

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

22658 - Oracle JDeveloper Critical Patch Update October 2017

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

Risk Level: High

CVE: CVE-2016-6814

Description

A vulnerability is present in some versions of Oracle JDeveloper.

Observation

Oracle JDeveloper is a popular development framework for Java applications.

A vulnerability is present in some versions of Oracle JDeveloper. The flaw lies in Java Business Objects. Successful exploitation could allow a remote attacker to affect confidentiality, integrity, and availability.

22649 - SpiderControl MicroBrowser DLL Hijacking Vulnerability

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

Risk Level: High

CVE: CVE-2017-14010

Description

A vulnerability is present in some versions of SpiderControl Scada MicroBrowser.

Observation

The SpiderControl MicroBrowser is a Viewer for HMI's designed with SpiderControl Editor.

A vulnerability is present in some versions of SpiderControl Scada MicroBrowser. The flaw is related to an uncontrolled search path element. Successful exploitation by a remote attacker could result in the execution of arbitrary code,

141770 - Red Hat Enterprise Linux RHSA-2017-3151 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15398, CVE-2017-15399

Description

The scan detected that the host is missing the following update:
RHSA-2017-3151

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00008.html>

RHEL6D

x86_64

chromium-browser-debuginfo-62.0.3202.89-1.el6_9

chromium-browser-62.0.3202.89-1.el6_9

i386

chromium-browser-debuginfo-62.0.3202.89-1.el6_9

chromium-browser-62.0.3202.89-1.el6_9

RHEL6S

x86_64

chromium-browser-debuginfo-62.0.3202.89-1.el6_9

chromium-browser-62.0.3202.89-1.el6_9

i386

chromium-browser-debuginfo-62.0.3202.89-1.el6_9

chromium-browser-62.0.3202.89-1.el6_9

RHEL6WS

x86_64

chromium-browser-debuginfo-62.0.3202.89-1.el6_9

chromium-browser-62.0.3202.89-1.el6_9

i386

chromium-browser-debuginfo-62.0.3202.89-1.el6_9

chromium-browser-62.0.3202.89-1.el6_9

22665 - Oracle GlassFish Server Critical Patch Update October 2017

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

Risk Level: High

CVE: CVE-2016-3092, CVE-2017-10385, CVE-2017-10391, CVE-2017-10393, CVE-2017-10400

Description

Multiple vulnerabilities are present in some versions of Oracle GlassFish.

Observation

Oracle GlassFish Server supports lightweight Java EE 6 Web Profile and the Java EE 6 platform.

Multiple vulnerabilities are present in some versions of Oracle GlassFish. The flaws lie in several components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or remotely execute arbitrary code on the target system.

22666 - Oracle WebLogic Server Critical Patch Update October 2017

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

Risk Level: High

CVE: CVE-2017-10152, CVE-2017-10271, CVE-2017-10334, CVE-2017-10336, CVE-2017-10352

Description

Multiple vulnerabilities are present in some versions of Oracle WebLogic Server.

Observation

Oracle WebLogic Server is a Java EE application server.

Multiple vulnerabilities are present in some versions of Oracle WebLogic Server. The flaws lie in several components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or remotely execute arbitrary code on the target system.

22640 - Oracle Database Server Critical Patch Update October 2017

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

Risk Level: High

CVE: CVE-2016-6814, CVE-2016-8735, CVE-2017-10190, CVE-2017-10261, CVE-2017-10292, CVE-2017-10321

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, retrieve sensitive data or locally bypass security measures.

22641 - Oracle Database Server Critical Patch Update October 2017

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-6814, CVE-2016-8735, CVE-2017-10190, CVE-2017-10261, CVE-2017-10292, CVE-2017-10321

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, retrieve sensitive data or locally bypass security measures.

22657 - (CTX229057) Citrix XenServer Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-15597

Description

A vulnerability is present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

A vulnerability is present in some versions of Citrix XenServer. The flaw is due to pin count / page reference race in grant table code. Successful exploitation could allow a malicious administrator of a guest VM to compromise the host.

22670 - Trihedral VTScada Multiple Vulnerabilities Prior To 11.3.05

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

Risk Level: High

CVE: CVE-2017-14029, CVE-2017-14031

Description

Multiple vulnerabilities are present in some versions of Trihedral VTScada.

Observation

Trihedral VTScada is an industrial control and monitoring software.

Multiple vulnerabilities are present in some versions of Trihedral VTScada. The flaws lie in multiple components. Successful exploitation could allow an attacker to remotely execute arbitrary code.

130923 - Debian Linux 9.0 DSA-4019-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11446, CVE-2017-11523, CVE-2017-11533, CVE-2017-11535, CVE-2017-11537, CVE-2017-11639, CVE-2017-11640, CVE-2017-12428, CVE-2017-12431, CVE-2017-12432, CVE-2017-12434, CVE-2017-12587, CVE-2017-12640, CVE-2017-12671, CVE-2017-13139, CVE-2017-13140, CVE-2017-13141, CVE-2017-13142, CVE-2017-13143, CVE-2017-13144, CVE-2017-13145, CVE-2017-9500

Description

The scan detected that the host is missing the following update:
DSA-4019-1

Observation

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

<http://www.debian.org/security/2017/dsa-4019>

Debian 9.0
all
imagemagick_8:6.9.7.4+dfsg-11+deb9u2

130928 - Debian Linux 8.0, 9.0 DSA-4016-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10965, CVE-2017-10966, CVE-2017-15227, CVE-2017-15228, CVE-2017-15721, CVE-2017-15722, CVE-2017-15723

Description

The scan detected that the host is missing the following update:
DSA-4016-1

Observation

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

<http://www.debian.org/security/2017/dsa-4016>

Debian 8.0
all
irssi_0.8.17-1+deb8u5

Debian 9.0
all
irssi_1.0.2-1+deb9u3

132413 - Oracle VM OVMSA-2017-0168 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10044, CVE-2017-1000363, CVE-2017-1000380, CVE-2017-10661, CVE-2017-11473, CVE-2017-14489, CVE-2017-2671, CVE-2017-8831, CVE-2017-9075, CVE-2017-9077

Description

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

OVMSA-2017-0168

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-November/000799.html>

OVM3.3
x86_64
kernel-uek-3.8.13-118.19.12.el6uek
kernel-uek-firmware-3.8.13-118.19.12.el6uek

132414 - Oracle VM OVMSA-2017-0167 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000112, CVE-2017-10661, CVE-2017-12154, CVE-2017-14106, CVE-2017-14489, CVE-2017-7482, CVE-2017-7541, CVE-2017-7542, CVE-2017-7618

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0167

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-November/000798.html>

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-103.9.2.el6uek
kernel-uek-4.1.12-103.9.2.el6uek

146042 - SuSE SLES 11 SP4 SUSE-SU-2017:2923-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15638

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2923-1

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-November/003370.html>

SuSE SLES 11 SP4
noarch
SuSEfirewall2-3.6_SVNr208-2.18.3.1

146043 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2924-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10911, CVE-2017-12809, CVE-2017-13672, CVE-2017-13711, CVE-2017-14167, CVE-2017-15038, CVE-2017-15268, CVE-2017-15289

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2924-1

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-November/003371.html>

SuSE SLED 12 SP3

x86_64

qemu-debugsource-2.9.1-6.6.3

qemu-2.9.1-6.6.3

qemu-tools-2.9.1-6.6.3

qemu-block-curl-2.9.1-6.6.3

qemu-kvm-2.9.1-6.6.3

qemu-tools-debuginfo-2.9.1-6.6.3

qemu-block-curl-debuginfo-2.9.1-6.6.3

qemu-x86-2.9.1-6.6.3

noarch

qemu-sgabios-8-6.6.3

qemu-seabios-1.10.2-6.6.3

qemu-vgabios-1.10.2-6.6.3

qemu-ipxe-1.0.0-6.6.3

SuSE SLES 12 SP3

noarch

qemu-sgabios-8-6.6.3

qemu-seabios-1.10.2-6.6.3

qemu-vgabios-1.10.2-6.6.3

qemu-ipxe-1.0.0-6.6.3

x86_64

qemu-block-curl-debuginfo-2.9.1-6.6.3

qemu-guest-agent-debuginfo-2.9.1-6.6.3

qemu-block-iscsi-2.9.1-6.6.3

qemu-tools-debuginfo-2.9.1-6.6.3

qemu-kvm-2.9.1-6.6.3

qemu-x86-2.9.1-6.6.3

qemu-block-ssh-2.9.1-6.6.3

qemu-block-rbd-debuginfo-2.9.1-6.6.3

qemu-tools-2.9.1-6.6.3

qemu-2.9.1-6.6.3

qemu-block-iscsi-debuginfo-2.9.1-6.6.3

qemu-guest-agent-2.9.1-6.6.3

qemu-block-curl-2.9.1-6.6.3

qemu-debugsource-2.9.1-6.6.3

qemu-lang-2.9.1-6.6.3

qemu-block-rbd-2.9.1-6.6.3

qemu-block-ssh-debuginfo-2.9.1-6.6.3

146044 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2932-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15638

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2932-1

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-November/003373.html>

SuSE SLED 12 SP2
noarch
SuSEfirewall2-3.6.312-2.13.1

SuSE SLES 12 SP2
noarch
SuSEfirewall2-3.6.312-2.13.1

146045 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2933-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7586, CVE-2016-7589, CVE-2016-7592, CVE-2016-7599, CVE-2016-7623, CVE-2016-7632, CVE-2016-7635, CVE-2016-7639, CVE-2016-7641, CVE-2016-7645, CVE-2016-7652, CVE-2016-7654, CVE-2016-7656, CVE-2017-2350, CVE-2017-2354, CVE-2017-2355, CVE-2017-2356, CVE-2017-2362, CVE-2017-2363, CVE-2017-2364, CVE-2017-2365, CVE-2017-2366, CVE-2017-2369, CVE-2017-2371, CVE-2017-2373, CVE-2017-2496, CVE-2017-2510, CVE-2017-2538, CVE-2017-2539, CVE-2017-7018, CVE-2017-7030, CVE-2017-7034, CVE-2017-7037, CVE-2017-7039, CVE-2017-7046, CVE-2017-7048, CVE-2017-7055, CVE-2017-7056, CVE-2017-7061, CVE-2017-7064

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2933-1

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-November/003374.html>

SuSE SLED 12 SP2
x86_64
typelib-1_0-WebKit2-4_0-2.18.0-2.9.1
libjavascriptcoregtk-4_0-18-2.18.0-2.9.1
libwebkit2gtk-4_0-37-2.18.0-2.9.1
typelib-1_0-JavaScriptCore-4_0-2.18.0-2.9.1
webkit2gtk-4_0-injected-bundles-2.18.0-2.9.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.0-2.9.1
libwebkit2gtk-4_0-37-debuginfo-2.18.0-2.9.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.0-2.9.1
webkit2gtk3-debugsource-2.18.0-2.9.1

noarch
libwebkit2gtk3-lang-2.18.0-2.9.1

SuSE SLES 12 SP3
x86_64
typelib-1_0-WebKit2-4_0-2.18.0-2.9.1
libjavascriptcoregtk-4_0-18-2.18.0-2.9.1
libwebkit2gtk-4_0-37-2.18.0-2.9.1
typelib-1_0-JavaScriptCore-4_0-2.18.0-2.9.1
webkit2gtk-4_0-injected-bundles-2.18.0-2.9.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.0-2.9.1
libwebkit2gtk-4_0-37-debuginfo-2.18.0-2.9.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.0-2.9.1
webkit2gtk3-debugsource-2.18.0-2.9.1

SuSE SLES 12 SP2
x86_64

typelib-1_0-WebKit2-4_0-2.18.0-2.9.1
libjavascriptcoregtk-4_0-18-2.18.0-2.9.1
libwebkit2gtk-4_0-37-2.18.0-2.9.1
typelib-1_0-JavaScriptCore-4_0-2.18.0-2.9.1
webkit2gtk-4_0-injected-bundles-2.18.0-2.9.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.0-2.9.1
libwebkit2gtk-4_0-37-debuginfo-2.18.0-2.9.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.0-2.9.1
webkit2gtk3-debugsource-2.18.0-2.9.1

SuSE SLED 12 SP3

x86_64

typelib-1_0-WebKit2-4_0-2.18.0-2.9.1
libjavascriptcoregtk-4_0-18-2.18.0-2.9.1
libwebkit2gtk-4_0-37-2.18.0-2.9.1
typelib-1_0-JavaScriptCore-4_0-2.18.0-2.9.1
webkit2gtk-4_0-injected-bundles-2.18.0-2.9.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.18.0-2.9.1
libwebkit2gtk-4_0-37-debuginfo-2.18.0-2.9.1
libjavascriptcoregtk-4_0-18-debuginfo-2.18.0-2.9.1
webkit2gtk3-debugsource-2.18.0-2.9.1

noarch

libwebkit2gtk3-lang-2.18.0-2.9.1

146046 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2936-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10664, CVE-2017-10806, CVE-2017-10911, CVE-2017-11334, CVE-2017-11434, CVE-2017-12809, CVE-2017-13672, CVE-2017-14167, CVE-2017-15038, CVE-2017-15268, CVE-2017-15289, CVE-2017-9524

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2936-1

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-November/003376.html>

SuSE SLED 12 SP2

x86_64

qemu-kvm-2.6.2-41.22.2
qemu-2.6.2-41.22.2
qemu-tools-2.6.2-41.22.2
qemu-debugsource-2.6.2-41.22.2
qemu-tools-debuginfo-2.6.2-41.22.2
qemu-block-curl-2.6.2-41.22.2
qemu-x86-2.6.2-41.22.2
qemu-block-curl-debuginfo-2.6.2-41.22.2

noarch

qemu-pxe-1.0.0-41.22.2
qemu-vgabios-1.9.1-41.22.2
qemu-sgabios-8-41.22.2
qemu-seabios-1.9.1-41.22.2

SuSE SLES 12 SP2

noarch

qemu-pxe-1.0.0-41.22.2
qemu-vgabios-1.9.1-41.22.2
qemu-sgabios-8-41.22.2
qemu-seabios-1.9.1-41.22.2

x86_64
qemu-block-curl-2.6.2-41.22.2
qemu-block-rbd-2.6.2-41.22.2
qemu-tools-2.6.2-41.22.2
qemu-x86-2.6.2-41.22.2
qemu-block-ssh-debuginfo-2.6.2-41.22.2
qemu-block-ssh-2.6.2-41.22.2
qemu-kvm-2.6.2-41.22.2
qemu-block-curl-debuginfo-2.6.2-41.22.2
qemu-block-rbd-debuginfo-2.6.2-41.22.2
qemu-2.6.2-41.22.2
qemu-debugsource-2.6.2-41.22.2
qemu-tools-debuginfo-2.6.2-41.22.2
qemu-lang-2.6.2-41.22.2
qemu-guest-agent-debuginfo-2.6.2-41.22.2
qemu-guest-agent-2.6.2-41.22.2

146048 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2937-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2937-1

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-November/003377.html>

SuSE SLES 12 SP2

x86_64
sssd-ipa-1.13.4-34.7.1
sssd-krb5-debuginfo-1.13.4-34.7.1
sssd-32bit-1.13.4-34.7.1
python-sssd-config-debuginfo-1.13.4-34.7.1
sssd-ipa-debuginfo-1.13.4-34.7.1
sssd-tools-1.13.4-34.7.1
libsss_idmap0-1.13.4-34.7.1
libsss_idmap0-debuginfo-1.13.4-34.7.1
libipa_hbac0-1.13.4-34.7.1
sssd-ad-1.13.4-34.7.1
sssd-tools-debuginfo-1.13.4-34.7.1
libipa_hbac0-debuginfo-1.13.4-34.7.1
sssd-proxy-1.13.4-34.7.1
sssd-proxy-debuginfo-1.13.4-34.7.1
sssd-ad-debuginfo-1.13.4-34.7.1
sssd-krb5-common-1.13.4-34.7.1
sssd-krb5-common-debuginfo-1.13.4-34.7.1
libsss_sudo-1.13.4-34.7.1
sssd-debuginfo-1.13.4-34.7.1
sssd-ldap-debuginfo-1.13.4-34.7.1
sssd-ldap-1.13.4-34.7.1
sssd-krb5-1.13.4-34.7.1
sssd-debuginfo-32bit-1.13.4-34.7.1
python-sssd-config-1.13.4-34.7.1
sssd-1.13.4-34.7.1
libsss_sudo-debuginfo-1.13.4-34.7.1
sssd-debugsource-1.13.4-34.7.1

SuSE SLED 12 SP3

x86_64

sssd-ipa-1.13.4-34.7.1
sssd-krb5-debuginfo-1.13.4-34.7.1
libipa_hbac0-debuginfo-1.13.4-34.7.1
python-sssd-config-debuginfo-1.13.4-34.7.1
sssd-ipa-debuginfo-1.13.4-34.7.1
sssd-tools-1.13.4-34.7.1
libsss_idmap0-1.13.4-34.7.1
libsss_nss_idmap0-debuginfo-1.13.4-34.7.1
libsss_idmap0-debuginfo-1.13.4-34.7.1
libipa_hbac0-1.13.4-34.7.1
libsss_nss_idmap0-1.13.4-34.7.1
sssd-ad-1.13.4-34.7.1
sssd-tools-debuginfo-1.13.4-34.7.1
sssd-32bit-1.13.4-34.7.1
sssd-proxy-1.13.4-34.7.1
sssd-proxy-debuginfo-1.13.4-34.7.1
sssd-ad-debuginfo-1.13.4-34.7.1
sssd-krb5-common-1.13.4-34.7.1
sssd-krb5-common-debuginfo-1.13.4-34.7.1
libsss_sudo-1.13.4-34.7.1
sssd-debuginfo-1.13.4-34.7.1
sssd-ldap-debuginfo-1.13.4-34.7.1
sssd-ldap-1.13.4-34.7.1
sssd-krb5-1.13.4-34.7.1
sssd-debuginfo-32bit-1.13.4-34.7.1
python-sssd-config-1.13.4-34.7.1
sssd-1.13.4-34.7.1
libsss_sudo-debuginfo-1.13.4-34.7.1
sssd-debugsource-1.13.4-34.7.1

SuSE SLED 12 SP2

x86_64

sssd-ipa-1.13.4-34.7.1
sssd-krb5-debuginfo-1.13.4-34.7.1
sssd-32bit-1.13.4-34.7.1
python-sssd-config-debuginfo-1.13.4-34.7.1
sssd-ipa-debuginfo-1.13.4-34.7.1
sssd-tools-1.13.4-34.7.1
libsss_idmap0-1.13.4-34.7.1
libsss_idmap0-debuginfo-1.13.4-34.7.1
libipa_hbac0-1.13.4-34.7.1
sssd-ad-1.13.4-34.7.1
sssd-tools-debuginfo-1.13.4-34.7.1
libipa_hbac0-debuginfo-1.13.4-34.7.1
sssd-proxy-1.13.4-34.7.1
sssd-proxy-debuginfo-1.13.4-34.7.1
sssd-ad-debuginfo-1.13.4-34.7.1
sssd-krb5-common-1.13.4-34.7.1
sssd-krb5-common-debuginfo-1.13.4-34.7.1
libsss_sudo-1.13.4-34.7.1
sssd-debuginfo-1.13.4-34.7.1
sssd-ldap-debuginfo-1.13.4-34.7.1
sssd-ldap-1.13.4-34.7.1
sssd-krb5-1.13.4-34.7.1
sssd-debuginfo-32bit-1.13.4-34.7.1
python-sssd-config-1.13.4-34.7.1
sssd-1.13.4-34.7.1
libsss_sudo-debuginfo-1.13.4-34.7.1
sssd-debugsource-1.13.4-34.7.1

SuSE SLES 12 SP3

x86_64

sssd-ipa-1.13.4-34.7.1
sssd-krb5-debuginfo-1.13.4-34.7.1
sssd-32bit-1.13.4-34.7.1
python-sssd-config-debuginfo-1.13.4-34.7.1
sssd-ipa-debuginfo-1.13.4-34.7.1

sssd-tools-1.13.4-34.7.1
libsss_idmap0-1.13.4-34.7.1
libsss_nss_idmap0-debuginfo-1.13.4-34.7.1
libsss_idmap0-debuginfo-1.13.4-34.7.1
libipa_hbac0-1.13.4-34.7.1
libsss_nss_idmap0-1.13.4-34.7.1
sssd-ad-1.13.4-34.7.1
sssd-tools-debuginfo-1.13.4-34.7.1
libipa_hbac0-debuginfo-1.13.4-34.7.1
sssd-proxy-1.13.4-34.7.1
sssd-proxy-debuginfo-1.13.4-34.7.1
sssd-ad-debuginfo-1.13.4-34.7.1
sssd-krb5-common-1.13.4-34.7.1
sssd-krb5-common-debuginfo-1.13.4-34.7.1
libsss_sudo-1.13.4-34.7.1
sssd-debuginfo-1.13.4-34.7.1
sssd-ldap-debuginfo-1.13.4-34.7.1
sssd-ldap-1.13.4-34.7.1
sssd-krb5-1.13.4-34.7.1
sssd-debuginfo-32bit-1.13.4-34.7.1
python-sssd-config-1.13.4-34.7.1
sssd-1.13.4-34.7.1
libsss_sudo-debuginfo-1.13.4-34.7.1
sssd-debugsource-1.13.4-34.7.1

146049 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2935-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15638

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2935-1

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-November/003375.html>

SuSE SLED 12 SP3
noarch
SuSEfirewall2-3.6.312.333-3.10.1

SuSE SLES 12 SP3
noarch
SuSEfirewall2-3.6.312.333-3.10.1

146050 - SuSE Linux 42.2 openSUSE-SU-2017:2941-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10664, CVE-2017-10806, CVE-2017-10911, CVE-2017-11334, CVE-2017-11434, CVE-2017-12809,
CVE-2017-13672, CVE-2017-14167, CVE-2017-15038, CVE-2017-15268, CVE-2017-15289, CVE-2017-9524

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2941-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00015.html>

SuSE Linux 42.2

i586

qemu-arm-2.6.2-31.9.1
qemu-tools-2.6.2-31.9.1
qemu-tools-debuginfo-2.6.2-31.9.1
qemu-block-dmg-2.6.2-31.9.1
qemu-kvm-2.6.2-31.9.1
qemu-lang-2.6.2-31.9.1
qemu-block-ssh-debuginfo-2.6.2-31.9.1
qemu-block-iscsi-debuginfo-2.6.2-31.9.1
qemu-extra-2.6.2-31.9.1
qemu-block-dmg-debuginfo-2.6.2-31.9.1
qemu-arm-debuginfo-2.6.2-31.9.1
qemu-x86-debuginfo-2.6.2-31.9.1
qemu-x86-2.6.2-31.9.1
qemu-extra-debuginfo-2.6.2-31.9.1
qemu-linux-user-2.6.2-31.9.1
qemu-block-iscsi-2.6.2-31.9.1
qemu-block-curl-2.6.2-31.9.1
qemu-guest-agent-2.6.2-31.9.1
qemu-ppc-debuginfo-2.6.2-31.9.1
qemu-s390-debuginfo-2.6.2-31.9.1
qemu-2.6.2-31.9.1
qemu-guest-agent-debuginfo-2.6.2-31.9.1
qemu-ppc-2.6.2-31.9.1
qemu-linux-user-debuginfo-2.6.2-31.9.1
qemu-block-curl-debuginfo-2.6.2-31.9.1
qemu-block-ssh-2.6.2-31.9.1
qemu-s390-2.6.2-31.9.1
qemu-testsuite-2.6.2-31.9.2
qemu-linux-user-debugsource-2.6.2-31.9.1
qemu-debugsource-2.6.2-31.9.1

noarch

qemu-sgabios-8-31.9.1
qemu-ipxe-1.0.0-31.9.1
qemu-seabios-1.9.1-31.9.1
qemu-vgabios-1.9.1-31.9.1

x86_64

qemu-arm-2.6.2-31.9.1
qemu-tools-2.6.2-31.9.1
qemu-tools-debuginfo-2.6.2-31.9.1
qemu-block-dmg-2.6.2-31.9.1
qemu-kvm-2.6.2-31.9.1
qemu-lang-2.6.2-31.9.1
qemu-block-ssh-debuginfo-2.6.2-31.9.1
qemu-block-iscsi-debuginfo-2.6.2-31.9.1
qemu-extra-2.6.2-31.9.1
qemu-block-dmg-debuginfo-2.6.2-31.9.1
qemu-arm-debuginfo-2.6.2-31.9.1
qemu-x86-debuginfo-2.6.2-31.9.1
qemu-x86-2.6.2-31.9.1
qemu-extra-debuginfo-2.6.2-31.9.1
qemu-linux-user-2.6.2-31.9.1
qemu-block-iscsi-2.6.2-31.9.1
qemu-block-curl-2.6.2-31.9.1
qemu-block-rbd-debuginfo-2.6.2-31.9.1
qemu-guest-agent-2.6.2-31.9.1
qemu-ppc-debuginfo-2.6.2-31.9.1
qemu-s390-debuginfo-2.6.2-31.9.1
qemu-2.6.2-31.9.1
qemu-guest-agent-debuginfo-2.6.2-31.9.1
qemu-ppc-2.6.2-31.9.1

qemu-linux-user-debuginfo-2.6.2-31.9.1
qemu-block-curl-debuginfo-2.6.2-31.9.1
qemu-block-ssh-2.6.2-31.9.1
qemu-s390-2.6.2-31.9.1
qemu-testsuite-2.6.2-31.9.2
qemu-linux-user-debugsource-2.6.2-31.9.1
qemu-debugsource-2.6.2-31.9.1
qemu-block-rbd-2.6.2-31.9.1

146051 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2940-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15638

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2940-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00014.html>

SuSE Linux 42.2
noarch
SuSEfirewall2-3.6.312-5.9.1

SuSE Linux 42.3
noarch
SuSEfirewall2-3.6.312.333-7.1

146053 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2942-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2942-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00016.html>

SuSE Linux 42.2
x86_64
python-ipa_hbac-debuginfo-1.13.4-5.6.1
sssd-ipa-1.13.4-5.6.1
sssd-debuginfo-1.13.4-5.6.1
libipa_hbac-devel-1.13.4-5.6.1
sssd-debugsource-1.13.4-5.6.1
sssd-ipa-debuginfo-1.13.4-5.6.1
sssd-krb5-debuginfo-1.13.4-5.6.1
python-ipa_hbac-1.13.4-5.6.1
python-sss_nss_idmap-debuginfo-1.13.4-5.6.1
sssd-krb5-common-debuginfo-1.13.4-5.6.1
sssd-proxy-1.13.4-5.6.1

libsss_nss_idmap-devel-1.13.4-5.6.1
libipa_hbac0-1.13.4-5.6.1
sssd-krb5-1.13.4-5.6.1
libsss_sudo-debuginfo-1.13.4-5.6.1
libsss_nss_idmap0-debuginfo-1.13.4-5.6.1
libsss_sudo-1.13.4-5.6.1
python-sssd-config-debuginfo-1.13.4-5.6.1
sssd-ad-debuginfo-1.13.4-5.6.1
sssd-ldap-1.13.4-5.6.1
libipa_hbac0-debuginfo-1.13.4-5.6.1
sssd-krb5-common-1.13.4-5.6.1
libsss_idmap0-1.13.4-5.6.1
sssd-32bit-1.13.4-5.6.1
sssd-tools-debuginfo-1.13.4-5.6.1
sssd-1.13.4-5.6.1
sssd-ldap-debuginfo-1.13.4-5.6.1
libsss_idmap-devel-1.13.4-5.6.1
python-sssd-config-1.13.4-5.6.1
sssd-proxy-debuginfo-1.13.4-5.6.1
sssd-debuginfo-32bit-1.13.4-5.6.1
sssd-ad-1.13.4-5.6.1
libsss_idmap0-debuginfo-1.13.4-5.6.1
libsss_nss_idmap0-1.13.4-5.6.1
python-sss_nss_idmap-1.13.4-5.6.1
sssd-tools-1.13.4-5.6.1

i586

python-ipa_hbac-debuginfo-1.13.4-5.6.1
sssd-ipa-1.13.4-5.6.1
sssd-debuginfo-1.13.4-5.6.1
libipa_hbac-devel-1.13.4-5.6.1
sssd-debugsource-1.13.4-5.6.1
sssd-ipa-debuginfo-1.13.4-5.6.1
sssd-krb5-debuginfo-1.13.4-5.6.1
python-ipa_hbac-1.13.4-5.6.1
python-sss_nss_idmap-debuginfo-1.13.4-5.6.1
sssd-krb5-common-debuginfo-1.13.4-5.6.1
sssd-proxy-1.13.4-5.6.1
libsss_nss_idmap-devel-1.13.4-5.6.1
libipa_hbac0-1.13.4-5.6.1
sssd-krb5-1.13.4-5.6.1
libsss_sudo-debuginfo-1.13.4-5.6.1
libsss_nss_idmap0-debuginfo-1.13.4-5.6.1
libsss_sudo-1.13.4-5.6.1
python-sssd-config-debuginfo-1.13.4-5.6.1
sssd-ad-debuginfo-1.13.4-5.6.1
sssd-ldap-1.13.4-5.6.1
libipa_hbac0-debuginfo-1.13.4-5.6.1
sssd-krb5-common-1.13.4-5.6.1
libsss_idmap0-1.13.4-5.6.1
sssd-tools-debuginfo-1.13.4-5.6.1
sssd-1.13.4-5.6.1
sssd-ldap-debuginfo-1.13.4-5.6.1
libsss_idmap-devel-1.13.4-5.6.1
python-sssd-config-1.13.4-5.6.1
sssd-proxy-debuginfo-1.13.4-5.6.1
sssd-ad-1.13.4-5.6.1
libsss_idmap0-debuginfo-1.13.4-5.6.1
libsss_nss_idmap0-1.13.4-5.6.1
python-sss_nss_idmap-1.13.4-5.6.1
sssd-tools-1.13.4-5.6.1

SuSE Linux 42.3

x86_64

sssd-proxy-1.13.4-9.1
sssd-ldap-debuginfo-1.13.4-9.1
sssd-ipa-1.13.4-9.1
sssd-ldap-1.13.4-9.1

python-ipa_hbac-debuginfo-1.13.4-9.1
python-sssd-config-debuginfo-1.13.4-9.1
sssd-debuginfo-1.13.4-9.1
python-sss_nss_idmap-debuginfo-1.13.4-9.1
libsss_nss_idmap-devel-1.13.4-9.1
libsss_sudo-debuginfo-1.13.4-9.1
sssd-ipa-debuginfo-1.13.4-9.1
sssd-debugsource-1.13.4-9.1
sssd-krb5-debuginfo-1.13.4-9.1
sssd-ad-1.13.4-9.1
libsss_nss_idmap0-1.13.4-9.1
libsss_idmap0-1.13.4-9.1
libsss_idmap-devel-1.13.4-9.1
sssd-ad-debuginfo-1.13.4-9.1
python-sssd-config-1.13.4-9.1
sssd-tools-debuginfo-1.13.4-9.1
python-sss_nss_idmap-1.13.4-9.1
sssd-krb5-1.13.4-9.1
python-ipa_hbac-1.13.4-9.1
sssd-tools-1.13.4-9.1
libsss_sudo-1.13.4-9.1
sssd-proxy-debuginfo-1.13.4-9.1
sssd-debuginfo-32bit-1.13.4-9.1
libipa_hbac-devel-1.13.4-9.1
sssd-32bit-1.13.4-9.1
libipa_hbac0-1.13.4-9.1
sssd-krb5-common-1.13.4-9.1
sssd-krb5-common-debuginfo-1.13.4-9.1
sssd-1.13.4-9.1
libsss_idmap0-debuginfo-1.13.4-9.1
libipa_hbac0-debuginfo-1.13.4-9.1
libsss_nss_idmap0-debuginfo-1.13.4-9.1

i586

sssd-proxy-1.13.4-9.1
sssd-ldap-debuginfo-1.13.4-9.1
sssd-ipa-1.13.4-9.1
sssd-ldap-1.13.4-9.1
python-ipa_hbac-debuginfo-1.13.4-9.1
python-sssd-config-debuginfo-1.13.4-9.1
sssd-debuginfo-1.13.4-9.1
python-sss_nss_idmap-debuginfo-1.13.4-9.1
libsss_nss_idmap-devel-1.13.4-9.1
libsss_sudo-debuginfo-1.13.4-9.1
sssd-ipa-debuginfo-1.13.4-9.1
sssd-debugsource-1.13.4-9.1
sssd-krb5-debuginfo-1.13.4-9.1
sssd-ad-1.13.4-9.1
libsss_nss_idmap0-1.13.4-9.1
libsss_idmap0-1.13.4-9.1
libsss_idmap-devel-1.13.4-9.1
sssd-ad-debuginfo-1.13.4-9.1
python-sssd-config-1.13.4-9.1
sssd-tools-debuginfo-1.13.4-9.1
python-sss_nss_idmap-1.13.4-9.1
sssd-krb5-1.13.4-9.1
python-ipa_hbac-1.13.4-9.1
sssd-tools-1.13.4-9.1
libsss_sudo-1.13.4-9.1
sssd-proxy-debuginfo-1.13.4-9.1
libipa_hbac-devel-1.13.4-9.1
libipa_hbac0-1.13.4-9.1
sssd-krb5-common-1.13.4-9.1
sssd-krb5-common-debuginfo-1.13.4-9.1
sssd-1.13.4-9.1
libsss_idmap0-debuginfo-1.13.4-9.1
libipa_hbac0-debuginfo-1.13.4-9.1
libsss_nss_idmap0-debuginfo-1.13.4-9.1

146054 - SuSE Linux 42.2 openSUSE-SU-2017:2916-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15591, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-5526

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2916-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00005.html>

SuSE Linux 42.2

x86_64

xen-debugsource-4.7.3_06-11.18.1
xen-tools-debuginfo-4.7.3_06-11.18.1
xen-libs-32bit-4.7.3_06-11.18.1
xen-tools-4.7.3_06-11.18.1
xen-tools-domU-debuginfo-4.7.3_06-11.18.1
xen-libs-debuginfo-4.7.3_06-11.18.1
xen-4.7.3_06-11.18.1
xen-libs-debuginfo-32bit-4.7.3_06-11.18.1
xen-libs-4.7.3_06-11.18.1
xen-devel-4.7.3_06-11.18.1
xen-doc-html-4.7.3_06-11.18.1
xen-tools-domU-4.7.3_06-11.18.1

i586

xen-debugsource-4.7.3_06-11.18.1
xen-tools-domU-debuginfo-4.7.3_06-11.18.1
xen-libs-debuginfo-4.7.3_06-11.18.1
xen-libs-4.7.3_06-11.18.1
xen-devel-4.7.3_06-11.18.1
xen-tools-domU-4.7.3_06-11.18.1

146056 - SuSE Linux 42.3 openSUSE-SU-2017:2938-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10911, CVE-2017-12809, CVE-2017-13672, CVE-2017-13711, CVE-2017-14167, CVE-2017-15038, CVE-2017-15268, CVE-2017-15289

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2938-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00012.html>

SuSE Linux 42.3

i586

qemu-linux-user-debuginfo-2.9.1-35.1
qemu-linux-user-debugsource-2.9.1-35.1
qemu-linux-user-2.9.1-35.1

noarch
qemu-seabios-1.10.2-35.1
qemu-sgabios-8-35.1
qemu-vgabios-1.10.2-35.1
qemu-ipxe-1.0.0-35.1

x86_64
qemu-block-curl-2.9.1-35.1
qemu-block-iscsi-debuginfo-2.9.1-35.1
qemu-guest-agent-debuginfo-2.9.1-35.1
qemu-extra-2.9.1-35.1
qemu-arm-2.9.1-35.1
qemu-x86-debuginfo-2.9.1-35.1
qemu-debugsource-2.9.1-35.1
qemu-ppc-2.9.1-35.1
qemu-block-ssh-debuginfo-2.9.1-35.1
qemu-testsuite-2.9.1-35.1
qemu-arm-debuginfo-2.9.1-35.1
qemu-guest-agent-2.9.1-35.1
qemu-linux-user-debugsource-2.9.1-35.1
qemu-tools-debuginfo-2.9.1-35.1
qemu-block-rbd-debuginfo-2.9.1-35.1
qemu-block-iscsi-2.9.1-35.1
qemu-linux-user-2.9.1-35.1
qemu-block-dmg-debuginfo-2.9.1-35.1
qemu-block-dmg-2.9.1-35.1
qemu-lang-2.9.1-35.1
qemu-kvm-2.9.1-35.1
qemu-block-ssh-2.9.1-35.1
qemu-block-rbd-2.9.1-35.1
qemu-s390-debuginfo-2.9.1-35.1
qemu-tools-2.9.1-35.1
qemu-2.9.1-35.1
qemu-s390-2.9.1-35.1
qemu-extra-debuginfo-2.9.1-35.1
qemu-x86-2.9.1-35.1
qemu-ppc-debuginfo-2.9.1-35.1
qemu-ksm-2.9.1-35.1
qemu-block-curl-debuginfo-2.9.1-35.1
qemu-linux-user-debuginfo-2.9.1-35.1

163490 - Oracle Enterprise Linux ELSA-2017-3637 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10044, CVE-2017-1000363, CVE-2017-1000380, CVE-2017-10661, CVE-2017-11473, CVE-2017-14489, CVE-2017-7308, CVE-2017-8831, CVE-2017-9074, CVE-2017-9075, CVE-2017-9077

Description

The scan detected that the host is missing the following update:
ELSA-2017-3637

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-November/007323.html>

OEL6
x86_64
kernel-uek-debug-devel-2.6.39-400.297.12.el6uek
kernel-uek-2.6.39-400.297.12.el6uek
kernel-uek-doc-2.6.39-400.297.12.el6uek
kernel-uek-devel-2.6.39-400.297.12.el6uek
kernel-uek-debug-2.6.39-400.297.12.el6uek

kernel-uek-firmware-2.6.39-400.297.12.el6uek

i386

kernel-uek-debug-devel-2.6.39-400.297.12.el6uek

kernel-uek-2.6.39-400.297.12.el6uek

kernel-uek-firmware-2.6.39-400.297.12.el6uek

kernel-uek-doc-2.6.39-400.297.12.el6uek

kernel-uek-debug-2.6.39-400.297.12.el6uek

kernel-uek-devel-2.6.39-400.297.12.el6uek

163491 - Oracle Enterprise Linux ELSA-2017-3636 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10044, CVE-2017-1000363, CVE-2017-1000380, CVE-2017-10661, CVE-2017-11473, CVE-2017-14489, CVE-2017-2671, CVE-2017-8831, CVE-2017-9075, CVE-2017-9077

Description

The scan detected that the host is missing the following update:
ELSA-2017-3636

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-November/007322.html>

<http://oss.oracle.com/pipermail/el-errata/2017-November/007321.html>

OEL7

x86_64

kernel-uek-firmware-3.8.13-118.19.12.el7uek

kernel-uek-devel-3.8.13-118.19.12.el7uek

kernel-uek-3.8.13-118.19.12.el7uek

kernel-uek-debug-3.8.13-118.19.12.el7uek

kernel-uek-doc-3.8.13-118.19.12.el7uek

kernel-uek-debug-devel-3.8.13-118.19.12.el7uek

dtrace-modules-3.8.13-118.19.12.el7uek-0.4.5-3.el7

OEL6

x86_64

dtrace-modules-3.8.13-118.19.12.el6uek-0.4.5-3.el6

kernel-uek-devel-3.8.13-118.19.12.el6uek

kernel-uek-debug-3.8.13-118.19.12.el6uek

kernel-uek-3.8.13-118.19.12.el6uek

kernel-uek-firmware-3.8.13-118.19.12.el6uek

kernel-uek-doc-3.8.13-118.19.12.el6uek

kernel-uek-debug-devel-3.8.13-118.19.12.el6uek

163493 - Oracle Enterprise Linux ELSA-2017-3635 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000112, CVE-2017-10661, CVE-2017-12154, CVE-2017-14106, CVE-2017-14489, CVE-2017-7482, CVE-2017-7541, CVE-2017-7542, CVE-2017-7618

Description

The scan detected that the host is missing the following update:
ELSA-2017-3635

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-November/007320.html>
<http://oss.oracle.com/pipermail/el-errata/2017-November/007319.html>

OEL7

x86_64
kernel-uek-4.1.12-103.9.2.el7uek
kernel-uek-debug-4.1.12-103.9.2.el7uek
kernel-uek-firmware-4.1.12-103.9.2.el7uek
kernel-uek-devel-4.1.12-103.9.2.el7uek
kernel-uek-doc-4.1.12-103.9.2.el7uek
kernel-uek-debug-devel-4.1.12-103.9.2.el7uek

OEL6

x86_64
kernel-uek-debug-devel-4.1.12-103.9.2.el6uek
kernel-uek-debug-4.1.12-103.9.2.el6uek
kernel-uek-devel-4.1.12-103.9.2.el6uek
kernel-uek-4.1.12-103.9.2.el6uek
kernel-uek-doc-4.1.12-103.9.2.el6uek
kernel-uek-firmware-4.1.12-103.9.2.el6uek

170896 - Amazon Linux AMI ALAS-2017-918 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15041, CVE-2017-15042

Description

The scan detected that the host is missing the following update:
ALAS-2017-918

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-918.html>

Amazon Linux AMI

i686
golang-bin-1.8.4-1.41.amzn1
golang-1.8.4-1.41.amzn1

noarch
golang-src-1.8.4-1.41.amzn1
golang-docs-1.8.4-1.41.amzn1
golang-misc-1.8.4-1.41.amzn1
golang-tests-1.8.4-1.41.amzn1

x86_64
golang-1.8.4-1.41.amzn1
golang-bin-1.8.4-1.41.amzn1
golang-race-1.8.4-1.41.amzn1

192839 - Fedora Linux 26 FEDORA-2017-0af85ae851 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1283

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0af85ae851

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/2017/11/?count=200&page=1>

Fedora Core 26

php-7.1.11-1.fc26

192841 - Fedora Linux 26 FEDORA-2017-c7bdf540b4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12629

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c7bdf540b4

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/2017/11/?count=200&page=3>

Fedora Core 26

lucene-6.1.0-6.fc26

192845 - Fedora Linux 26 FEDORA-2017-9149114fba Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11434, CVE-2017-12809, CVE-2017-13672, CVE-2017-14167, CVE-2017-15038, CVE-2017-15268

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9149114fba

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/2017/11/?count=200&page=1>

Fedora Core 26

qemu-2.9.1-2.fc26

192850 - Fedora Linux 25 FEDORA-2017-d4709b0d8b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13672, CVE-2017-13673, CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15591, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595

Description

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

FEDORA-2017-d4709b0d8b

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/2017/11/?count=200&page=2>

Fedora Core 25

xen-4.7.3-7.fc25

192853 - Fedora Linux 25 FEDORA-2017-005f8f7f7d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12629

Description

The scan detected that the host is missing the following update:
FEDORA-2017-005f8f7f7d

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/2017/11/?count=200&page=2>

Fedora Core 25

lucene-5.5.0-5.fc25

192857 - Fedora Linux 25 FEDORA-2017-cdaaf6ea12 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1283

Description

The scan detected that the host is missing the following update:
FEDORA-2017-cdaaf6ea12

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/2017/11/?count=200&page=1>

Fedora Core 25

php-7.0.25-1.fc25

192859 - Fedora Linux 26 FEDORA-2017-5bcddc1984 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13672, CVE-2017-13673, CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15591, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5bcddc1984

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/2017/11/?count=200&page=3>

Fedora Core 26

xen-4.8.2-4.fc26

192863 - Fedora Linux 26 FEDORA-2017-9c29af2c64 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-9099, CVE-2015-9100, CVE-2017-11720, CVE-2017-13712, CVE-2017-15018, CVE-2017-15019, CVE-2017-15045, CVE-2017-15046, CVE-2017-8419, CVE-2017-9410, CVE-2017-9411, CVE-2017-9412

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9c29af2c64

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/2017/11/?count=200&page=3>

Fedora Core 26

lame-3.100-1.fc26

22659 - Oracle JRockit Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2016-10165, CVE-2017-10281, CVE-2017-10295, CVE-2017-10345, CVE-2017-10347, CVE-2017-10355, CVE-2017-10356

Description

Multiple vulnerabilities are present in some versions of Oracle JRockit.

Observation

Oracle JRockit is a Java Virtual Machine (JVM).

Multiple vulnerabilities are present in some versions of Oracle JRockit. The flaws lie in several components. Successful exploitation could allow an attacker to disclose sensitive information or cause a denial of service condition.

130922 - Debian Linux 8.0, 9.0 DSA-4021-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14635

Description

The scan detected that the host is missing the following update:
DSA-4021-1

Observation

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

<http://www.debian.org/security/2017/dsa-4021>

Debian 8.0
all
otrs2_3.3.18-1+deb8u1

Debian 9.0
all
otrs2_5.0.16-1+deb9u2

130927 - Debian Linux 9.0 DSA-4015-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
DSA-4015-1

Observation

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

<http://www.debian.org/security/2017/dsa-4015>

Debian 9.0
all
openjdk-8-jdk_8u151-b12-1~deb9u1
openjdk-8-demo_8u151-b12-1~deb9u1
openjdk-8-doc_8u151-b12-1~deb9u1
openjdk-8-jre_8u151-b12-1~deb9u1
openjdk-8-jre-headless_8u151-b12-1~deb9u1
openjdk-8-jdk-headless_8u151-b12-1~deb9u1
openjdk-8-jre-zero_8u151-b12-1~deb9u1
openjdk-8-dbg_8u151-b12-1~deb9u1
openjdk-8-source_8u151-b12-1~deb9u1

130929 - Debian Linux 8.0, 9.0 DSA-4013-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10504, CVE-2016-1628, CVE-2016-5152, CVE-2016-5157, CVE-2016-9118, CVE-2017-14039, CVE-2017-14040, CVE-2017-14041, CVE-2017-14151, CVE-2017-14152

Description

The scan detected that the host is missing the following update:
DSA-4013-1

Observation

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

<http://www.debian.org/security/2017/dsa-4013>

Debian 8.0

all

libopenjpip-server_2.1.0-2+deb8u3
libopenjpip-viewer_2.1.0-2+deb8u3
libopenjp3d7_2.1.0-2+deb8u3
libopenjpip7_2.1.0-2+deb8u3
libopenjp2-tools_2.1.0-2+deb8u3
libopenjp2-7-dev_2.1.0-2+deb8u3
libopenjpip-dec-server_2.1.0-2+deb8u3
libopenjp3d-tools_2.1.0-2+deb8u3
libopenjp2-7_2.1.0-2+deb8u3
libopenjp2-7-dbg_2.1.0-2+deb8u3

Debian 9.0

all

libopenjp2-tools_2.1.2-1.1+deb9u2
libopenjp2-7-dbg_2.1.2-1.1+deb9u2
libopenjp3d-tools_2.1.2-1.1+deb9u2
libopenjpip-dec-server_2.1.2-1.1+deb9u2
libopenjp2-7-dev_2.1.2-1.1+deb9u2
libopenjp2-7_2.1.2-1.1+deb9u2
libopenjpip7_2.1.2-1.1+deb9u2
libopenjpip-viewer_2.1.2-1.1+deb9u2
libopenjpip-server_2.1.2-1.1+deb9u2
libopenjp3d7_2.1.2-1.1+deb9u2

141769 - Red Hat Enterprise Linux RHSA-2017-3111 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8184, CVE-2017-13738, CVE-2017-13740, CVE-2017-13741, CVE-2017-13742, CVE-2017-13743, CVE-2017-13744

Description

The scan detected that the host is missing the following update:
RHSA-2017-3111

Observation

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

<http://www.redhat.com/archives/rhsc-announce/2017-November/msg00001.html>

RHEL7D

x86_64

liblouis-2.5.2-11.el7_4
liblouis-debuginfo-2.5.2-11.el7_4
liblouis-devel-2.5.2-11.el7_4
liblouis-utils-2.5.2-11.el7_4

noarch

liblouis-doc-2.5.2-11.el7_4
liblouis-python-2.5.2-11.el7_4

RHEL7S

noarch

liblouis-doc-2.5.2-11.el7_4
liblouis-python-2.5.2-11.el7_4

x86_64

liblouis-2.5.2-11.el7_4
liblouis-debuginfo-2.5.2-11.el7_4
liblouis-devel-2.5.2-11.el7_4
liblouis-utils-2.5.2-11.el7_4

RHEL7WS
x86_64
liblouis-2.5.2-11.el7_4
liblouis-debuginfo-2.5.2-11.el7_4
liblouis-devel-2.5.2-11.el7_4
liblouis-utils-2.5.2-11.el7_4

noarch
liblouis-doc-2.5.2-11.el7_4
liblouis-python-2.5.2-11.el7_4

160322 - CentOS 7 CESA-2017-3111 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8184, CVE-2017-13738, CVE-2017-13740, CVE-2017-13741, CVE-2017-13742, CVE-2017-13743, CVE-2017-13744

Description

The scan detected that the host is missing the following update:
CESA-2017-3111

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-November/022612.html>

CentOS 7
i686
liblouis-devel-2.5.2-11.el7_4
liblouis-2.5.2-11.el7_4

noarch
liblouis-python-2.5.2-11.el7_4
liblouis-doc-2.5.2-11.el7_4

x86_64
liblouis-2.5.2-11.el7_4
liblouis-devel-2.5.2-11.el7_4
liblouis-utils-2.5.2-11.el7_4

163492 - Oracle Enterprise Linux ELSA-2017-3111 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8184, CVE-2017-13738, CVE-2017-13740, CVE-2017-13741, CVE-2017-13742, CVE-2017-13743, CVE-2017-13744

Description

The scan detected that the host is missing the following update:
ELSA-2017-3111

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-November/007325.html>

OEL7
x86_64
liblouis-2.5.2-11.el7_4

liblouis-python-2.5.2-11.el7_4
liblouis-doc-2.5.2-11.el7_4
liblouis-devel-2.5.2-11.el7_4
liblouis-utils-2.5.2-11.el7_4

170898 - Amazon Linux AMI ALAS-2017-920 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12166

Description

The scan detected that the host is missing the following update:
ALAS-2017-920

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-920.html>

Amazon Linux AMI
x86_64
openvpn-debuginfo-2.4.4-1.21.amzn1
openvpn-devel-2.4.4-1.21.amzn1
openvpn-2.4.4-1.21.amzn1

i686
openvpn-devel-2.4.4-1.21.amzn1
openvpn-debuginfo-2.4.4-1.21.amzn1
openvpn-2.4.4-1.21.amzn1

175284 - Scientific Linux Security ERRATA Moderate: liblouis on SL7.x x86_64 (1711-79)

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

Risk Level: Medium

CVE: CVE-2014-8184, CVE-2017-13738, CVE-2017-13740, CVE-2017-13741, CVE-2017-13742, CVE-2017-13743, CVE-2017-13744

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: liblouis on SL7.x x86_64 (1711-79)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1711&L=scientific-linux-errata&F=&S=&P=79>

SL7
x86_64
liblouis-2.5.2-11.el7_4
liblouis-debuginfo-2.5.2-11.el7_4
liblouis-devel-2.5.2-11.el7_4
liblouis-utils-2.5.2-11.el7_4

noarch
liblouis-doc-2.5.2-11.el7_4
liblouis-python-2.5.2-11.el7_4

185955 - Ubuntu Linux 16.04, 17.04, 17.10 USN-3473-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
USN-3473-1

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-November/004131.html>

Ubuntu 16.04

openjdk-8-jdk_8u151-b12-0ubuntu0.16.04.2
openjdk-8-jre-jamvm_8u151-b12-0ubuntu0.16.04.2
openjdk-8-jre_8u151-b12-0ubuntu0.16.04.2
openjdk-8-jre-headless_8u151-b12-0ubuntu0.16.04.2
openjdk-8-jdk-headless_8u151-b12-0ubuntu0.16.04.2
openjdk-8-jre-zero_8u151-b12-0ubuntu0.16.04.2

Ubuntu 17.04

openjdk-8-jdk-headless_8u151-b12-0ubuntu0.17.04.2
openjdk-8-jre-zero_8u151-b12-0ubuntu0.17.04.2
openjdk-8-jre_8u151-b12-0ubuntu0.17.04.2
openjdk-8-jdk_8u151-b12-0ubuntu0.17.04.2
openjdk-8-jre-headless_8u151-b12-0ubuntu0.17.04.2

Ubuntu 17.10

openjdk-8-jre_8u151-b12-0ubuntu0.17.10.2
openjdk-8-jre-zero_8u151-b12-0ubuntu0.17.10.2
openjdk-8-jdk_8u151-b12-0ubuntu0.17.10.2
openjdk-8-jre-headless_8u151-b12-0ubuntu0.17.10.2
openjdk-8-jdk-headless_8u151-b12-0ubuntu0.17.10.2

192851 - Fedora Linux 25 FEDORA-2017-2aa4d11993 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12166

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2aa4d11993

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/2017/11/?count=200&page=3>

Fedora Core 25

openvpn-2.4.4-1.fc25

192855 - Fedora Linux 25 FEDORA-2017-805d9423f8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14517, CVE-2017-14518, CVE-2017-14519, CVE-2017-14520, CVE-2017-14617, CVE-2017-14926, CVE-2017-14927, CVE-2017-14928, CVE-2017-14929

Description

The scan detected that the host is missing the following update:
FEDORA-2017-805d9423f8

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/2017/11/?count=200&page=2>

Fedora Core 25

poppler-0.45.0-9.fc25

192860 - Fedora Linux 26 FEDORA-2017-5b132e3803 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2888

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5b132e3803

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/2017/11/?count=200&page=3>

Fedora Core 26

SDL2-2.0.7-1.fc26

192870 - Fedora Linux 26 FEDORA-2017-51ff8fe326 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14517, CVE-2017-14518, CVE-2017-14519, CVE-2017-14617, CVE-2017-14926, CVE-2017-14927, CVE-2017-14928, CVE-2017-14929

Description

The scan detected that the host is missing the following update:
FEDORA-2017-51ff8fe326

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/2017/11/?count=200&page=1>

Fedora Core 26

poppler-0.52.0-9.fc26

22638 - Cisco NX-OS Software Python Parser Escape Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12301

Description

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

Observation

Cisco NX-OS is a network operating system .

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the Python scripting subsystem. Successful exploitation could allow a local attacker to gain privileges and execute arbitrary code on the target system.

22646 - Oracle iPlanet Web Server Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2017-10055

Description

A vulnerability is present in some versions of Oracle iPlanet Web Server.

Observation

Oracle iPlanet Web Server is an enterprise web application server.

A vulnerability is present in some versions of Oracle iPlanet Web Server. The flaw lies in the Administrative Graphical User Interface component. Successful exploitation could allow an attacker to compromise the integrity of the server and could lead to information disclosure.

22647 - Oracle iPlanet Web Server Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2017-10055

Description

A vulnerability is present in some versions of Oracle iPlanet Web Server.

Observation

Oracle iPlanet Web Server is an enterprise web application server.

A vulnerability is present in some versions of Oracle iPlanet Web Server. The flaw lies in the Administrative Graphical User Interface component. Successful exploitation could allow an attacker to compromise the integrity of the server and could lead to information disclosure.

22653 - (K62279530) F5 BIG-IP ConfigSync mcpd Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6161

Description

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

Observation

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

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

22654 - IBM WebSphere Application Server Multiple JSF Vulnerabilities (swg22008707)

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

Risk Level: Medium

CVE: CVE-2011-4343, CVE-2017-1583

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a Java application server.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaws lie in the Java Server Faces component. Successful exploitation could allow an attacker to obtain sensitive information.

22656 - (K74413297) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3184

Description

A 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 vulnerability is present in some versions of F5 BIG-IP products. The flaw is due to improper handling of a crafted device that provides a small report descriptor. Successful exploitation could allow a physically proximate attacker to obtain unauthorized information, perform unauthorized modification of data, or cause a denial of service.

22660 - Oracle Access Manager Critical Patch Update October 2017

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

Risk Level: Medium

CVE: CVE-2017-10154, CVE-2017-10259

Description

A vulnerability is present in some versions of Oracle Access Manager.

Observation

Oracle Access Manager is a software solution providing identity and access management for access to enterprise.

A vulnerability is present in some versions of Oracle Access Manager. The flaw lies in oracle access manager web server plugin. Successful exploitation could allow an attacker to disclose sensitive information.

22671 - (HPESBMU03753) HPE System Management Homepage Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-8743, CVE-2017-12544, CVE-2017-12545, CVE-2017-12546, CVE-2017-12547, CVE-2017-12548, CVE-2017-12549, CVE-2017-12550, CVE-2017-12551, CVE-2017-12552, CVE-2017-12553

Description

Multiple vulnerabilities are present in some versions of HPE System Management Homepage.

Observation

HPE System Management Homepage is a web-based interface that consolidates and simplifies the management of individual ProLiant and Integrity servers.

Multiple vulnerabilities are present in some versions of HPE System Management Homepage. The flaws lie in multiple components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or execute arbitrary code on the target system.

130925 - Debian Linux 9.0 DSA-4018-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

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

DSA-4018-1

Observation

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

<http://www.debian.org/security/2017/dsa-4018>

Debian 9.0

all

openssl_1.1.0f-3+deb9u1

130930 - Debian Linux 9.0 DSA-4017-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

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

DSA-4017-1

Observation

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

<http://www.debian.org/security/2017/dsa-4017>

Debian 9.0

all

libssl1.0.2-udeb_1.0.2l-2+deb9u1

libcrypto1.0.2-udeb_1.0.2l-2+deb9u1

libssl1.0-dev_1.0.2l-2+deb9u1

libssl1.0.2_1.0.2l-2+deb9u1

146047 - SuSE SLED 12 SP2, 12 SP3 SUSE-SU-2017:2931-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14226

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2931-1

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-November/003372.html>

SuSE SLED 12 SP3

x86_64

libwpd-debugsource-0.10.2-2.4.1

libwpd-0_10-10-0.10.2-2.4.1

libwpd-0_10-10-debuginfo-0.10.2-2.4.1

SuSE SLED 12 SP2

x86_64

libwpd-debugsource-0.10.2-2.4.1

libwpd-0_10-10-0.10.2-2.4.1

libwpd-0_10-10-debuginfo-0.10.2-2.4.1

146052 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2943-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14226

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2943-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00017.html>

SuSE Linux 42.2

i586

libwpd-debugsource-0.10.2-5.3.1

libwpd-tools-debuginfo-0.10.2-5.3.1

libwpd-tools-0.10.2-5.3.1

libwpd-0_10-10-debuginfo-0.10.2-5.3.1

libwpd-0_10-10-0.10.2-5.3.1

libwpd-devel-0.10.2-5.3.1

noarch

libwpd-devel-doc-0.10.2-5.3.1

x86_64

libwpd-debugsource-0.10.2-5.3.1

libwpd-tools-debuginfo-0.10.2-5.3.1

libwpd-tools-0.10.2-5.3.1

libwpd-0_10-10-debuginfo-0.10.2-5.3.1

libwpd-0_10-10-0.10.2-5.3.1

libwpd-devel-0.10.2-5.3.1

SuSE Linux 42.3

x86_64

libwpd-tools-0.10.2-8.1

libwpd-0_10-10-debuginfo-0.10.2-8.1

libwpd-devel-0.10.2-8.1

libwpd-tools-debuginfo-0.10.2-8.1
libwpd-0_10-10-0.10.2-8.1
libwpd-debugsource-0.10.2-8.1

noarch
libwpd-devel-doc-0.10.2-8.1

146055 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2939-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11554, CVE-2017-11555, CVE-2017-11556, CVE-2017-11605, CVE-2017-11608

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2939-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00013.html>

SuSE Linux 42.2
x86_64
libsass-devel-3.3.2-2.3.1
libsass-debugsource-3.3.2-2.3.1
libsass-3_3_2-0-debuginfo-3.3.2-2.3.1
libsass-3_3_2-0-3.3.2-2.3.1

i586
libsass-devel-3.3.2-2.3.1
libsass-debugsource-3.3.2-2.3.1
libsass-3_3_2-0-debuginfo-3.3.2-2.3.1
libsass-3_3_2-0-3.3.2-2.3.1

SuSE Linux 42.3
x86_64
libsass-3_3_2-0-debuginfo-3.3.2-5.1
libsass-devel-3.3.2-5.1
libsass-debugsource-3.3.2-5.1
libsass-3_3_2-0-3.3.2-5.1

i586
libsass-3_3_2-0-debuginfo-3.3.2-5.1
libsass-devel-3.3.2-5.1
libsass-debugsource-3.3.2-5.1
libsass-3_3_2-0-3.3.2-5.1

170895 - Amazon Linux AMI ALAS-2017-919 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000254

Description

The scan detected that the host is missing the following update:
ALAS-2017-919

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-919.html>

Amazon Linux AMI
x86_64
curl-7.53.1-11.78.amzn1
libcurl-devel-7.53.1-11.78.amzn1
curl-debuginfo-7.53.1-11.78.amzn1
libcurl-7.53.1-11.78.amzn1

i686
curl-7.53.1-11.78.amzn1
libcurl-devel-7.53.1-11.78.amzn1
curl-debuginfo-7.53.1-11.78.amzn1
libcurl-7.53.1-11.78.amzn1

170897 - Amazon Linux AMI ALAS-2017-921 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12171

Description

The scan detected that the host is missing the following update:
ALAS-2017-921

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-921.html>

Amazon Linux AMI
i686
httpd-devel-2.2.34-1.16.amzn1
mod_ssl-2.2.34-1.16.amzn1
httpd-2.2.34-1.16.amzn1
httpd-tools-2.2.34-1.16.amzn1
httpd-debuginfo-2.2.34-1.16.amzn1

noarch
httpd-manual-2.2.34-1.16.amzn1

x86_64
httpd-devel-2.2.34-1.16.amzn1
mod_ssl-2.2.34-1.16.amzn1
httpd-2.2.34-1.16.amzn1
httpd-tools-2.2.34-1.16.amzn1
httpd-debuginfo-2.2.34-1.16.amzn1

182508 - FreeBSD OpenSSL Multiple Vulnerabilities (f40f07aa-c00f-11e7-ac58-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

The scan detected that the host is missing the following update:
OpenSSL -- Multiple vulnerabilities (f40f07aa-c00f-11e7-ac58-b499baebfeaf)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/f40f07aa-c00f-11e7-ac58-b499baebfeaf.html>

Affected packages:

openssl < 1.0.2m,1

openssl-devel < 1.1.0g

185959 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3475-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

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

USN-3475-1

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-November/004130.html>

Ubuntu 16.04

libssl1.0.0_1.0.2g-1ubuntu4.9

Ubuntu 14.04

libssl1.0.0_1.0.1f-1ubuntu2.23

Ubuntu 17.04

libssl1.0.0_1.0.2g-1ubuntu11.3

Ubuntu 17.10

libssl1.0.0_1.0.2g-1ubuntu13.2

192843 - Fedora Linux 25 FEDORA-2017-95327e44ec Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10279, CVE-2017-10283, CVE-2017-10286, CVE-2017-10294, CVE-2017-10314, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

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

FEDORA-2017-95327e44ec

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/2017/11/?count=200&page=1>

Fedora Core 25

community-mysql-5.7.20-1.fc25

192865 - Fedora Linux 26 FEDORA-2017-50c790aaed Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10279, CVE-2017-10283, CVE-2017-10286, CVE-2017-10294, CVE-2017-10314, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

The scan detected that the host is missing the following update:
FEDORA-2017-50c790aaed

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/2017/11/?count=200&page=1>

Fedora Core 26

community-mysql-5.7.20-1.fc26

192868 - Fedora Linux 26 FEDORA-2017-bcdeca9d41 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0379

Description

The scan detected that the host is missing the following update:
FEDORA-2017-bcdeca9d41

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/2017/11/?count=200&page=1>

Fedora Core 26

libgcrypt-1.7.9-1.fc26

88896 - Slackware Linux 14.1, 14.2 SSA:2017-306-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10268, CVE-2017-10378

Description

The scan detected that the host is missing the following update:
SSA:2017-306-01

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.393003>

Slackware 14.1

x86_64

mariadb-5.5.58-x86_64-1

Slackware 14.2

x86_64
mariadb-10.0.33-x86_64-1

i586
mariadb-10.0.33-i586-1

22651 - (K30201296) F5 BIG-IP SOCKS proxy Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2017-0303

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 SOCKS Profile. Successful exploitation could allow an attacker to cause denial of service.

33375 - Oracle Solaris 145333-38 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
145333-38

Observation

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

<https://getupdates.oracle.com/readme/145333-38>

Oracle Solaris Cluster 3.3: Core Patch for Oracle Solaris 10

SOLARIS_10

SUNWscsal:3.3.0,REV=2010.07.26.13.19
SUNWscmasasen:3.3.0,REV=2010.07.26.13.19
SUNWsccomzu:3.3.0,REV=2010.07.26.13.19
SUNWsczu:3.3.0,REV=2010.07.26.13.19
SUNWscmasau:3.3.0,REV=2010.07.26.13.19
SUNWudlmr:3.3.0,REV=2010.07.26.13.19
SUNWsczr:3.3.0,REV=2010.07.26.13.19
SUNWscsckr:3.3.0,REV=2010.07.26.13.19
SUNWscderby:3.3.0,REV=2010.07.26.13.19
SUNWscmasa:3.3.0,REV=2010.07.26.13.19
SUNWscrtlh:3.3.0,REV=2010.07.26.13.19
SUNWscmasar:3.3.0,REV=2010.07.26.13.19
SUNWscmasazu:3.3.0,REV=2010.07.26.13.19
SUNWscu:3.3.0,REV=2010.07.26.13.19
SUNWscucm:3.3.0,REV=2010.07.26.13.19
SUNWscsmf:3.3.0,REV=2010.07.26.13.19
SUNWscspmu:3.3.0,REV=2010.07.26.13.19
SUNWscdev:3.3.0,REV=2010.07.26.13.19
SUNWcvmr:3.3.0,REV=2010.07.26.13.19
SUNWsc telemetry:3.3.0,REV=2010.07.26.13.19
SUNWscmd:3.3.0,REV=2010.07.26.13.19

SUNWscmautil:3.3.0,REV=2010.07.26.13.19
SUNWsccomu:3.3.0,REV=2010.07.26.13.19
SUNWscgds:3.3.0,REV=2010.07.26.13.19
SUNWscr:3.3.0,REV=2010.07.26.13.19

33376 - Oracle Solaris 145334-38 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
145334-38

Observation

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

<https://getupdates.oracle.com/readme/145334-38>

Oracle Solaris Cluster 3.3: Core Patch for Oracle Solaris 10(x86)

SOLARIS_10_x86

SUNWscderby:3.3.0,REV=2010.07.26.13.13
SUNWscr:3.3.0,REV=2010.07.26.13.13
SUNWscmautil:3.3.0,REV=2010.07.26.13.13
SUNWscmasasen:3.3.0,REV=2010.07.26.13.13
SUNWsc telemetry:3.3.0,REV=2010.07.26.13.13
SUNWscmasazu:3.3.0,REV=2010.07.26.13.13
SUNWscsmf:3.3.0,REV=2010.07.26.13.13
SUNWscu:3.3.0,REV=2010.07.26.13.13
SUNWscucm:3.3.0,REV=2010.07.26.13.13
SUNWscmasau:3.3.0,REV=2010.07.26.13.13
SUNWscsckr:3.3.0,REV=2010.07.26.13.13
SUNWscgds:3.3.0,REV=2010.07.26.13.13
SUNWscspmu:3.3.0,REV=2010.07.26.13.13
SUNWsczr:3.3.0,REV=2010.07.26.13.13
SUNWscdev:3.3.0,REV=2010.07.26.13.13
SUNWscrtlh:3.3.0,REV=2010.07.26.13.13
SUNWscmasa:3.3.0,REV=2010.07.26.13.13
SUNWsccomu:3.3.0,REV=2010.07.26.13.13
SUNWscmd:3.3.0,REV=2010.07.26.13.13
SUNWscmasar:3.3.0,REV=2010.07.26.13.13
SUNWsccomzu:3.3.0,REV=2010.07.26.13.13
SUNWsczu:3.3.0,REV=2010.07.26.13.13
SUNWscsal:3.3.0,REV=2010.07.26.13.13

88895 - Slackware Linux 14.2 SSA:2017-306-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3736

Description

The scan detected that the host is missing the following update:
SSA:2017-306-02

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.493670>

Slackware 14.2
x86_64
openssl-solibs-1.0.2m-x86_64-1
openssl-1.0.2m-x86_64-1

i586
openssl-1.0.2m-i586-1
openssl-solibs-1.0.2m-i586-1

130924 - Debian Linux 9.0 DSA-4020-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-15396, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

Description

The scan detected that the host is missing the following update:
DSA-4020-1

Observation

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

<http://www.debian.org/security/2017/dsa-4020>

Debian 9.0
all
chromium-l10n_62.0.3202.75-1~deb9u1
chromedriver_62.0.3202.75-1~deb9u1
chromium-driver_62.0.3202.75-1~deb9u1
chromium-widevine_62.0.3202.75-1~deb9u1
chromium_62.0.3202.75-1~deb9u1
chromium-shell_62.0.3202.75-1~deb9u1

130926 - Debian Linux 9.0 DSA-4023-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15566

Description

The scan detected that the host is missing the following update:
DSA-4023-1

Observation

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

<http://www.debian.org/security/2017/dsa-4023>

Debian 9.0
all
slurm-llnl_16.05.9-1+deb9u1

182509 - FreeBSD wordpress Multiple Issues (cee3d12f-bf41-11e7-bced-00e04c1ea73d)

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:
wordpress -- multiple issues (cee3d12f-bf41-11e7-bced-00e04c1ea73d)

Observation

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

<http://www.vuxml.org/freebsd/cee3d12f-bf41-11e7-bced-00e04c1ea73d.html>

Affected packages:
wordpress < 4.8.3,1

185957 - Ubuntu Linux 14.04 USN-3472-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12607, CVE-2017-12608

Description

The scan detected that the host is missing the following update:
USN-3472-1

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-November/004127.html>

Ubuntu 14.04

libreoffice-core_4.2.8-0ubuntu5.2

192838 - Fedora Linux 25 FEDORA-2017-ebab38baf6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15951

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ebab38baf6

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/2017/11/?count=200&page=2>

Fedora Core 25

kernel-4.13.10-100.fc25

192840 - Fedora Linux 25 FEDORA-2017-b1492e4844 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-b1492e4844

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/2017/11/?count=200&page=2>

Fedora Core 25

java-1.8.0-openjdk-1.8.0.151-1.b12.fc25

192842 - Fedora Linux 26 FEDORA-2017-9232eac8e8 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7500, CVE-2017-7501

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9232eac8e8

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/2017/11/?count=200&page=1>

Fedora Core 26

rpm-4.13.0.2-1.fc26

192844 - Fedora Linux 26 FEDORA-2017-94a173c491 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1002157

Description

The scan detected that the host is missing the following update:
FEDORA-2017-94a173c491

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/2017/11/?count=200&page=1>

Fedora Core 26

modulemd-1.3.2-1.fc26

192846 - Fedora Linux 25 FEDORA-2017-e3bf383b11 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-e3bf383b11

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/2017/11/?count=200&page=3>

Fedora Core 25

gnome-shell-3.22.3-2.fc25

192847 - Fedora Linux 26 FEDORA-2017-a47c76eeb1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15096

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a47c76eeb1

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/2017/11/?count=200&page=3>

Fedora Core 26

glusterfs-3.10.6-4.fc26

192848 - Fedora Linux 26 FEDORA-2017-6f8fcff58c 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-2017-6f8fcff58c

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/2017/11/?count=200&page=3>

Fedora Core 26

systemd-233-7.fc26

192849 - Fedora Linux 26 FEDORA-2017-7b17451b82 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-2017-7b17451b82

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/2017/11/?count=200&page=3>

Fedora Core 26

java-1.8.0-openjdk-1.8.0.151-1.b12.fc26

192852 - Fedora Linux 26 FEDORA-2017-9fbb35aeda Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12193

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9fbb35aeda

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/2017/11/?count=200&page=1>

Fedora Core 26

kernel-4.13.11-200.fc26

192854 - Fedora Linux 25 FEDORA-2017-8258f76154 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1002157

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8258f76154

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/2017/11/?count=200&page=1>

Fedora Core 25

modulemd-1.3.2-1.fc25

192856 - Fedora Linux 25 FEDORA-2017-6e2071419d 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-2017-6e2071419d

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/2017/11/?count=200&page=2>

Fedora Core 25

seamonkey-2.49.1-1.fc25

192858 - Fedora Linux 25 FEDORA-2017-c582c1e728 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14919

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c582c1e728

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/2017/11/?count=200&page=1>

Fedora Core 25

nodejs-6.11.5-1.fc25

192861 - Fedora Linux 26 FEDORA-2017-10faeda281 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15951

Description

The scan detected that the host is missing the following update:
FEDORA-2017-10faeda281

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/2017/11/?count=200&page=2>

Fedora Core 26

kernel-4.13.10-200.fc26

192862 - Fedora Linux 25 FEDORA-2017-150762f6be Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15096

Description

The scan detected that the host is missing the following update:
FEDORA-2017-150762f6be

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/2017/11/?count=200&page=2>

Fedora Core 25

glusterfs-3.10.6-4.fc25

192864 - Fedora Linux 25 FEDORA-2017-38b37120a2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12193

Description

The scan detected that the host is missing the following update:
FEDORA-2017-38b37120a2

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/2017/11/?count=200&page=1>

Fedora Core 25

kernel-4.13.11-100.fc25

192866 - Fedora Linux 26 FEDORA-2017-f0b3231763 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13089, CVE-2017-13090

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f0b3231763

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/2017/11/?count=200&page=1>

Fedora Core 26

wget-1.19.2-1.fc26

192867 - Fedora Linux 26 FEDORA-2017-ebf32659bf Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000257

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ebf32659bf

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/2017/11/?count=200&page=3>

Fedora Core 26

curl-7.53.1-12.fc26

192869 - Fedora Linux 26 FEDORA-2017-2e7badfe67 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-2017-2e7badfe67

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/2017/11/?count=200&page=2>

Fedora Core 26

seamonkey-2.49.1-1.fc26

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.

22487 - iniNet Solutions GmbH SCADA Webserver Improper Authentication Vulnerability

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

Risk Level: High

CVE: CVE-2017-13995

Update Details

Observation is updated

22626 - iniNet Solutions GmbH SCADA Webserver Improper Authentication Vulnerability

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

Risk Level: High

CVE: CVE-2017-13995

Update Details

Observation is updated FASLScript is updated

20746 - (JSA10763) Juniper Junos Multiple Privilege Escalation Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4922

[Update Details](#)

Risk is updated

93465 - Mandriva Linux MBS1 MDVSA-2015-025 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9474

[Update Details](#)

Risk is updated

93563 - Mandriva Linux MBS2 MDVSA-2015-143 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9474

[Update Details](#)

Risk is updated

141745 - Red Hat Enterprise Linux RHSA-2017-2886 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6664, CVE-2016-8327, CVE-2017-3238, CVE-2017-3244, CVE-2017-3251, CVE-2017-3256, CVE-2017-3257, CVE-2017-3258, CVE-2017-3273, CVE-2017-3291, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3319, CVE-2017-3320, CVE-2017-3331, CVE-2017-3450, CVE-2017-3453, CVE-2017-3454, CVE-2017-3455, CVE-2017-3456, CVE-2017-3457, CVE-2017-3458, CVE-2017-3459, CVE-2017-3460, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3465, CVE-2017-3467, CVE-2017-3468, CVE-2017-3529, CVE-2017-3599, CVE-2017-3600, CVE-2017-3633, CVE-2017-3634, CVE-2017-3637, CVE-2017-3638, CVE-2017-3639, CVE-2017-3640, CVE-2017-3641, CVE-2017-3642, CVE-2017-3643, CVE-2017-3644, CVE-2017-3645, CVE-2017-3646, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3650, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

[Update Details](#)

CVE is updated

143464 - SuSE SLES 11 SP3, SLED 11 SP3 SUSE-SU-2015:0219-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9474

[Update Details](#)

Risk is updated

178140 - Gentoo Linux GLSA-201512-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9474

[Update Details](#)

Risk is updated

181632 - FreeBSD p5-UI-Dialog Shell Command Execution Vulnerability (00dadbf0-6f61-11e5-a2a1-002590263bf5)

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

Risk Level: High

CVE: CVE-2008-7315

[Update Details](#)

Risk is updated

182076 - FreeBSD FreeBSD Local Privilege Escalation In IRET Handler (0dfa5dde-600a-11e6-a6c3-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2015-5675

[Update Details](#)

Risk is updated

182476 - FreeBSD rubygems Deserialization Vulnerability (2c8bd00d-ada2-11e7-82af-8dbff7d75206)

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

Risk Level: High

CVE: CVE-2017-0903

[Update Details](#)

Risk is updated

182489 - FreeBSD solr Code Execution Via Entity Expansion (e837390d-0ceb-46b8-9b32-29c1195f5dc7)

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

Risk Level: High

CVE: CVE-2017-12629

[Update Details](#)

Risk is updated

188782 - Fedora Linux 21 FEDORA-2014-16967 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9474

[Update Details](#)

Risk is updated

188793 - Fedora Linux 20 FEDORA-2014-16964 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9474

[Update Details](#)

Risk is updated

19974 - (JSA10723) Juniper Junos J-web Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-1261

[Update Details](#)

Risk is updated

141746 - Red Hat Enterprise Linux RHSA-2017-2899 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11292

[Update Details](#)

Risk is updated

146027 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2895-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2888

[Update Details](#)

Risk is updated

182482 - FreeBSD Flash Player Remote Code Execution (a73518da-b2fa-11e7-98ef-d43d7ef03aa6)

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

Risk Level: Medium

CVE: CVE-2017-11292

[Update Details](#)

Risk is updated

190745 - Fedora Linux 22 FEDORA-2016-90836ca57d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8239

[Update Details](#)

Risk is updated

190863 - Fedora Linux 23 FEDORA-2016-f1e8e27e27 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8239

[Update Details](#)

Risk is updated

192780 - Fedora Linux 27 FEDORA-2017-2c58422bc0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2887

[Update Details](#)

Risk is updated

192798 - Fedora Linux 27 FEDORA-2017-ce403f01ce Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2888

[Update Details](#)

Risk is updated

192807 - Fedora Linux 25 FEDORA-2017-15987a1b7f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2887

[Update Details](#)

Risk is updated

192814 - Fedora Linux 26 FEDORA-2017-9b0095a6f2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2887

[Update Details](#)

Risk is updated

192836 - Fedora Linux 25 FEDORA-2017-5934ecf841 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2888

[Update Details](#)

Risk is updated

14558 - Microsoft TURKTRUST.Inc Fraudulent Certificates Spoofing (2798897)

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

22629 - (JSA10811) Juniper SRX Series Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10608

[Update Details](#)

Risk is updated

130269 - Debian Linux 7.0, 8.0 DSA-3353-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5177

[Update Details](#)

Risk is updated

130785 - Debian Linux 8.0 DSA-3871-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5637

[Update Details](#)

Risk is updated

130893 - Debian Linux 8.0, 9.0 DSA-3990-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14603

[Update Details](#)

Risk is updated

146006 - SuSE Linux 42.3 openSUSE-SU-2017:2820-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11424

[Update Details](#)

CVE is updated

182474 - FreeBSD zookeeper Denial Of Service (af61b271-9e47-4db0-a0f6-29fb032236a3)

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

Risk Level: Medium

CVE: CVE-2017-5637

[Update Details](#)

Risk is updated

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

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

Risk Level: Medium

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

[Update Details](#)

FASLScript is updated

184970 - Ubuntu Linux 12.04, 14.04, 15.04 USN-2730-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-4428, CVE-2015-5177

[Update Details](#)

Risk is updated

190789 - Fedora Linux 22 FEDORA-2016-03c0ed3127 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7503

[Update Details](#)

Risk is updated

190890 - Fedora Linux 23 FEDORA-2016-8952105d59 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7503

[Update Details](#)

Risk is updated

13888 - Microsoft Unauthorized Digital Certificates Could Allow Spoofing (2728973)

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

20707 - (JSA10764) Juniper Junos J-web Cross Site Scripting Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-4923

[Update Details](#)

Risk is updated

22628 - (JSA10813) Juniper SRX Series Flowd Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-10610

[Update Details](#)

Risk is updated

93461 - Mandriva Linux MBS1 MDVSA-2015-014 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

93523 - Mandriva Linux MBS2 MDVSA-2015-152 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

130907 - Debian Linux 8.0, 9.0 DSA-4000-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12176, CVE-2017-12177, CVE-2017-12178, CVE-2017-12179, CVE-2017-12180, CVE-2017-12181, CVE-2017-12182, CVE-2017-12183, CVE-2017-12184, CVE-2017-12185, CVE-2017-12186, CVE-2017-12187, CVE-2017-13721, CVE-2017-13723

[Update Details](#)

Risk is updated

142558 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1637-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

143372 - SuSE SLES 12, SLED 12 SUSE-SU-2015:0029-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

170517 - Amazon Linux AMI ALAS-2015-540 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

170770 - Amazon Linux AMI ALAS-2017-794 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8734

[Update Details](#)

Risk is updated

182184 - FreeBSD subversion Unrestricted XML Entity Expansion In Mod_dontdothat And Subversionclients Using Http (s) (ac256985-b6a9-11e6-

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

Risk Level: Medium

CVE: CVE-2016-8734

[Update Details](#)

Risk is updated

182473 - FreeBSD xorg-server Multiple Vulnerabilities (4f8ffb9c-f388-4fbd-b90f-b3131559d888)

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

Risk Level: Medium

CVE: CVE-2017-13721, CVE-2017-13723

[Update Details](#)

Risk is updated

185914 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3453-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13721, CVE-2017-13723

[Update Details](#)

Risk is updated

188747 - Fedora Linux 21 FEDORA-2014-17543 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

188754 - Fedora Linux 20 FEDORA-2014-17561 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

188938 - Fedora Linux 20 FEDORA-2015-2580 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

188953 - Fedora Linux 21 FEDORA-2015-2615 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9092

[Update Details](#)

Risk is updated

191588 - Fedora Linux 25 FEDORA-2017-c629f16f6c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8734

[Update Details](#)

Risk is updated

22632 - (JSA10816) Juniper Junos OS Kernel Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2017-10613

[Update Details](#)

Risk is updated

22633 - (JSA10809) Juniper SRX Series Cryptographic Weakness Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2017-10606

[Update Details](#)

Risk is updated

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFFEE 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