo-2.6.32-431.77.1.el6
python-perf-2.6.32-431.77.1.el6
kernel-debug-debuginfo-2.6.32-431.77.1.el6
kernel-devel-2.6.32-431.77.1.el6
kernel-debug-devel-2.6.32-431.77.1.el6
kernel-debuginfo-common-x86_64-2.6.32-431.77.1.el6
kernel-headers-2.6.32-431.77.1.el6
kernel-debug-2.6.32-431.77.1.el6
perf-2.6.32-431.77.1.el6

noarch
kernel-abi-whitelists-2.6.32-431.77.1.el6
kernel-firmware-2.6.32-431.77.1.el6
kernel-doc-2.6.32-431.77.1.el6

141451 - Red Hat Enterprise Linux RHSA-2017-0216 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

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

RHSA-2017-0216

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0216.html>

RHEL6_6S
x86_64
kernel-2.6.32-504.56.1.el6
kernel-debuginfo-common-x86_64-2.6.32-504.56.1.el6
perf-debuginfo-2.6.32-504.56.1.el6
kernel-debuginfo-2.6.32-504.56.1.el6
kernel-devel-2.6.32-504.56.1.el6
perf-2.6.32-504.56.1.el6
kernel-debug-2.6.32-504.56.1.el6
python-perf-2.6.32-504.56.1.el6
python-perf-debuginfo-2.6.32-504.56.1.el6
kernel-headers-2.6.32-504.56.1.el6
kernel-debug-debuginfo-2.6.32-504.56.1.el6
kernel-debug-devel-2.6.32-504.56.1.el6

noarch
kernel-firmware-2.6.32-504.56.1.el6
kernel-abi-whitelists-2.6.32-504.56.1.el6
kernel-doc-2.6.32-504.56.1.el6

141454 - Red Hat Enterprise Linux RHSA-2017-0270 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

Description

The scan detected that the host is missing the following update:
RHSA-2017-0270

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0270.html>

RHEL7_1S

noarch

kernel-doc-3.10.0-229.48.1.el7

kernel-abi-whitelists-3.10.0-229.48.1.el7

x86_64

kernel-3.10.0-229.48.1.el7

kernel-debuginfo-3.10.0-229.48.1.el7

kernel-debug-3.10.0-229.48.1.el7

kernel-tools-libs-devel-3.10.0-229.48.1.el7

python-perf-3.10.0-229.48.1.el7

kernel-debuginfo-common-x86_64-3.10.0-229.48.1.el7

kernel-headers-3.10.0-229.48.1.el7

python-perf-debuginfo-3.10.0-229.48.1.el7

perf-3.10.0-229.48.1.el7

perf-debuginfo-3.10.0-229.48.1.el7

kernel-tools-libs-3.10.0-229.48.1.el7

kernel-tools-debuginfo-3.10.0-229.48.1.el7

kernel-tools-3.10.0-229.48.1.el7

kernel-debug-debuginfo-3.10.0-229.48.1.el7

kernel-devel-3.10.0-229.48.1.el7

kernel-debug-devel-3.10.0-229.48.1.el7

145243 - SuSE SLES 11 SP4 SUSE-SU-2017:0585-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2108, CVE-2016-7056, CVE-2016-8610

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0585-1

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-March/002670.html>

SuSE SLES 11 SP4

i586

libopenssl0_9_8-0.9.8j-0.105.1

libopenssl0_9_8-hmac-0.9.8j-0.105.1
openssl-0.9.8j-0.105.1
openssl-doc-0.9.8j-0.105.1

x86_64
openssl-0.9.8j-0.105.1
openssl-doc-0.9.8j-0.105.1
libopenssl0_9_8-hmac-32bit-0.9.8j-0.105.1
libopenssl0_9_8-hmac-0.9.8j-0.105.1
libopenssl0_9_8-32bit-0.9.8j-0.105.1
libopenssl0_9_8-0.9.8j-0.105.1

145245 - SuSE SLED 12 SP1, 12 SP2 SUSE-SU-2017:0605-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2108, CVE-2016-7056, CVE-2016-8610

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0605-1

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-March/002678.html>

SuSE SLED 12 SP2

x86_64
libopenssl0_9_8-debuginfo-0.9.8j-105.1
libopenssl0_9_8-debuginfo-32bit-0.9.8j-105.1
libopenssl0_9_8-0.9.8j-105.1
libopenssl0_9_8-32bit-0.9.8j-105.1
compat-openssl098-debugsource-0.9.8j-105.1

SuSE SLED 12 SP1

x86_64
libopenssl0_9_8-debuginfo-0.9.8j-105.1
libopenssl0_9_8-debuginfo-32bit-0.9.8j-105.1
libopenssl0_9_8-0.9.8j-105.1
libopenssl0_9_8-32bit-0.9.8j-105.1
compat-openssl098-debugsource-0.9.8j-105.1

21240 - VIPA Controls WinPLC7 Stack Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2017-5177

Description

A vulnerability is present in some versions of VIPA Controls WinPLC7.

Observation

VIPA Controls WinPLC7 is a SCADA/HMI application development platform.

A vulnerability is present in some versions of VIPA Controls WinPLC7. The flaw lies in the management of network packet. Successful exploitation could allow a remote attacker to execute remote code or cause a denial of service condition.

21300 - NVIDIA Windows Drivers Multiple Vulnerabilities 02-2017

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

Risk Level: High

CVE: CVE-2017-0308, CVE-2017-0309, CVE-2017-0310, CVE-2017-0311, CVE-2017-0312, CVE-2017-0313, CVE-2017-0314, CVE-2017-0315, CVE-2017-0319, CVE-2017-0320, CVE-2017-0321, CVE-2017-0322, CVE-2017-0323, CVE-2017-0324

Description

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

Observation

NVIDIA is a technology company which manufactures graphics processing units.

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers. The flaws occur within the kernel mode layer. Successful exploitation could allow an attacker to escalate privileges or cause a denial of service condition.

21307 - (K31510510) F5 BIG-IP OpenSSH Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-6515

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw is due to improper handling of a long string for password authentication. Successful exploitation could allow an attacker to cause a denial of service condition.

21310 - Splunk Enterprise Persistent Cross Site Scripting Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A cross-site scripting vulnerability is present in some versions of Splunk Enterprise.

Observation

Splunk Enterprise is a platform for real-time operational intelligence.

A cross-site scripting vulnerability is present in some versions of Splunk Enterprise. The flaw lies in all components running Splunk Web. Successful exploitation could allow an attacker to inject and store arbitrary scripts.

21311 - (SOL24923910) F5 BIG-IP LibTIFF Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-3632

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in LibTIFF component. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

21312 - (K28056114) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5829

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Linux kernel drivers. Successful exploitation could allow an attacker to corrupt kernel memory, escalate privileges or cause a denial of service condition.

21313 - (K70938105) F5 BIG-IP Expat XML Library Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5300

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the XML parser in Expat. Successful exploitation could allow an attacker to cause a denial of service condition.

21323 - (K10558632) F5 BIG-IP Linux Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5195

Description

A race condition 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 race condition vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the Linux kernel. Successful exploitation could allow a local attacker to escalate privileges.

130713 - Debian Linux 8.0 DSA-3802-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10134

Description

The scan detected that the host is missing the following update:
DSA-3802-1

Observation

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

<http://www.debian.org/security/2017/dsa-3802>

Debian 8.0

all

zabbix-server-mysql_1:2.2.7+dfsg-2+deb8u2

zabbix-proxy-sqlite3_1:2.2.7+dfsg-2+deb8u2

zabbix-frontend-php_1:2.2.7+dfsg-2+deb8u2

zabbix-server-pgsql_1:2.2.7+dfsg-2+deb8u2

zabbix-proxy-pgsql_1:2.2.7+dfsg-2+deb8u2

zabbix-java-gateway_1:2.2.7+dfsg-2+deb8u2

zabbix-proxy-mysql_1:2.2.7+dfsg-2+deb8u2

zabbix-agent_1:2.2.7+dfsg-2+deb8u2

130715 - Debian Linux 8.0 DSA-3801-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5946

Description

The scan detected that the host is missing the following update:
DSA-3801-1

Observation

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

<http://www.debian.org/security/2017/dsa-3801>

Debian 8.0

all

ruby-zip_1.1.6-1+deb8u1

132343 - Oracle VM OVMSA-2017-0047 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2620

Description

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

OVMSA-2017-0047

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000656.html>

OVM3.4

x86_64

qemu-img-0.12.1.2-2.491.el6_8.7

141438 - Red Hat Enterprise Linux RHSA-2017-0324 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

Description

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

RHSA-2017-0324

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0324.html>

RHEL6_6S

x86_64

perf-debuginfo-2.6.32-504.57.1.el6

kernel-debug-devel-2.6.32-504.57.1.el6

kernel-debuginfo-common-x86_64-2.6.32-504.57.1.el6

kernel-2.6.32-504.57.1.el6

python-perf-2.6.32-504.57.1.el6

kernel-devel-2.6.32-504.57.1.el6

kernel-debug-debuginfo-2.6.32-504.57.1.el6

python-perf-debuginfo-2.6.32-504.57.1.el6

kernel-debuginfo-2.6.32-504.57.1.el6

kernel-debug-2.6.32-504.57.1.el6

perf-2.6.32-504.57.1.el6

kernel-headers-2.6.32-504.57.1.el6

noarch

kernel-firmware-2.6.32-504.57.1.el6

kernel-doc-2.6.32-504.57.1.el6

kernel-abi-whitelists-2.6.32-504.57.1.el6

141439 - Red Hat Enterprise Linux RHSA-2017-0396 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2615, CVE-2017-2620

Description

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

RHSA-2017-0396

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0396.html>

RHEL7D

x86_64

qemu-kvm-tools-1.5.3-126.el7_3.5

qemu-kvm-common-1.5.3-126.el7_3.5

qemu-kvm-debuginfo-1.5.3-126.el7_3.5

qemu-img-1.5.3-126.el7_3.5

qemu-kvm-1.5.3-126.el7_3.5

RHEL7S

x86_64

qemu-kvm-tools-1.5.3-126.el7_3.5

qemu-kvm-common-1.5.3-126.el7_3.5

qemu-kvm-debuginfo-1.5.3-126.el7_3.5

qemu-img-1.5.3-126.el7_3.5

qemu-kvm-1.5.3-126.el7_3.5

RHEL7WS

x86_64

qemu-kvm-tools-1.5.3-126.el7_3.5

qemu-kvm-common-1.5.3-126.el7_3.5

qemu-kvm-debuginfo-1.5.3-126.el7_3.5

qemu-img-1.5.3-126.el7_3.5

qemu-kvm-1.5.3-126.el7_3.5

141440 - Red Hat Enterprise Linux RHSA-2017-0386 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084

Description

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

RHSA-2017-0386

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0386.html>

RHEL7D

x86_64

kernel-debug-debuginfo-3.10.0-514.10.2.el7
perf-debuginfo-3.10.0-514.10.2.el7
kernel-debug-3.10.0-514.10.2.el7
kernel-tools-debuginfo-3.10.0-514.10.2.el7
kernel-debuginfo-3.10.0-514.10.2.el7
kernel-tools-3.10.0-514.10.2.el7
kernel-debug-devel-3.10.0-514.10.2.el7
kernel-devel-3.10.0-514.10.2.el7
kernel-headers-3.10.0-514.10.2.el7
python-perf-3.10.0-514.10.2.el7
kernel-debuginfo-common-x86_64-3.10.0-514.10.2.el7
python-perf-debuginfo-3.10.0-514.10.2.el7
kernel-3.10.0-514.10.2.el7
kernel-tools-libs-3.10.0-514.10.2.el7
perf-3.10.0-514.10.2.el7
kernel-tools-libs-devel-3.10.0-514.10.2.el7

noarch
kernel-doc-3.10.0-514.10.2.el7
kernel-abi-whitelists-3.10.0-514.10.2.el7

RHEL7S

noarch
kernel-doc-3.10.0-514.10.2.el7
kernel-abi-whitelists-3.10.0-514.10.2.el7

x86_64

kernel-debug-debuginfo-3.10.0-514.10.2.el7
perf-debuginfo-3.10.0-514.10.2.el7
kernel-debug-3.10.0-514.10.2.el7
kernel-tools-debuginfo-3.10.0-514.10.2.el7
kernel-debuginfo-3.10.0-514.10.2.el7
kernel-tools-3.10.0-514.10.2.el7
kernel-debug-devel-3.10.0-514.10.2.el7
kernel-devel-3.10.0-514.10.2.el7
kernel-headers-3.10.0-514.10.2.el7
python-perf-3.10.0-514.10.2.el7
kernel-debuginfo-common-x86_64-3.10.0-514.10.2.el7
python-perf-debuginfo-3.10.0-514.10.2.el7
kernel-3.10.0-514.10.2.el7
kernel-tools-libs-3.10.0-514.10.2.el7
perf-3.10.0-514.10.2.el7
kernel-tools-libs-devel-3.10.0-514.10.2.el7

RHEL7WS

x86_64
kernel-debug-debuginfo-3.10.0-514.10.2.el7
perf-debuginfo-3.10.0-514.10.2.el7
kernel-debug-3.10.0-514.10.2.el7
kernel-tools-debuginfo-3.10.0-514.10.2.el7
kernel-debuginfo-3.10.0-514.10.2.el7
kernel-tools-3.10.0-514.10.2.el7
kernel-debug-devel-3.10.0-514.10.2.el7
kernel-devel-3.10.0-514.10.2.el7
kernel-headers-3.10.0-514.10.2.el7
python-perf-3.10.0-514.10.2.el7
kernel-debuginfo-common-x86_64-3.10.0-514.10.2.el7
python-perf-debuginfo-3.10.0-514.10.2.el7
kernel-3.10.0-514.10.2.el7
kernel-tools-libs-3.10.0-514.10.2.el7

perf-3.10.0-514.10.2.el7
kernel-tools-libs-devel-3.10.0-514.10.2.el7

noarch
kernel-doc-3.10.0-514.10.2.el7
kernel-abi-whitelists-3.10.0-514.10.2.el7

141441 - Red Hat Enterprise Linux RHSA-2017-0352 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2620

Description

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

RHSA-2017-0352

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0352.html>

RHEL6D

x86_64

qemu-kvm-0.12.1.2-2.491.el6_8.7
qemu-kvm-tools-0.12.1.2-2.491.el6_8.7
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.7
qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-img-0.12.1.2-2.491.el6_8.7

i386

qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.7

RHEL6S

i386

qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.7

x86_64

qemu-kvm-0.12.1.2-2.491.el6_8.7
qemu-kvm-tools-0.12.1.2-2.491.el6_8.7
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.7
qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-img-0.12.1.2-2.491.el6_8.7

RHEL6WS

x86_64

qemu-kvm-0.12.1.2-2.491.el6_8.7
qemu-kvm-tools-0.12.1.2-2.491.el6_8.7
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.7
qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-img-0.12.1.2-2.491.el6_8.7

i386

qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.7

141446 - Red Hat Enterprise Linux RHSA-2017-0366 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

Description

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

RHSA-2017-0366

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0366.html>

RHEL6_5S

x86_64

kernel-2.6.32-431.78.1.el6

kernel-debug-2.6.32-431.78.1.el6

kernel-debuginfo-common-x86_64-2.6.32-431.78.1.el6

kernel-debug-devel-2.6.32-431.78.1.el6

perf-debuginfo-2.6.32-431.78.1.el6

kernel-headers-2.6.32-431.78.1.el6

kernel-debuginfo-2.6.32-431.78.1.el6

python-perf-debuginfo-2.6.32-431.78.1.el6

python-perf-2.6.32-431.78.1.el6

kernel-devel-2.6.32-431.78.1.el6

perf-2.6.32-431.78.1.el6

kernel-debug-debuginfo-2.6.32-431.78.1.el6

noarch

kernel-firmware-2.6.32-431.78.1.el6

kernel-doc-2.6.32-431.78.1.el6

kernel-abi-whitelists-2.6.32-431.78.1.el6

141448 - Red Hat Enterprise Linux RHSA-2017-0345 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

Description

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

RHSA-2017-0345

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0345.html>

RHEL6_4S

x86_64

kernel-debuginfo-common-x86_64-2.6.32-358.77.1.el6

kernel-debug-debuginfo-2.6.32-358.77.1.el6
kernel-debuginfo-2.6.32-358.77.1.el6
perf-2.6.32-358.77.1.el6
kernel-devel-2.6.32-358.77.1.el6
python-perf-debuginfo-2.6.32-358.77.1.el6
perf-debuginfo-2.6.32-358.77.1.el6
kernel-debug-devel-2.6.32-358.77.1.el6
python-perf-2.6.32-358.77.1.el6
kernel-headers-2.6.32-358.77.1.el6
kernel-2.6.32-358.77.1.el6
kernel-debug-2.6.32-358.77.1.el6

noarch
kernel-doc-2.6.32-358.77.1.el6
kernel-firmware-2.6.32-358.77.1.el6

141450 - Red Hat Enterprise Linux RHSA-2017-0347 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2634, CVE-2017-6074

Description

The scan detected that the host is missing the following update:
RHSA-2017-0347

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0347.html>

RHEL5_6S

i386
kernel-PAE-devel-2.6.18-238.58.1.el5
kernel-xen-debuginfo-2.6.18-238.58.1.el5
kernel-xen-devel-2.6.18-238.58.1.el5
kernel-debuginfo-2.6.18-238.58.1.el5
kernel-debug-debuginfo-2.6.18-238.58.1.el5
kernel-PAE-2.6.18-238.58.1.el5
kernel-debug-2.6.18-238.58.1.el5
kernel-xen-2.6.18-238.58.1.el5
kernel-PAE-debuginfo-2.6.18-238.58.1.el5
kernel-headers-2.6.18-238.58.1.el5
kernel-2.6.18-238.58.1.el5
kernel-debug-devel-2.6.18-238.58.1.el5
kernel-debuginfo-common-2.6.18-238.58.1.el5
kernel-devel-2.6.18-238.58.1.el5

noarch
kernel-doc-2.6.18-238.58.1.el5

x86_64

kernel-xen-2.6.18-238.58.1.el5
kernel-headers-2.6.18-238.58.1.el5
kernel-2.6.18-238.58.1.el5
kernel-debug-2.6.18-238.58.1.el5
kernel-debug-devel-2.6.18-238.58.1.el5

kernel-debuginfo-2.6.18-238.58.1.el5
kernel-xen-debuginfo-2.6.18-238.58.1.el5
kernel-debug-debuginfo-2.6.18-238.58.1.el5
kernel-xen-devel-2.6.18-238.58.1.el5
kernel-debuginfo-common-2.6.18-238.58.1.el5
kernel-devel-2.6.18-238.58.1.el5

141453 - Red Hat Enterprise Linux RHSA-2017-0403 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

Description

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

RHSA-2017-0403

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0403.html>

RHEL7_1S

noarch

kernel-doc-3.10.0-229.49.1.el7

kernel-abi-whitelists-3.10.0-229.49.1.el7

x86_64

kernel-tools-3.10.0-229.49.1.el7

kernel-devel-3.10.0-229.49.1.el7

kernel-tools-debuginfo-3.10.0-229.49.1.el7

kernel-tools-libs-3.10.0-229.49.1.el7

perf-3.10.0-229.49.1.el7

python-perf-debuginfo-3.10.0-229.49.1.el7

perf-debuginfo-3.10.0-229.49.1.el7

kernel-debuginfo-common-x86_64-3.10.0-229.49.1.el7

kernel-debuginfo-3.10.0-229.49.1.el7

kernel-tools-libs-devel-3.10.0-229.49.1.el7

kernel-debug-3.10.0-229.49.1.el7

kernel-debug-devel-3.10.0-229.49.1.el7

kernel-headers-3.10.0-229.49.1.el7

kernel-debug-debuginfo-3.10.0-229.49.1.el7

python-perf-3.10.0-229.49.1.el7

kernel-3.10.0-229.49.1.el7

141455 - Red Hat Enterprise Linux RHSA-2017-0004 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8666

Description

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

RHSA-2017-0004

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0004.html>

RHEL7_1S

noarch

kernel-abi-whitelists-3.10.0-229.46.1.el7

kernel-doc-3.10.0-229.46.1.el7

x86_64

kernel-debuginfo-3.10.0-229.46.1.el7

kernel-devel-3.10.0-229.46.1.el7

kernel-debug-devel-3.10.0-229.46.1.el7

kernel-tools-debuginfo-3.10.0-229.46.1.el7

kernel-debug-debuginfo-3.10.0-229.46.1.el7

kernel-headers-3.10.0-229.46.1.el7

kernel-tools-libs-3.10.0-229.46.1.el7

kernel-tools-libs-devel-3.10.0-229.46.1.el7

kernel-debuginfo-common-x86_64-3.10.0-229.46.1.el7

kernel-3.10.0-229.46.1.el7

kernel-debug-3.10.0-229.46.1.el7

perf-debuginfo-3.10.0-229.46.1.el7

kernel-tools-3.10.0-229.46.1.el7

python-perf-debuginfo-3.10.0-229.46.1.el7

python-perf-3.10.0-229.46.1.el7

perf-3.10.0-229.46.1.el7

141456 - Red Hat Enterprise Linux RHSA-2017-0365 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

Description

The scan detected that the host is missing the following update:
RHSA-2017-0365

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0365.html>

RHEL6_2S

x86_64

kernel-headers-2.6.32-220.70.1.el6

perf-2.6.32-220.70.1.el6

kernel-debug-2.6.32-220.70.1.el6

python-perf-debuginfo-2.6.32-220.70.1.el6

kernel-debuginfo-common-x86_64-2.6.32-220.70.1.el6

kernel-2.6.32-220.70.1.el6

perf-debuginfo-2.6.32-220.70.1.el6

kernel-debug-debuginfo-2.6.32-220.70.1.el6

kernel-debuginfo-2.6.32-220.70.1.el6

kernel-devel-2.6.32-220.70.1.el6

python-perf-2.6.32-220.70.1.el6

kernel-debug-devel-2.6.32-220.70.1.el6

noarch

kernel-doc-2.6.32-220.70.1.el6

kernel-firmware-2.6.32-220.70.1.el6

141457 - Red Hat Enterprise Linux RHSA-2017-0316 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

Description

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

RHSA-2017-0316

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0316.html>

RHEL6_7S

i386

kernel-debuginfo-common-i686-2.6.32-573.40.1.el6

kernel-headers-2.6.32-573.40.1.el6

kernel-debuginfo-2.6.32-573.40.1.el6

python-perf-2.6.32-573.40.1.el6

perf-debuginfo-2.6.32-573.40.1.el6

kernel-debug-devel-2.6.32-573.40.1.el6

kernel-devel-2.6.32-573.40.1.el6

perf-2.6.32-573.40.1.el6

kernel-2.6.32-573.40.1.el6

python-perf-debuginfo-2.6.32-573.40.1.el6

kernel-debug-debuginfo-2.6.32-573.40.1.el6

kernel-debug-2.6.32-573.40.1.el6

noarch

kernel-doc-2.6.32-573.40.1.el6

kernel-firmware-2.6.32-573.40.1.el6

kernel-abi-whitelists-2.6.32-573.40.1.el6

x86_64

kernel-debuginfo-common-x86_64-2.6.32-573.40.1.el6

kernel-debuginfo-2.6.32-573.40.1.el6

perf-debuginfo-2.6.32-573.40.1.el6

python-perf-debuginfo-2.6.32-573.40.1.el6

kernel-debug-2.6.32-573.40.1.el6

kernel-2.6.32-573.40.1.el6

kernel-headers-2.6.32-573.40.1.el6

kernel-debug-devel-2.6.32-573.40.1.el6

python-perf-2.6.32-573.40.1.el6

kernel-debug-debuginfo-2.6.32-573.40.1.el6

kernel-devel-2.6.32-573.40.1.el6

kernel-debuginfo-common-i686-2.6.32-573.40.1.el6

perf-2.6.32-573.40.1.el6

141458 - Red Hat Enterprise Linux RHSA-2017-0346 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2634, CVE-2017-6074

Description

The scan detected that the host is missing the following update:
RHSA-2017-0346

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0346.html>

RHEL5_9S

i386

kernel-headers-2.6.18-348.33.1.el5
kernel-debuginfo-common-2.6.18-348.33.1.el5
kernel-PAE-devel-2.6.18-348.33.1.el5
kernel-2.6.18-348.33.1.el5
kernel-debug-2.6.18-348.33.1.el5
kernel-debuginfo-2.6.18-348.33.1.el5
kernel-PAE-debuginfo-2.6.18-348.33.1.el5
kernel-xen-devel-2.6.18-348.33.1.el5
kernel-debug-debuginfo-2.6.18-348.33.1.el5
kernel-PAE-2.6.18-348.33.1.el5
kernel-xen-debuginfo-2.6.18-348.33.1.el5
kernel-devel-2.6.18-348.33.1.el5
kernel-xen-2.6.18-348.33.1.el5
kernel-debug-devel-2.6.18-348.33.1.el5

noarch

kernel-doc-2.6.18-348.33.1.el5

x86_64

kernel-xen-devel-2.6.18-348.33.1.el5
kernel-debug-devel-2.6.18-348.33.1.el5
kernel-devel-2.6.18-348.33.1.el5
kernel-xen-2.6.18-348.33.1.el5
kernel-debug-debuginfo-2.6.18-348.33.1.el5
kernel-2.6.18-348.33.1.el5
kernel-debuginfo-2.6.18-348.33.1.el5
kernel-headers-2.6.18-348.33.1.el5
kernel-xen-debuginfo-2.6.18-348.33.1.el5
kernel-debuginfo-common-2.6.18-348.33.1.el5
kernel-debug-2.6.18-348.33.1.el5

145241 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0622-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10207, CVE-2016-9941, CVE-2016-9942

Description

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

SUSE-SU-2017:0622-1

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-March/002682.html>

SuSE SLED 12 SP2

x86_64
libXvnc1-debuginfo-1.6.0-16.4
xorg-x11-Xvnc-1.6.0-16.4
libXvnc1-1.6.0-16.4
tigervnc-debuginfo-1.6.0-16.4
tigervnc-1.6.0-16.4
xorg-x11-Xvnc-debuginfo-1.6.0-16.4
tigervnc-debugsource-1.6.0-16.4

SuSE SLES 12 SP2

x86_64
libXvnc1-debuginfo-1.6.0-16.4
xorg-x11-Xvnc-1.6.0-16.4
libXvnc1-1.6.0-16.4
tigervnc-debuginfo-1.6.0-16.4
tigervnc-1.6.0-16.4
xorg-x11-Xvnc-debuginfo-1.6.0-16.4
tigervnc-debugsource-1.6.0-16.4

145242 - SuSE SLES 11 SP4 SUSE-SU-2017:0603-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10009, CVE-2016-10011, CVE-2016-8858

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0603-1

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-March/002677.html>

SuSE SLES 11 SP4

i586
openssh-askpass-gnome-6.6p1-35.4
openssh-helpers-6.6p1-35.1
openssh-6.6p1-35.1
openssh-fips-6.6p1-35.1

x86_64

openssh-askpass-gnome-6.6p1-35.4
openssh-helpers-6.6p1-35.1
openssh-6.6p1-35.1
openssh-fips-6.6p1-35.1

145247 - SuSE SLES 12 SP1 SUSE-SU-2017:0607-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10009, CVE-2016-10011, CVE-2016-8858

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0607-1

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-March/002680.html>

SuSE SLES 12 SP1

x86_64

openssh-askpass-gnome-debuginfo-6.6p1-54.7.1

openssh-6.6p1-54.7.1

openssh-helpers-debuginfo-6.6p1-54.7.1

openssh-debuginfo-6.6p1-54.7.1

openssh-debugsource-6.6p1-54.7.1

openssh-fips-6.6p1-54.7.1

openssh-helpers-6.6p1-54.7.1

openssh-askpass-gnome-6.6p1-54.7.1

145248 - SuSE SLES 11 SP4 SUSE-SU-2017:0595-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3135

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0595-1

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-March/002673.html>

SuSE SLES 11 SP4

i586

bind-doc-9.9.6P1-0.39.1

bind-libs-9.9.6P1-0.39.1

bind-chrootenv-9.9.6P1-0.39.1

bind-9.9.6P1-0.39.1

bind-utils-9.9.6P1-0.39.1

x86_64

bind-utils-9.9.6P1-0.39.1

bind-doc-9.9.6P1-0.39.1

bind-9.9.6P1-0.39.1

bind-chrootenv-9.9.6P1-0.39.1

bind-libs-9.9.6P1-0.39.1
bind-libs-32bit-9.9.6P1-0.39.1

145249 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0596-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3135

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0596-1

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-March/002674.html>

SuSE SLED 12 SP1

x86_64
bind-debuginfo-9.9.9P1-56.1
bind-libs-32bit-9.9.9P1-56.1
bind-utils-debuginfo-9.9.9P1-56.1
bind-debugsource-9.9.9P1-56.1
bind-libs-debuginfo-9.9.9P1-56.1
bind-libs-9.9.9P1-56.1
bind-utils-9.9.9P1-56.1
bind-libs-debuginfo-32bit-9.9.9P1-56.1

SuSE SLES 12 SP2

noarch
bind-doc-9.9.9P1-56.1

x86_64

bind-chrootenv-9.9.9P1-56.1
bind-debuginfo-9.9.9P1-56.1
bind-libs-debuginfo-9.9.9P1-56.1
bind-utils-debuginfo-9.9.9P1-56.1
bind-debugsource-9.9.9P1-56.1
bind-9.9.9P1-56.1
bind-utils-9.9.9P1-56.1
bind-libs-32bit-9.9.9P1-56.1
bind-libs-debuginfo-32bit-9.9.9P1-56.1
bind-libs-9.9.9P1-56.1

SuSE SLED 12 SP2

x86_64
bind-debuginfo-9.9.9P1-56.1
bind-libs-32bit-9.9.9P1-56.1
bind-utils-debuginfo-9.9.9P1-56.1
bind-debugsource-9.9.9P1-56.1
bind-libs-debuginfo-9.9.9P1-56.1
bind-libs-9.9.9P1-56.1
bind-utils-9.9.9P1-56.1
bind-libs-debuginfo-32bit-9.9.9P1-56.1

SuSE SLES 12 SP1

noarch
bind-doc-9.9.9P1-56.1

x86_64
bind-chrootenv-9.9.9P1-56.1
bind-debuginfo-9.9.9P1-56.1
bind-libs-debuginfo-9.9.9P1-56.1
bind-utils-debuginfo-9.9.9P1-56.1
bind-debugsource-9.9.9P1-56.1
bind-9.9.9P1-56.1
bind-utils-9.9.9P1-56.1
bind-libs-32bit-9.9.9P1-56.1
bind-libs-debuginfo-32bit-9.9.9P1-56.1
bind-libs-9.9.9P1-56.1

160218 - CentOS 7 CESA-2017-0386 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084

Description

The scan detected that the host is missing the following update:
CESA-2017-0386

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-March/022324.html>

CentOS 7
x86_64
perf-3.10.0-514.10.2.el7
kernel-debug-3.10.0-514.10.2.el7
kernel-3.10.0-514.10.2.el7
kernel-headers-3.10.0-514.10.2.el7
kernel-tools-3.10.0-514.10.2.el7
kernel-tools-libs-devel-3.10.0-514.10.2.el7
kernel-tools-libs-3.10.0-514.10.2.el7
kernel-debug-devel-3.10.0-514.10.2.el7
kernel-devel-3.10.0-514.10.2.el7
python-perf-3.10.0-514.10.2.el7

noarch
kernel-doc-3.10.0-514.10.2.el7
kernel-abi-whitelists-3.10.0-514.10.2.el7

160219 - CentOS 7 CESA-2017-0396 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-2615, CVE-2017-2620

Description

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

CESA-2017-0396

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-March/022321.html>

CentOS 7
x86_64
qemu-kvm-tools-1.5.3-126.el7_3.5
qemu-kvm-common-1.5.3-126.el7_3.5
qemu-img-1.5.3-126.el7_3.5
qemu-kvm-1.5.3-126.el7_3.5

160220 - CentOS 6 CESA-2017-0352 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2620

Description

The scan detected that the host is missing the following update:
CESA-2017-0352

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-March/022294.html>

CentOS 6
x86_64
qemu-kvm-0.12.1.2-2.491.el6_8.7
qemu-kvm-tools-0.12.1.2-2.491.el6_8.7
qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-img-0.12.1.2-2.491.el6_8.7

i686
qemu-guest-agent-0.12.1.2-2.491.el6_8.7

163292 - Oracle Enterprise Linux ELSA-2017-0454 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2615, CVE-2017-2620

Description

The scan detected that the host is missing the following update:
ELSA-2017-0454

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-March/006773.html>

OEL5

x86_64

kvm-83-277.0.1.el5_11

kmod-kvm-debug-83-277.0.1.el5_11

kvm-qemu-img-83-277.0.1.el5_11

kvm-tools-83-277.0.1.el5_11

kmod-kvm-83-277.0.1.el5_11

163293 - Oracle Enterprise Linux ELSA-2017-0386 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084

Description

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

ELSA-2017-0386

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006771.html>

<http://oss.oracle.com/pipermail/el-errata/2017-March/006747.html>

OEL7

x86_64

kernel-tools-3.10.0-514.10.2.el7

kernel-devel-3.10.0-514.10.2.0.1.el7

python-perf-3.10.0-514.10.2.0.1.el7

kernel-debug-3.10.0-514.10.2.el7

kernel-abi-whitelists-3.10.0-514.10.2.el7

kernel-tools-3.10.0-514.10.2.0.1.el7

kernel-debug-3.10.0-514.10.2.0.1.el7

kernel-debug-devel-3.10.0-514.10.2.0.1.el7

kernel-debug-devel-3.10.0-514.10.2.el7

perf-3.10.0-514.10.2.0.1.el7

kernel-headers-3.10.0-514.10.2.0.1.el7

kernel-devel-3.10.0-514.10.2.el7

kernel-doc-3.10.0-514.10.2.0.1.el7

kernel-headers-3.10.0-514.10.2.el7

python-perf-3.10.0-514.10.2.el7

kernel-3.10.0-514.10.2.0.1.el7

kernel-tools-libs-3.10.0-514.10.2.0.1.el7

kernel-abi-whitelists-3.10.0-514.10.2.0.1.el7

kernel-tools-libs-devel-3.10.0-514.10.2.0.1.el7

kernel-3.10.0-514.10.2.el7

kernel-tools-libs-3.10.0-514.10.2.el7

perf-3.10.0-514.10.2.el7

kernel-doc-3.10.0-514.10.2.el7

kernel-tools-libs-devel-3.10.0-514.10.2.el7

163294 - Oracle Enterprise Linux ELSA-2017-0396 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2615, CVE-2017-2620

Description

The scan detected that the host is missing the following update:
ELSA-2017-0396

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-March/006748.html>

OEL7

x86_64

qemu-kvm-tools-1.5.3-126.el7_3.5

qemu-kvm-common-1.5.3-126.el7_3.5

qemu-img-1.5.3-126.el7_3.5

qemu-kvm-1.5.3-126.el7_3.5

163295 - Oracle Enterprise Linux ELSA-2017-0352 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2620

Description

The scan detected that the host is missing the following update:
ELSA-2017-0352

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-March/006743.html>

OEL6

x86_64

qemu-kvm-0.12.1.2-2.491.el6_8.7

qemu-kvm-tools-0.12.1.2-2.491.el6_8.7

qemu-guest-agent-0.12.1.2-2.491.el6_8.7

qemu-img-0.12.1.2-2.491.el6_8.7

i386

qemu-guest-agent-0.12.1.2-2.491.el6_8.7

170778 - Amazon Linux AMI ALAS-2017-802 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8870, CVE-2016-5652, CVE-2016-9533, CVE-2016-9534, CVE-2016-9535, CVE-2016-9536, CVE-2016-9537, CVE-2016-9540

Description

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

ALAS-2017-802

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-802.html>

Amazon Linux AMI

x86_64

libtiff-devel-4.0.3-27.29.amzn1

libtiff-4.0.3-27.29.amzn1

libtiff-debuginfo-4.0.3-27.29.amzn1

compat-libtiff3-debuginfo-3.9.4-21.15.amzn1

libtiff-static-4.0.3-27.29.amzn1

compat-libtiff3-3.9.4-21.15.amzn1

i686

libtiff-devel-4.0.3-27.29.amzn1

libtiff-4.0.3-27.29.amzn1

libtiff-debuginfo-4.0.3-27.29.amzn1

compat-libtiff3-debuginfo-3.9.4-21.15.amzn1

libtiff-static-4.0.3-27.29.amzn1

compat-libtiff3-3.9.4-21.15.amzn1

170781 - Amazon Linux AMI ALAS-2017-805 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7097, CVE-2017-5551, CVE-2017-5897, CVE-2017-5986, CVE-2017-6074

Description

The scan detected that the host is missing the following update:
ALAS-2017-805

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-805.html>

Amazon Linux AMI

i686

kernel-debuginfo-4.4.51-40.58.amzn1

kernel-tools-4.4.51-40.58.amzn1

kernel-debuginfo-common-i686-4.4.51-40.58.amzn1

perf-4.4.51-40.58.amzn1

kernel-4.4.51-40.58.amzn1

perf-debuginfo-4.4.51-40.58.amzn1

kernel-tools-debuginfo-4.4.51-40.58.amzn1

kernel-headers-4.4.51-40.58.amzn1

kernel-tools-devel-4.4.51-40.58.amzn1

kernel-devel-4.4.51-40.58.amzn1

noarch

kernel-doc-4.4.51-40.58.amzn1

x86_64
kernel-tools-devel-4.4.51-40.58.amzn1
kernel-tools-4.4.51-40.58.amzn1
kernel-debuginfo-common-x86_64-4.4.51-40.58.amzn1
kernel-devel-4.4.51-40.58.amzn1
perf-4.4.51-40.58.amzn1
perf-debuginfo-4.4.51-40.58.amzn1
kernel-tools-debuginfo-4.4.51-40.58.amzn1
kernel-headers-4.4.51-40.58.amzn1
kernel-4.4.51-40.58.amzn1
kernel-debuginfo-4.4.51-40.58.amzn1

170782 - Amazon Linux AMI ALAS-2017-801 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7459

Description

The scan detected that the host is missing the following update:
ALAS-2017-801

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-801.html>

Amazon Linux AMI

x86_64
python-crypto-debuginfo-2.6.1-1.14.amzn1
python26-crypto-2.6.1-1.14.amzn1
python27-crypto-2.6.1-1.14.amzn1

i686
python-crypto-debuginfo-2.6.1-1.14.amzn1
python26-crypto-2.6.1-1.14.amzn1
python27-crypto-2.6.1-1.14.amzn1

175121 - Scientific Linux Security ERRATA Important: kvm on SL5.x x86_64 (1703-6365)

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

Risk Level: High

CVE: CVE-2017-2615, CVE-2017-2620

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kvm on SL5.x x86_64 (1703-6365)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=6365>

SL5

x86_64
kvm-debuginfo-83-277.el5_11
kmod-kvm-83-277.el5_11
kvm-tools-83-277.el5_11
kvm-qemu-img-83-277.el5_11
kvm-83-277.el5_11
kmod-kvm-debug-83-277.el5_11

175122 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1703-76)

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

Risk Level: High

CVE: CVE-2017-2620

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1703-76)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=76>

SL6
x86_64
qemu-kvm-0.12.1.2-2.491.el6_8.7
qemu-kvm-tools-0.12.1.2-2.491.el6_8.7
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.7
qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-img-0.12.1.2-2.491.el6_8.7

i386
qemu-guest-agent-0.12.1.2-2.491.el6_8.7
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.7

175123 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1703-761)

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

Risk Level: High

CVE: CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1703-761)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=761>

SL7
x86_64
kernel-debug-debuginfo-3.10.0-514.10.2.el7
perf-debuginfo-3.10.0-514.10.2.el7

kernel-debug-3.10.0-514.10.2.el7
kernel-tools-debuginfo-3.10.0-514.10.2.el7
kernel-debuginfo-3.10.0-514.10.2.el7
kernel-tools-3.10.0-514.10.2.el7
kernel-debug-devel-3.10.0-514.10.2.el7
kernel-devel-3.10.0-514.10.2.el7
kernel-headers-3.10.0-514.10.2.el7
python-perf-3.10.0-514.10.2.el7
kernel-debuginfo-common-x86_64-3.10.0-514.10.2.el7
python-perf-debuginfo-3.10.0-514.10.2.el7
kernel-3.10.0-514.10.2.el7
kernel-tools-libs-3.10.0-514.10.2.el7
perf-3.10.0-514.10.2.el7
kernel-tools-libs-devel-3.10.0-514.10.2.el7

noarch
kernel-doc-3.10.0-514.10.2.el7
kernel-abi-whitelists-3.10.0-514.10.2.el7

175124 - Scientific Linux Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1703-406)

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

Risk Level: High

CVE: CVE-2017-2615, CVE-2017-2620

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1703-406)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=406>

SL7
x86_64
qemu-kvm-tools-1.5.3-126.el7_3.5
qemu-kvm-common-1.5.3-126.el7_3.5
qemu-kvm-debuginfo-1.5.3-126.el7_3.5
qemu-img-1.5.3-126.el7_3.5
qemu-kvm-1.5.3-126.el7_3.5

185604 - Ubuntu Linux 16.04, 16.10 USN-3211-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-10162, CVE-2016-7479, CVE-2016-9137, CVE-2016-9935, CVE-2016-9936, CVE-2017-5340

Description

The scan detected that the host is missing the following update:
USN-3211-2

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003752.html>

Ubuntu 16.10

php7.0-fpm_7.0.15-0ubuntu0.16.10.4
libapache2-mod-php7.0_7.0.15-0ubuntu0.16.10.4
php7.0-cgi_7.0.15-0ubuntu0.16.10.4
php7.0-cli_7.0.15-0ubuntu0.16.10.4

Ubuntu 16.04

php7.0-fpm_7.0.15-0ubuntu0.16.04.4
php7.0-cli_7.0.15-0ubuntu0.16.04.4
libapache2-mod-php7.0_7.0.15-0ubuntu0.16.04.4
php7.0-cgi_7.0.15-0ubuntu0.16.04.4

191781 - Fedora Linux 24 FEDORA-2016-93679a91df Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9299

Description

The scan detected that the host is missing the following update:
FEDORA-2016-93679a91df

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/2017/3/?count=200&page=2>

Fedora Core 24

jenkins-remoting-2.62.3-1.fc24
jenkins-1.651.3-2.fc24

191784 - Fedora Linux 25 FEDORA-2017-8494d0142c Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6349, CVE-2017-6350

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8494d0142c

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/2017/3/?count=200&page=3>

Fedora Core 25

vim-8.0.386-1.fc25

191786 - Fedora Linux 25 FEDORA-2017-d875ae8299 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6347

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d875ae8299

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/2017/3/?count=200&page=2>

Fedora Core 25

kernel-4.9.13-200.fc25

191787 - Fedora Linux 25 FEDORA-2017-9a819664a6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6525, CVE-2016-8674, CVE-2017-5896, CVE-2017-6060

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9a819664a6

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/2017/3/?count=200&page=1>

Fedora Core 25

mupdf-1.10a-4.fc25

191788 - Fedora Linux 24 FEDORA-2017-ad67543fc5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6347

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ad67543fc5

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/2017/3/?count=200&page=3>

Fedora Core 24

kernel-4.9.13-100.fc24

191794 - Fedora Linux 24 FEDORA-2017-a9e6a5c249 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a9e6a5c249

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/2017/3/?count=200&page=2>

Fedora Core 24

gtk-vnc-0.7.0-1.fc24

191796 - Fedora Linux 24 FEDORA-2017-e9171a0c00 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6349, CVE-2017-6350

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e9171a0c00

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/2017/3/?count=200&page=2>

Fedora Core 24

vim-8.0.386-1.fc24

130711 - Debian Linux 8.0 DSA-3800-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2399

Description

The scan detected that the host is missing the following update:
DSA-3800-1

Observation

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

<http://www.debian.org/security/2017/dsa-3800>

Debian 8.0

all

libquicktime-dev_2:1.2.4-7+deb8u1

quicktime-x11utils_2:1.2.4-7+deb8u1

libquicktime-doc_2:1.2.4-7+deb8u1

libquicktime2_2:1.2.4-7+deb8u1

quicktime-utils_2:1.2.4-7+deb8u1

130712 - Debian Linux 8.0 DSA-3798-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
DSA-3798-1

Observation

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

<http://www.debian.org/security/2017/dsa-3798>

Debian 8.0

all

tnef_1.4.9-1+deb8u1

130714 - Debian Linux 8.0 DSA-3799-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10062, CVE-2016-10144, CVE-2016-10145, CVE-2016-10146, CVE-2016-8707, CVE-2017-5506, CVE-2017-5507, CVE-2017-5508, CVE-2017-5510, CVE-2017-5511

Description

The scan detected that the host is missing the following update:
DSA-3799-1

Observation

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

<http://www.debian.org/security/2017/dsa-3799>

Debian 8.0
all
imagemagick_8:6.8.9.9-5+deb8u7

145240 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0610-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2399

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0610-1

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-March/002681.html>

SuSE SLED 12 SP1

x86_64
libquicktime0-debuginfo-1.2.4-10.1
libquicktime0-1.2.4-10.1
libquicktime-debugsource-1.2.4-10.1

SuSE SLES 12 SP2

x86_64
libquicktime0-debuginfo-1.2.4-10.1
libquicktime0-1.2.4-10.1
libquicktime-debugsource-1.2.4-10.1

SuSE SLED 12 SP2

x86_64
libquicktime0-debuginfo-1.2.4-10.1
libquicktime0-1.2.4-10.1
libquicktime-debugsource-1.2.4-10.1

SuSE SLES 12 SP1

x86_64
libquicktime0-debuginfo-1.2.4-10.1
libquicktime0-1.2.4-10.1
libquicktime-debugsource-1.2.4-10.1

145246 - SuSE SLES 11 SP4 SUSE-SU-2017:0586-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10046, CVE-2016-10048, CVE-2016-10049, CVE-2016-10050, CVE-2016-10051, CVE-2016-10052, CVE-2016-10059, CVE-2016-10060, CVE-2016-10063, CVE-2016-10064, CVE-2016-10065, CVE-2016-10068, CVE-2016-10070, CVE-2016-10071, CVE-2016-10144, CVE-2016-10145, CVE-2016-10146, CVE-2017-5506, CVE-2017-5507, CVE-2017-5508, CVE-2017-5511

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0586-1

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-March/002671.html>

SuSE SLES 11 SP4

i586

libMagickCore1-6.4.3.6-7.65.1

x86_64

libMagickCore1-6.4.3.6-7.65.1

libMagickCore1-32bit-6.4.3.6-7.65.1

185602 - Ubuntu Linux 12.04, 14.04 USN-3214-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633

Description

The scan detected that the host is missing the following update:
USN-3214-1

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-March/003753.html>

Ubuntu 12.04

w3m_0.5.3-5ubuntu1.2

Ubuntu 14.04

w3m_0.5.3-15ubuntu0.1

21103 - (K11251130) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-1547

Description

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

Observation

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

A denial-of-service vulnerability is present in some versions of F5 BIG-IP systems. The flaw is due to improper handling of spoofed

crypto-NAK packets. Successful exploitation could allow an attacker to cause a denial of service condition.

21241 - (K55672042) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-4470

Description

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

Observation

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

A denial-of-service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Linux kernel. Successful exploitation could allow a malicious user to cause a denial of service condition.

21301 - (K23512141) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-2179

Description

A denial of service 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 denial of service vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the OpenSSL components. Successful exploitation could allow an attacker to cause a denial of service condition.

21305 - (CTX220771) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-2615, CVE-2017-2620

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in Quick emulator (QEMU). Successful exploitation could allow a privileged attacker to cause a denial-of-service or execute arbitrary code with privileges of the QEMU process.

21306 - IBM AIX Openssl Out Of Bounds Read Vulnerability (openssl_advisory23)

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

Risk Level: Medium

CVE: CVE-2017-3731

Description

A vulnerability is present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

A vulnerability is present in some versions of IBM AIX. The flaw is due to improper handling of specially crafted truncated packets. Successful exploitation could allow an attacker to cause a denial of service condition.

21324 - (K80533167) F5 BIG-IP BIND Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-3135

Description

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

Observation

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

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

141443 - Red Hat Enterprise Linux RHSA-2017-0388 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2590

Description

The scan detected that the host is missing the following update:
RHSA-2017-0388

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0388.html>

RHEL7D

x86_64

ipa-server-trust-ad-4.4.0-14.el7_3.6

ipa-server-4.4.0-14.el7_3.6

ipa-debuginfo-4.4.0-14.el7_3.6

ipa-client-4.4.0-14.el7_3.6

noarch

python2-ipaclient-4.4.0-14.el7_3.6

ipa-server-dns-4.4.0-14.el7_3.6

ipa-admintools-4.4.0-14.el7_3.6

ipa-client-common-4.4.0-14.el7_3.6

ipa-python-compat-4.4.0-14.el7_3.6

python2-ipalib-4.4.0-14.el7_3.6
ipa-server-common-4.4.0-14.el7_3.6
ipa-common-4.4.0-14.el7_3.6
python2-ipaserver-4.4.0-14.el7_3.6

RHEL7S

noarch
python2-ipaclient-4.4.0-14.el7_3.6
ipa-server-dns-4.4.0-14.el7_3.6
ipa-admintools-4.4.0-14.el7_3.6
ipa-client-common-4.4.0-14.el7_3.6
ipa-python-compat-4.4.0-14.el7_3.6
python2-ipalib-4.4.0-14.el7_3.6
ipa-server-common-4.4.0-14.el7_3.6
ipa-common-4.4.0-14.el7_3.6
python2-ipaserver-4.4.0-14.el7_3.6

x86_64

ipa-server-trust-ad-4.4.0-14.el7_3.6
ipa-server-4.4.0-14.el7_3.6
ipa-debuginfo-4.4.0-14.el7_3.6
ipa-client-4.4.0-14.el7_3.6

RHEL7WS

x86_64
ipa-server-trust-ad-4.4.0-14.el7_3.6
ipa-server-4.4.0-14.el7_3.6
ipa-debuginfo-4.4.0-14.el7_3.6
ipa-client-4.4.0-14.el7_3.6

noarch

python2-ipaclient-4.4.0-14.el7_3.6
ipa-server-dns-4.4.0-14.el7_3.6
ipa-admintools-4.4.0-14.el7_3.6
ipa-client-common-4.4.0-14.el7_3.6
ipa-python-compat-4.4.0-14.el7_3.6
python2-ipalib-4.4.0-14.el7_3.6
ipa-server-common-4.4.0-14.el7_3.6
ipa-common-4.4.0-14.el7_3.6
python2-ipaserver-4.4.0-14.el7_3.6

160221 - CentOS 7 CESA-2017-0388 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2590

Description

The scan detected that the host is missing the following update:
CESA-2017-0388

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-March/022310.html>

CentOS 7

x86_64
ipa-server-trust-ad-4.4.0-14.el7.centos.6
ipa-server-4.4.0-14.el7.centos.6
ipa-client-4.4.0-14.el7.centos.6

noarch
python2-ipalib-4.4.0-14.el7.centos.6
ipa-common-4.4.0-14.el7.centos.6
ipa-python-compat-4.4.0-14.el7.centos.6
python2-ipaclient-4.4.0-14.el7.centos.6
ipa-admintools-4.4.0-14.el7.centos.6
ipa-server-dns-4.4.0-14.el7.centos.6
ipa-client-common-4.4.0-14.el7.centos.6
ipa-server-common-4.4.0-14.el7.centos.6
python2-ipaserver-4.4.0-14.el7.centos.6

163291 - Oracle Enterprise Linux ELSA-2017-0388 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2590

Description

The scan detected that the host is missing the following update:
ELSA-2017-0388

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-March/006746.html>

OEL7
x86_64
python2-ipaserver-4.4.0-14.0.1.el7_3.6
ipa-server-4.4.0-14.0.1.el7_3.6
ipa-python-compat-4.4.0-14.0.1.el7_3.6
python2-ipalib-4.4.0-14.0.1.el7_3.6
python2-ipaclient-4.4.0-14.0.1.el7_3.6
ipa-client-common-4.4.0-14.0.1.el7_3.6
ipa-client-4.4.0-14.0.1.el7_3.6
ipa-server-common-4.4.0-14.0.1.el7_3.6
ipa-server-trust-ad-4.4.0-14.0.1.el7_3.6
ipa-common-4.4.0-14.0.1.el7_3.6
ipa-admintools-4.4.0-14.0.1.el7_3.6
ipa-server-dns-4.4.0-14.0.1.el7_3.6

170779 - Amazon Linux AMI ALAS-2017-803 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8610, CVE-2017-3731

Description

The scan detected that the host is missing the following update:
ALAS-2017-803

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-803.html>

Amazon Linux AMI

x86_64

openssl-1.0.1k-15.99.amzn1

openssl-static-1.0.1k-15.99.amzn1

openssl-perl-1.0.1k-15.99.amzn1

openssl-debuginfo-1.0.1k-15.99.amzn1

openssl-devel-1.0.1k-15.99.amzn1

i686

openssl-1.0.1k-15.99.amzn1

openssl-devel-1.0.1k-15.99.amzn1

openssl-perl-1.0.1k-15.99.amzn1

openssl-debuginfo-1.0.1k-15.99.amzn1

openssl-static-1.0.1k-15.99.amzn1

175125 - Scientific Linux Security ERRATA Moderate: ipa on SL7.x x86_64 (1703-1161)

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

Risk Level: Medium

CVE: CVE-2017-2590

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ipa on SL7.x x86_64 (1703-1161)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=1161>

SL7

x86_64

ipa-server-trust-ad-4.4.0-14.el7_3.6

ipa-server-4.4.0-14.el7_3.6

ipa-debuginfo-4.4.0-14.el7_3.6

ipa-client-4.4.0-14.el7_3.6

noarch

python2-ipaclient-4.4.0-14.el7_3.6

ipa-server-dns-4.4.0-14.el7_3.6

ipa-admintools-4.4.0-14.el7_3.6

ipa-client-common-4.4.0-14.el7_3.6

ipa-python-compat-4.4.0-14.el7_3.6

python2-ipalib-4.4.0-14.el7_3.6

ipa-server-common-4.4.0-14.el7_3.6

ipa-common-4.4.0-14.el7_3.6

python2-ipaserver-4.4.0-14.el7_3.6

182296 - FreeBSD ikiwiki Multiple Vulnerabilities (5ed094a0-0150-11e7-ae1b-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-10026, CVE-2016-9645, CVE-2016-9646

Description

The scan detected that the host is missing the following update:
ikiwiki -- multiple vulnerabilities (5ed094a0-0150-11e7-ae1b-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/5ed094a0-0150-11e7-ae1b-002590263bf5.html>

Affected packages:

ikiwiki < 3.20161229

191783 - Fedora Linux 24 FEDORA-2017-05e32fe278 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1430

Description

The scan detected that the host is missing the following update:
FEDORA-2017-05e32fe278

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/2017/3/?count=200&page=3>

Fedora Core 24

xrdp-0.9.1-5.fc24

191790 - Fedora Linux 25 FEDORA-2017-96b7f4f53e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864, CVE-2017-3135

Description

The scan detected that the host is missing the following update:
FEDORA-2017-96b7f4f53e

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/2017/3/?count=200&page=2>

Fedora Core 25

bind99-9.9.9-4.P6.fc25

191793 - Fedora Linux 24 FEDORA-2017-d0c9bf9508 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864, CVE-2017-3135

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d0c9bf9508

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/2017/3/?count=200&page=1>

Fedora Core 24

bind99-9.9.9-4.P6.fc24

21308 - (K90492697) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-6306

Description

A denial of service 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 denial of service vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the SSL profiles configured to request or require client certificates. Successful exploitation could allow an attacker to cause a denial of service condition.

141449 - Red Hat Enterprise Linux RHSA-2017-0003 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7796

Description

The scan detected that the host is missing the following update:
RHSA-2017-0003

Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0003.html>

RHEL7_1S
x86_64
systemd-sysv-208-20.el7_1.9
systemd-libs-208-20.el7_1.9
systemd-208-20.el7_1.9
systemd-devel-208-20.el7_1.9
systemd-journal-gateway-208-20.el7_1.9
systemd-debuginfo-208-20.el7_1.9
libgudev1-208-20.el7_1.9
libgudev1-devel-208-20.el7_1.9
systemd-python-208-20.el7_1.9

185605 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3216-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5412, CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5415, CVE-2017-5416, CVE-2017-5417, CVE-2017-5418, CVE-2017-5419, CVE-2017-5420, CVE-2017-5421, CVE-2017-5422, CVE-2017-5426, CVE-2017-5427

Description

The scan detected that the host is missing the following update:
USN-3216-1

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-March/003757.html>

Ubuntu 12.04

firefox_52.0+build2-0ubuntu0.12.04.1

Ubuntu 16.04

firefox_52.0+build2-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_52.0+build2-0ubuntu0.14.04.1

Ubuntu 16.10

firefox_52.0+build2-0ubuntu0.16.10.1

191791 - Fedora Linux 25 FEDORA-2017-f9ab92fa6c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6410

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f9ab92fa6c

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/2017/3/?count=200&page=2>

Fedora Core 25

kf5-kio-5.31.0-2.fc25

191799 - Fedora Linux 25 FEDORA-2017-53338ece0c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6410

Description

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

FEDORA-2017-53338ece0c

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/2017/3/?count=200&page=2>

Fedora Core 25

kdelibs-4.14.29-2.fc25

141442 - Red Hat Enterprise Linux RHSA-2017-0342 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

RHSA-2017-0342

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0342.html>

RHEL5_6S

i386

redhat-release-5Server-5.6.0.12

x86_64

redhat-release-5Server-5.6.0.12

141452 - Red Hat Enterprise Linux RHSA-2017-0341 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

RHSA-2017-0341

Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0341.html>

RHEL7_1S

x86_64

redhat-release-server-7.1-1.el7_1.5

182295 - FreeBSD codeigniter Multiple Vulnerabilities (71ebbc50-01c1-11e7-ae1b-002590263bf5)

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:

codeigniter -- multiple vulnerabilities (71ebbc50-01c1-11e7-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/71ebbc50-01c1-11e7-ae1b-002590263bf5.html>

Affected packages:

codeigniter < 3.1.3

182297 - FreeBSD ikiwiki Authentication Bypass Vulnerability (7b35a77a-0151-11e7-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2017-0356

Description

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

ikiwiki -- authentication bypass vulnerability (7b35a77a-0151-11e7-ae1b-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/7b35a77a-0151-11e7-ae1b-002590263bf5.html>

Affected packages:

182298 - FreeBSD mozilla Multiple Vulnerabilities (96eca031-1313-4daf-9be2-9d6e1c4f1eb5)

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

Risk Level: Low

CVE: CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5409, CVE-2017-5410, CVE-2017-5411, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5415, CVE-2017-5416, CVE-2017-5417, CVE-2017-5418, CVE-2017-5419, CVE-2017-5420, CVE-2017-5421, CVE-2017-5422, CVE-2017-5425, CVE-2017-5426, CVE-2017-5427

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (96eca031-1313-4daf-9be2-9d6e1c4f1eb5)

Observation

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

<http://www.vuxml.org/freebsd/96eca031-1313-4daf-9be2-9d6e1c4f1eb5.html>

Affected packages:

firefox < 52.0_1,1
seamonkey < 2.49
linux-seamonkey < 2.49
46.0,1 <= firefox-esr < 52.0,1
firefox-esr < 45.8.0_1,1
46.0,2 <= linux-firefox < 52.0,2
linux-firefox < 45.8.0_1,2
46.0 <= libxul < 52.0
libxul < 45.8.0_1
46.0 <= thunderbird < 52.0
46.0 <= linux-thunderbird < 52.0
thunderbird < 45.8.0
linux-thunderbird < 45.8.0

185606 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3217-1 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-3217-1

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-March/003756.html>

Ubuntu 12.04

network-manager-gnome_0.9.4.1-0ubuntu2.6

Ubuntu 16.04

network-manager-gnome_1.2.6-0ubuntu0.16.04.2

Ubuntu 14.04

network-manager-gnome_0.9.8.8-0ubuntu4.5

Ubuntu 16.10

network-manager-gnome_1.2.6-0ubuntu1.1

185607 - Ubuntu Linux 14.04 USN-3215-2 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-3215-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003755.html>

Ubuntu 14.04

munin_2.0.19-3ubuntu0.3

191779 - Fedora Linux 25 FEDORA-2017-8b0737b093 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-4000

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8b0737b093

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/2017/3/?count=200&page=1>

Fedora Core 25

cacti-1.0.4-1.fc25

191780 - Fedora Linux 25 FEDORA-2017-9a9328c159 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2625

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9a9328c159

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/2017/3/?count=200&page=2>

Fedora Core 25

libXdmcp-1.1.2-5.fc25

191782 - Fedora Linux 25 FEDORA-2017-b9ffa8b00f 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-b9ffa8b00f

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/2017/3/?count=200&page=1>

Fedora Core 25

canl-c-2.1.8-1.fc25

191785 - Fedora Linux 24 FEDORA-2017-fa4e441e03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2586, CVE-2017-2587, CVE-2017-5849

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fa4e441e03

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/2017/3/?count=200&page=3>

Fedora Core 24

netpbm-10.77.00-3.fc24

191789 - Fedora Linux 25 FEDORA-2017-c02eb668a7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2626

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c02eb668a7

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/2017/3/?count=200&page=2>

Fedora Core 25

libICE-1.0.9-8.fc25

191792 - Fedora Linux 25 FEDORA-2017-5a6ed9d326 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6414

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5a6ed9d326

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/2017/3/?count=200&page=2>

Fedora Core 25

libcacard-2.5.3-1.fc25

191795 - Fedora Linux 24 FEDORA-2017-d068b54614 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2626

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d068b54614

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/2017/3/?count=200&page=1>

Fedora Core 24

libICE-1.0.9-8.fc24

191797 - Fedora Linux 24 FEDORA-2017-bcb1999e65 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2625

Description

The scan detected that the host is missing the following update:
FEDORA-2017-bcb1999e65

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/2017/3/?count=200&page=1>

Fedora Core 24

libXdmcp-1.1.2-5.fc24

191798 - Fedora Linux 25 FEDORA-2017-d62c8f91e4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3156

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d62c8f91e4

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/2017/3/?count=200&page=3>

Fedora Core 25

cxfs-3.1.6-5.fc25

145244 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0625-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-10028, CVE-2016-10029, CVE-2016-10155, CVE-2016-9921, CVE-2016-9922, CVE-2017-2615, CVE-2017-2620, CVE-2017-5525, CVE-2017-5526, CVE-2017-5552, CVE-2017-5578, CVE-2017-5667, CVE-2017-5856, CVE-2017-5857, CVE-2017-

5898

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0625-1

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-March/002684.html>

SuSE SLED 12 SP2

x86_64

qemu-kvm-2.6.2-41.9.1
qemu-x86-2.6.2-41.9.1
qemu-debugsource-2.6.2-41.9.1
qemu-block-curl-debuginfo-2.6.2-41.9.1
qemu-tools-2.6.2-41.9.1
qemu-2.6.2-41.9.1
qemu-tools-debuginfo-2.6.2-41.9.1
qemu-block-curl-2.6.2-41.9.1

noarch

qemu-seabios-1.9.1-41.9.1
qemu-sgabios-8-41.9.1
qemu-vgabios-1.9.1-41.9.1
qemu-ipxe-1.0.0-41.9.1

SuSE SLES 12 SP2

noarch

qemu-seabios-1.9.1-41.9.1
qemu-sgabios-8-41.9.1
qemu-vgabios-1.9.1-41.9.1
qemu-ipxe-1.0.0-41.9.1

x86_64

qemu-tools-2.6.2-41.9.1
qemu-block-rbd-2.6.2-41.9.1
qemu-block-curl-debuginfo-2.6.2-41.9.1
qemu-guest-agent-debuginfo-2.6.2-41.9.1
qemu-block-ssh-2.6.2-41.9.1
qemu-block-ssh-debuginfo-2.6.2-41.9.1
qemu-kvm-2.6.2-41.9.1
qemu-tools-debuginfo-2.6.2-41.9.1
qemu-debugsource-2.6.2-41.9.1
qemu-block-rbd-debuginfo-2.6.2-41.9.1
qemu-2.6.2-41.9.1
qemu-block-curl-2.6.2-41.9.1
qemu-x86-2.6.2-41.9.1
qemu-guest-agent-2.6.2-41.9.1
qemu-lang-2.6.2-41.9.1

170780 - Amazon Linux AMI ALAS-2017-804 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9963

Description

The scan detected that the host is missing the following update:
ALAS-2017-804

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-804.html>

Amazon Linux AMI

x86_64
exim-debuginfo-4.88-2.11.amzn1
exim-4.88-2.11.amzn1
exim-pgsql-4.88-2.11.amzn1
exim-mon-4.88-2.11.amzn1
exim-mysql-4.88-2.11.amzn1
exim-greylis-4.88-2.11.amzn1

i686

exim-debuginfo-4.88-2.11.amzn1
exim-4.88-2.11.amzn1
exim-pgsql-4.88-2.11.amzn1
exim-mon-4.88-2.11.amzn1
exim-mysql-4.88-2.11.amzn1
exim-greylis-4.88-2.11.amzn1

185603 - Ubuntu Linux 14.04 USN-3215-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6188

Description

The scan detected that the host is missing the following update:
USN-3215-1

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-March/003754.html>

Ubuntu 14.04

munin_2.0.19-3ubuntu0.2

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.

141401 - Red Hat Enterprise Linux RHSA-2017-0086 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6828, CVE-2016-7117, CVE-2016-9555

[Update Details](#)

FASLScript is updated

141416 - Red Hat Enterprise Linux RHSA-2017-0215 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7117

[Update Details](#)

FASLScript is updated

141392 - Red Hat Enterprise Linux RHSA-2017-0002 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1669, CVE-2016-5180, CVE-2016-5325, CVE-2016-7099

[Update Details](#)

FASLScript is updated

141417 - Red Hat Enterprise Linux RHSA-2017-0190 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5373, CVE-2017-5375, CVE-2017-5376, CVE-2017-5378, CVE-2017-5380, CVE-2017-5383, CVE-2017-5386, CVE-2017-5390, CVE-2017-5396

[Update Details](#)

FASLScript is updated

141428 - Red Hat Enterprise Linux RHSA-2017-0294 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

[Update Details](#)

FASLScript is updated

160215 - CentOS 7 CESA-2017-0294 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

[Update Details](#)

FASLScript is updated

141418 - Red Hat Enterprise Linux RHSA-2017-0225 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8870, CVE-2016-5652, CVE-2016-9533, CVE-2016-9534, CVE-2016-9535, CVE-2016-9536, CVE-2016-9537, CVE-2016-9540

Update Details

FASLScript is updated

141419 - Red Hat Enterprise Linux RHSA-2017-0252 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311

Update Details

FASLScript is updated

141421 - Red Hat Enterprise Linux RHSA-2017-0238 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5373, CVE-2017-5375, CVE-2017-5376, CVE-2017-5378, CVE-2017-5380, CVE-2017-5383, CVE-2017-5390, CVE-2017-5396

Update Details

FASLScript is updated

182280 - FreeBSD chicken Multiple Vulnerabilities (c6932dd4-eaff-11e6-9ac1-a4badb2f4699)

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

Risk Level: High

CVE: CVE-2016-6830, CVE-2016-6831, CVE-2016-9954

Update Details

CVE is updated FASLScript is updated

33145 - Oracle Solaris 150401-48 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

Update Details

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

130678 - Debian Linux 8.0 DSA-3759-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10127, CVE-2016-10149

[Update Details](#)

Risk is updated

141399 - Red Hat Enterprise Linux RHSA-2017-0021 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9445, CVE-2016-9809, CVE-2016-9812, CVE-2016-9813

[Update Details](#)

FASLScript is updated

141400 - Red Hat Enterprise Linux RHSA-2017-0018 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9445, CVE-2016-9447, CVE-2016-9809

[Update Details](#)

FASLScript is updated

141423 - Red Hat Enterprise Linux RHSA-2017-0263 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3259, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

[Update Details](#)

FASLScript is updated

141424 - Red Hat Enterprise Linux RHSA-2017-0269 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

[Update Details](#)

FASLScript is updated

141431 - Red Hat Enterprise Linux RHSA-2017-0336 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3259, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

Update Details

FASLScript is updated

16834 - (K12636) F5 BIG-IP Slowloris Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2007-6750

Update Details

Name is updated Recommendation is updated

19550 - Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program (3123479)

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

141393 - Red Hat Enterprise Linux RHSA-2017-0001 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7030, CVE-2016-9575

Update Details

FASLScript is updated

141396 - Red Hat Enterprise Linux RHSA-2017-0020 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808

Update Details

FASLScript is updated

141398 - Red Hat Enterprise Linux RHSA-2017-0019 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808

Update Details

FASLScript is updated

141403 - Red Hat Enterprise Linux RHSA-2017-0062 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9131, CVE-2016-9147, CVE-2016-9444

Update Details

FASLScript is updated

141409 - Red Hat Enterprise Linux RHSA-2017-0180 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

Update Details

FASLScript is updated

141411 - Red Hat Enterprise Linux RHSA-2017-0182 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10002

Update Details

FASLScript is updated

141425 - Red Hat Enterprise Linux RHSA-2017-0276 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3135

Update Details

FASLScript is updated

141427 - Red Hat Enterprise Linux RHSA-2017-0286 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8610, CVE-2017-3731

Update Details

FASLScript is updated

33162 - Oracle Solaris 150400-48 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

[Update Details](#)

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

132322 - Oracle VM OVMSA-2017-0002 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

141394 - Red Hat Enterprise Linux RHSA-2017-0014 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

141397 - Red Hat Enterprise Linux RHSA-2017-0013 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7978, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated FASLScript is updated

144912 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2492-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5653, CVE-2016-7978, CVE-2016-7979

[Update Details](#)

Risk is updated

144951 - SuSE Linux 13.2 openSUSE-SU-2016:2648-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5653, CVE-2016-7978, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

145005 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2817-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2013-5653

[Update Details](#)

Risk is updated

160189 - CentOS 7 CESA-2017-0013 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7978, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

160192 - CentOS 6 CESA-2017-0014 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

163253 - Oracle Enterprise Linux ELSA-2017-0013 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7978, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

163255 - Oracle Enterprise Linux ELSA-2017-0014 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

170760 - Amazon Linux AMI ALAS-2017-784 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

175090 - Scientific Linux Security ERRATA Moderate: ghostscript on SL7.x x86_64 (1701-409)

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

Risk Level: Medium

CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7978, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

175093 - Scientific Linux Security ERRATA Moderate: ghostscript on SL6.x i386/x86_64 (1701-808)

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

Risk Level: Medium

CVE: CVE-2013-5653, CVE-2016-7977, CVE-2016-7979, CVE-2016-8602

[Update Details](#)

Risk is updated

141406 - Red Hat Enterprise Linux RHSA-2017-0083 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2857

[Update Details](#)

FASLScript is updated

70041 - rpm.fasl3.inc

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

Risk Level: Informational

CVE: CVE-2001-0923

[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.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2017 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates