2017-DEC-06
FSL version 7.5.978

MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

22792 - (HPSBMU02933) HPE SiteScope Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2013-4835, CVE-2013-6207

Description

Multiple vulnerabilities are present in some versions of HP SiteScope.

Observation

HP SiteScope is an agent-less monitoring software that monitors the availability and performance of IT infrastructures and application components remotely.

Multiple vulnerabilities are present in some versions of HP SiteScope. The flaws lie in multiple components. Successful exploitation could allow an attacker to access arbitrary file, cause a denial of service, or execute arbitrary code.

160329 - CentOS 7 CESA-2017-3269 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16844

Description

The scan detected that the host is missing the following update:
CESA-2017-3269

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/022647.html

CentOS 7
x86_64
procmail-3.22-36.el7_4.1

163507 - Oracle Enterprise Linux ELSA-2017-3269 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16844

Description

The scan detected that the host is missing the following update:
ELSA-2017-3269

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/007357.html

OEL7
x86_64
procmail-3.22-36.el7_4.1

175292 - Scientific Linux Security ERRATA Important: procmail on SL7.x x86_64 (1711-7080)

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

Risk Level: High

CVE: CVE-2017-16844

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: procmail on SL7.x x86_64 (1711-7080)

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=7080

SL7
x86_64
procmail-3.22-36.el7_4.1
procmail-debuginfo-3.22-36.el7_4.1

22785 - (HPESBHF03786) HPE Intelligent Management Center Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-8958

Description

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center. The flaw lies in an unknown component. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22795 - (HPESBHF03778) HPE Intelligent Management Center Multiple Vulnerabilities

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-12556, CVE-2017-12557, CVE-2017-12558

Description

Multiple remote code execution vulnerabilities are present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

Multiple remote code execution vulnerabilities are present in some versions of HPE Intelligent Management Center. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22796 - (HPESBHF03781) HPE Intelligent Management Center Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-12561

Description

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A remote code execution vulnerabilitiy is present in some versions of HPE Intelligent Management Center. The flaw lies in dbman service. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22798 - (HPESBHF03782) HPE Intelligent Management Center Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-12554

Description

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center. The flaw lies is due to improper input validation. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

130960 - Debian Linux 9.0 DSA-4050-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14316, CVE-2017-14317, CVE-2017-14318, CVE-2017-14319, CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-15597, CVE-2017-17044, CVE-2017-17045, CVE-2017-17046

Description

The scan detected that the host is missing the following update:
DSA-4050-1

Observation

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

http://www.debian.org/security/2017/dsa-4050

Debian 9.0
all
xen-system-armhf_4.8.2+xsa245-0+deb9u1
xen-system-arm64_4.8.2+xsa245-0+deb9u1
libxenstore3.0_4.8.2+xsa245-0+deb9u1
xen-utils-common_4.8.2+xsa245-0+deb9u1
xen-hypervisor-4.8-arm64_4.8.2+xsa245-0+deb9u1
xen-utils-4.8_4.8.2+xsa245-0+deb9u1
xen-hypervisor-4.8-amd64_4.8.2+xsa245-0+deb9u1
libxen-4.8_4.8.2+xsa245-0+deb9u1
xen-system-amd64_4.8.2+xsa245-0+deb9u1
xenstore-utils_4.8.2+xsa245-0+deb9u1
xen-hypervisor-4.8-armhf_4.8.2+xsa245-0+deb9u1
libxen-dev_4.8.2+xsa245-0+deb9u1

146108 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:3115-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15289, CVE-2017-15597

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3115-1

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/003422.html

SuSE SLED 12 SP3
x86_64
xen-libs-4.9.1_02-3.21.1
xen-4.9.1_02-3.21.1
xen-libs-debuginfo-4.9.1_02-3.21.1
xen-libs-32bit-4.9.1_02-3.21.1
xen-libs-debuginfo-32bit-4.9.1_02-3.21.1
xen-debugsource-4.9.1_02-3.21.1

SuSE SLES 12 SP3
x86_64
xen-doc-html-4.9.1_02-3.21.1
xen-tools-domU-4.9.1_02-3.21.1
xen-libs-4.9.1_02-3.21.1
xen-tools-domU-debuginfo-4.9.1_02-3.21.1
xen-4.9.1_02-3.21.1

xen-libs-debuginfo-4.9.1_02-3.21.1
xen-tools-4.9.1_02-3.21.1
xen-libs-32bit-4.9.1_02-3.21.1
xen-libs-debuginfo-32bit-4.9.1_02-3.21.1
xen-debugsource-4.9.1_02-3.21.1
xen-tools-debuginfo-4.9.1_02-3.21.1

146109 - SuSE Linux 42.3 openSUSE-SU-2017:3193-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15289, CVE-2017-15597

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3193-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00002.html

SuSE Linux 42.3
x86_64
xen-libs-4.9.1_02-13.2
xen-libs-debuginfo-4.9.1_02-13.2
xen-doc-html-4.9.1_02-13.2
xen-devel-4.9.1_02-13.2
xen-tools-domU-4.9.1_02-13.2
xen-tools-4.9.1_02-13.2
xen-debugsource-4.9.1_02-13.2
xen-4.9.1_02-13.2
xen-tools-debuginfo-4.9.1_02-13.2
xen-tools-domU-debuginfo-4.9.1_02-13.2

146111 - SuSE Linux 42.2 openSUSE-SU-2017:3194-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15289, CVE-2017-15597

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3194-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00003.html

SuSE Linux 42.2
x86_64
xen-tools-domU-4.7.4_02-11.21.1
xen-debugsource-4.7.4_02-11.21.1

xen-libs-debuginfo-4.7.4_02-11.21.1
xen-tools-domU-debuginfo-4.7.4_02-11.21.1
xen-doc-html-4.7.4_02-11.21.1
xen-4.7.4_02-11.21.1
xen-tools-4.7.4_02-11.21.1
xen-libs-32bit-4.7.4_02-11.21.1
xen-libs-4.7.4_02-11.21.1
xen-devel-4.7.4_02-11.21.1
xen-libs-debuginfo-32bit-4.7.4_02-11.21.1
xen-tools-debuginfo-4.7.4_02-11.21.1

i586
xen-tools-domU-4.7.4_02-11.21.1
xen-debugsource-4.7.4_02-11.21.1
xen-libs-debuginfo-4.7.4_02-11.21.1
xen-tools-domU-debuginfo-4.7.4_02-11.21.1
xen-libs-4.7.4_02-11.21.1
xen-devel-4.7.4_02-11.21.1

146136 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:3178-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15289, CVE-2017-15597

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3178-1

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-December/003466.html

SuSE SLED 12 SP2
x86_64
xen-libs-debuginfo-4.7.4_02-43.21.1
xen-4.7.4_02-43.21.1
xen-debugsource-4.7.4_02-43.21.1
xen-libs-32bit-4.7.4_02-43.21.1
xen-libs-4.7.4_02-43.21.1
xen-libs-debuginfo-32bit-4.7.4_02-43.21.1

SuSE SLES 12 SP2
x86_64
xen-tools-debuginfo-4.7.4_02-43.21.1
xen-libs-debuginfo-32bit-4.7.4_02-43.21.1
xen-4.7.4_02-43.21.1
xen-libs-4.7.4_02-43.21.1
xen-debugsource-4.7.4_02-43.21.1
xen-tools-domU-4.7.4_02-43.21.1
xen-tools-domU-debuginfo-4.7.4_02-43.21.1
xen-libs-debuginfo-4.7.4_02-43.21.1
xen-doc-html-4.7.4_02-43.21.1
xen-tools-4.7.4_02-43.21.1
xen-libs-32bit-4.7.4_02-43.21.1

22791 - (SYM17-013) Symantec Management Console Directory Traversal

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Symantec ITMS.

Observation

Symantec ITMS is a network-based computer management solution.

Multiple vulnerabilities are present in some versions of Symantec ITMS. The flaws lie in the Management Console. Successful exploitation by a remote attacker could allow the unauthorized access to the system.

22812 - Wireshark Multiple Vulnerabilities Prior To 2.2.11

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

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

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

141788 - Red Hat Enterprise Linux RHSA-2017-3194 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3167, CVE-2017-3169, CVE-2017-7668, CVE-2017-7679, CVE-2017-9788, CVE-2017-9798

Description

The scan detected that the host is missing the following update:
RHSA-2017-3194

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/msg00013.html

RHEL7_3S
noarch
httpd-manual-2.4.6-45.el7_3.5

x86_64
mod_session-2.4.6-45.el7_3.5

mod_ldap-2.4.6-45.el7_3.5
httpd-2.4.6-45.el7_3.5
httpd-tools-2.4.6-45.el7_3.5
httpd-devel-2.4.6-45.el7_3.5
mod_proxy_html-2.4.6-45.el7_3.5
mod_ssl-2.4.6-45.el7_3.5
httpd-debuginfo-2.4.6-45.el7_3.5

141789 - Red Hat Enterprise Linux RHSA-2017-3368 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14167, CVE-2017-15289

Description

The scan detected that the host is missing the following update:
RHSA-2017-3368

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/msg00047.html

RHEL7D
x86_64
qemu-img-1.5.3-141.el7_4.4
qemu-kvm-debuginfo-1.5.3-141.el7_4.4
qemu-kvm-tools-1.5.3-141.el7_4.4
qemu-kvm-1.5.3-141.el7_4.4
qemu-kvm-common-1.5.3-141.el7_4.4

RHEL7S
x86_64
qemu-img-1.5.3-141.el7_4.4
qemu-kvm-debuginfo-1.5.3-141.el7_4.4
qemu-kvm-tools-1.5.3-141.el7_4.4
qemu-kvm-1.5.3-141.el7_4.4
qemu-kvm-common-1.5.3-141.el7_4.4

RHEL7WS
x86_64
qemu-img-1.5.3-141.el7_4.4
qemu-kvm-debuginfo-1.5.3-141.el7_4.4
qemu-kvm-tools-1.5.3-141.el7_4.4
qemu-kvm-1.5.3-141.el7_4.4
qemu-kvm-common-1.5.3-141.el7_4.4

141794 - Red Hat Enterprise Linux RHSA-2017-3278 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

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

RHSA-2017-3278

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/msg00040.html

RHEL6D
x86_64
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-debuginfo-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

i386
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-debuginfo-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

RHEL6S
i386
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-debuginfo-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

x86_64
samba4-pidl-4.2.10-12.el6_9

samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-debuginfo-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

RHEL6WS
x86_64
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-debuginfo-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

i386
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-debuginfo-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

141795 - Red Hat Enterprise Linux RHSA-2017-3372 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
RHSA-2017-3372

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00000.html

RHEL7S
x86_64
thunderbird-52.5.0-1.el7_4
thunderbird-debuginfo-52.5.0-1.el7_4

RHEL6S
i386
thunderbird-52.5.0-1.el6_9
thunderbird-debuginfo-52.5.0-1.el6_9

x86_64
thunderbird-52.5.0-1.el6_9
thunderbird-debuginfo-52.5.0-1.el6_9

RHEL6WS
x86_64
thunderbird-52.5.0-1.el6_9
thunderbird-debuginfo-52.5.0-1.el6_9

i386
thunderbird-52.5.0-1.el6_9
thunderbird-debuginfo-52.5.0-1.el6_9

RHEL7D
x86_64
thunderbird-52.5.0-1.el7_4
thunderbird-debuginfo-52.5.0-1.el7_4

RHEL6D
x86_64
thunderbird-52.5.0-1.el6_9
thunderbird-debuginfo-52.5.0-1.el6_9

i386
thunderbird-52.5.0-1.el6_9
thunderbird-debuginfo-52.5.0-1.el6_9

RHEL7WS
x86_64
thunderbird-52.5.0-1.el7_4
thunderbird-debuginfo-52.5.0-1.el7_4

141796 - Red Hat Enterprise Linux RHSA-2017-3382 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7843

Description

The scan detected that the host is missing the following update:
RHSA-2017-3382

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00004.html

RHEL7S
x86_64
firefox-debuginfo-52.5.1-1.el7_4
firefox-52.5.1-1.el7_4

RHEL6S
i386
firefox-debuginfo-52.5.1-1.el6_9
firefox-52.5.1-1.el6_9

x86_64
firefox-debuginfo-52.5.1-1.el6_9
firefox-52.5.1-1.el6_9

RHEL6WS
x86_64
firefox-debuginfo-52.5.1-1.el6_9
firefox-52.5.1-1.el6_9

i386
firefox-debuginfo-52.5.1-1.el6_9
firefox-52.5.1-1.el6_9

RHEL7D
x86_64
firefox-debuginfo-52.5.1-1.el7_4
firefox-52.5.1-1.el7_4

RHEL6D
x86_64
firefox-debuginfo-52.5.1-1.el6_9
firefox-52.5.1-1.el6_9

i386
firefox-debuginfo-52.5.1-1.el6_9
firefox-52.5.1-1.el6_9

RHEL7WS
x86_64
firefox-debuginfo-52.5.1-1.el7_4
firefox-52.5.1-1.el7_4

146110 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3170-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9939, CVE-2017-12448, CVE-2017-12450, CVE-2017-12452, CVE-2017-12453, CVE-2017-12454, CVE-2017-12456, CVE-2017-12799, CVE-2017-13757, CVE-2017-14128, CVE-2017-14129, CVE-2017-14130, CVE-2017-14333, CVE-2017-14529, CVE-2017-14729, CVE-2017-14745, CVE-2017-14974, CVE-2017-6965, CVE-2017-6966, CVE-2017-6969, CVE-2017-7209, CVE-2017-7210, CVE-2017-7223, CVE-2017-7224, CVE-2017-7225, CVE-2017-7226, CVE-2017-7227, CVE-2017-7299, CVE-2017-7300, CVE-2017-7301, CVE-2017-7302, CVE-2017-7303, CVE-2017-7304, CVE-2017-7614, CVE-2017-8392, CVE-2017-8393, CVE-2017-8394, CVE-2017-8395, CVE-2017-8396, CVE-2017-8397, CVE-2017-8398, CVE-2017-8421, CVE-2017-9038, CVE-2017-9039, CVE-2017-9040, CVE-2017-9041, CVE-2017-9042, CVE-2017-9043, CVE-2017-9044, CVE-2017-9746, CVE-2017-9747, CVE-2017-9748, CVE-2017-9750, CVE-2017-9755, CVE-2017-9756, CVE-2017-9954, CVE-2017-9955

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3170-1

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/003462.html

SuSE SLES 12 SP2
x86_64
binutils-debuginfo-2.29.1-9.20.2
binutils-2.29.1-9.20.2
binutils-debugsource-2.29.1-9.20.2

SuSE SLED 12 SP3
x86_64
binutils-debuginfo-2.29.1-9.20.2
binutils-2.29.1-9.20.2
binutils-debugsource-2.29.1-9.20.2

SuSE SLED 12 SP2
x86_64
binutils-debuginfo-2.29.1-9.20.2
binutils-2.29.1-9.20.2
binutils-debugsource-2.29.1-9.20.2

SuSE SLES 12 SP3
x86_64
binutils-debuginfo-2.29.1-9.20.2
binutils-2.29.1-9.20.2
binutils-debugsource-2.29.1-9.20.2

146114 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3218-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15090, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3218-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00021.html

SuSE Linux 42.2
x86_64
pdns-recursor-debugsource-3.7.3-9.3.1
pdns-recursor-debuginfo-3.7.3-9.3.1
pdns-recursor-3.7.3-9.3.1

i586

pdns-recursor-debugsource-3.7.3-9.3.1
pdns-recursor-debuginfo-3.7.3-9.3.1
pdns-recursor-3.7.3-9.3.1

SuSE Linux 42.3
x86_64
pdns-recursor-4.0.5-3.1
pdns-recursor-debuginfo-4.0.5-3.1
pdns-recursor-debugsource-4.0.5-3.1

146116 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3203-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8819, CVE-2017-8820, CVE-2017-8821, CVE-2017-8822, CVE-2017-8823

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3203-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00012.html

SuSE Linux 42.2
x86_64
tor-debugsource-0.2.9.14-8.12.1
tor-debuginfo-0.2.9.14-8.12.1
tor-0.2.9.14-8.12.1

i586
tor-debugsource-0.2.9.14-8.12.1
tor-debuginfo-0.2.9.14-8.12.1
tor-0.2.9.14-8.12.1

SuSE Linux 42.3
x86_64
tor-0.3.0.13-9.1
tor-debuginfo-0.3.0.13-9.1
tor-debugsource-0.3.0.13-9.1

i586
tor-0.3.0.13-9.1
tor-debuginfo-0.3.0.13-9.1
tor-debugsource-0.3.0.13-9.1

146117 - SuSE SLES 11 SP4 SUSE-SU-2017:3168-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11534, CVE-2017-13133, CVE-2017-13139, CVE-2017-15033

Description

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

SUSE-SU-2017:3168-1

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/003460.html

SuSE SLES 11 SP4
i586
libMagickCore1-6.4.3.6-7.78.8.1

x86_64
libMagickCore1-6.4.3.6-7.78.8.1
libMagickCore1-32bit-6.4.3.6-7.78.8.1

146120 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3199-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9939, CVE-2017-12448, CVE-2017-12450, CVE-2017-12452, CVE-2017-12453, CVE-2017-12454, CVE-2017-12456, CVE-2017-12799, CVE-2017-13757, CVE-2017-14128, CVE-2017-14129, CVE-2017-14130, CVE-2017-14333, CVE-2017-14529, CVE-2017-14729, CVE-2017-14745, CVE-2017-14974, CVE-2017-6965, CVE-2017-6966, CVE-2017-6969, CVE-2017-7209, CVE-2017-7210, CVE-2017-7223, CVE-2017-7224, CVE-2017-7225, CVE-2017-7226, CVE-2017-7227, CVE-2017-7299, CVE-2017-7300, CVE-2017-7301, CVE-2017-7302, CVE-2017-7303, CVE-2017-7304, CVE-2017-7614, CVE-2017-8392, CVE-2017-8393, CVE-2017-8394, CVE-2017-8395, CVE-2017-8396, CVE-2017-8397, CVE-2017-8398, CVE-2017-8421, CVE-2017-9038, CVE-2017-9039, CVE-2017-9040, CVE-2017-9041, CVE-2017-9042, CVE-2017-9043, CVE-2017-9044, CVE-2017-9746, CVE-2017-9747, CVE-2017-9748, CVE-2017-9750, CVE-2017-9755, CVE-2017-9756, CVE-2017-9954, CVE-2017-9955

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3199-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00008.html

SuSE Linux 42.2
x86_64
cross-s390x-binutils-debuginfo-2.29.1-9.6.1
cross-mips-binutils-2.29.1-9.6.1
cross-ia64-binutils-debuginfo-2.29.1-9.6.1
cross-avr-binutils-debugsource-2.29.1-9.6.1
cross-sparc-binutils-debuginfo-2.29.1-9.6.1
cross-arm-binutils-2.29.1-9.6.1
cross-ppc64le-binutils-2.29.1-9.6.1
cross-avr-binutils-debuginfo-2.29.1-9.6.1
cross-hppa64-binutils-2.29.1-9.6.1
cross-s390x-binutils-debugsource-2.29.1-9.6.1
cross-ia64-binutils-2.29.1-9.6.1
cross-mips-binutils-debuginfo-2.29.1-9.6.1
cross-sparc-binutils-debugsource-2.29.1-9.6.1
cross-hppa-binutils-debuginfo-2.29.1-9.6.1
binutils-2.29.1-9.6.1
cross-ppc-binutils-debugsource-2.29.1-9.6.1

cross-ppc-binutils-debuginfo-2.29.1-9.6.1
cross-ia64-binutils-debugsource-2.29.1-9.6.1
cross-sparc-binutils-2.29.1-9.6.1
cross-ppc-binutils-2.29.1-9.6.1
cross-ppc64le-binutils-debugsource-2.29.1-9.6.1
cross-i386-binutils-debugsource-2.29.1-9.6.1
cross-arm-binutils-debugsource-2.29.1-9.6.1
cross-aarch64-binutils-debuginfo-2.29.1-9.6.1
cross-ppc64-binutils-debuginfo-2.29.1-9.6.1
binutils-devel-32bit-2.29.1-9.6.1
binutils-debuginfo-2.29.1-9.6.1
cross-sparc64-binutils-debugsource-2.29.1-9.6.1
cross-hppa-binutils-debugsource-2.29.1-9.6.1
cross-m68k-binutils-2.29.1-9.6.1
binutils-gold-2.29.1-9.6.1
cross-hppa64-binutils-debugsource-2.29.1-9.6.1
cross-spu-binutils-debuginfo-2.29.1-9.6.1
binutils-gold-debuginfo-2.29.1-9.6.1
cross-m68k-binutils-debugsource-2.29.1-9.6.1
cross-i386-binutils-debuginfo-2.29.1-9.6.1
cross-aarch64-binutils-2.29.1-9.6.1
cross-avr-binutils-2.29.1-9.6.1
cross-aarch64-binutils-debugsource-2.29.1-9.6.1
cross-ppc64le-binutils-debuginfo-2.29.1-9.6.1
cross-mips-binutils-debugsource-2.29.1-9.6.1
binutils-devel-2.29.1-9.6.1
cross-spu-binutils-debugsource-2.29.1-9.6.1
cross-s390-binutils-debuginfo-2.29.1-9.6.1
cross-s390-binutils-2.29.1-9.6.1
cross-hppa64-binutils-debuginfo-2.29.1-9.6.1
cross-spu-binutils-2.29.1-9.6.1
cross-i386-binutils-2.29.1-9.6.1
cross-ppc64-binutils-debugsource-2.29.1-9.6.1
cross-sparc64-binutils-debuginfo-2.29.1-9.6.1
binutils-debugsource-2.29.1-9.6.1
cross-arm-binutils-debuginfo-2.29.1-9.6.1
cross-hppa-binutils-2.29.1-9.6.1
cross-s390x-binutils-2.29.1-9.6.1
cross-m68k-binutils-debuginfo-2.29.1-9.6.1
cross-ppc64-binutils-2.29.1-9.6.1
cross-s390-binutils-debugsource-2.29.1-9.6.1
cross-sparc64-binutils-2.29.1-9.6.1

i586
cross-s390x-binutils-debuginfo-2.29.1-9.6.1
cross-mips-binutils-2.29.1-9.6.1
cross-ia64-binutils-debuginfo-2.29.1-9.6.1
cross-avr-binutils-debugsource-2.29.1-9.6.1
cross-sparc-binutils-debuginfo-2.29.1-9.6.1
cross-arm-binutils-2.29.1-9.6.1
cross-ppc64le-binutils-2.29.1-9.6.1
cross-avr-binutils-debuginfo-2.29.1-9.6.1
cross-hppa64-binutils-2.29.1-9.6.1
cross-x86_64-binutils-2.29.1-9.6.1
cross-s390x-binutils-debugsource-2.29.1-9.6.1
cross-ia64-binutils-2.29.1-9.6.1
cross-mips-binutils-debuginfo-2.29.1-9.6.1
cross-sparc-binutils-debugsource-2.29.1-9.6.1
cross-hppa-binutils-debuginfo-2.29.1-9.6.1
binutils-2.29.1-9.6.1

cross-ppc-binutils-debugsource-2.29.1-9.6.1
cross-ppc-binutils-debuginfo-2.29.1-9.6.1
cross-ia64-binutils-debugsource-2.29.1-9.6.1
cross-sparc-binutils-2.29.1-9.6.1
cross-x86_64-binutils-debugsource-2.29.1-9.6.1
cross-ppc-binutils-2.29.1-9.6.1
cross-ppc64le-binutils-debugsource-2.29.1-9.6.1
cross-arm-binutils-debugsource-2.29.1-9.6.1
cross-aarch64-binutils-debuginfo-2.29.1-9.6.1
cross-ppc64-binutils-debuginfo-2.29.1-9.6.1
binutils-debuginfo-2.29.1-9.6.1
cross-sparc64-binutils-debugsource-2.29.1-9.6.1
cross-hppa-binutils-debugsource-2.29.1-9.6.1
cross-m68k-binutils-2.29.1-9.6.1
binutils-gold-2.29.1-9.6.1
cross-x86_64-binutils-debuginfo-2.29.1-9.6.1
cross-hppa64-binutils-debugsource-2.29.1-9.6.1
cross-spu-binutils-debuginfo-2.29.1-9.6.1
binutils-gold-debuginfo-2.29.1-9.6.1
cross-m68k-binutils-debugsource-2.29.1-9.6.1
cross-aarch64-binutils-2.29.1-9.6.1
cross-avr-binutils-2.29.1-9.6.1
cross-aarch64-binutils-debugsource-2.29.1-9.6.1
cross-ppc64le-binutils-debuginfo-2.29.1-9.6.1
cross-mips-binutils-debugsource-2.29.1-9.6.1
binutils-devel-2.29.1-9.6.1
cross-spu-binutils-debugsource-2.29.1-9.6.1
cross-s390-binutils-debuginfo-2.29.1-9.6.1
cross-s390-binutils-2.29.1-9.6.1
cross-hppa64-binutils-debuginfo-2.29.1-9.6.1
cross-spu-binutils-2.29.1-9.6.1
cross-ppc64-binutils-debugsource-2.29.1-9.6.1
cross-sparc64-binutils-debuginfo-2.29.1-9.6.1
binutils-debugsource-2.29.1-9.6.1
cross-arm-binutils-debuginfo-2.29.1-9.6.1
cross-hppa-binutils-2.29.1-9.6.1
cross-s390x-binutils-2.29.1-9.6.1
cross-m68k-binutils-debuginfo-2.29.1-9.6.1
cross-ppc64-binutils-2.29.1-9.6.1
cross-s390-binutils-debugsource-2.29.1-9.6.1
cross-sparc64-binutils-2.29.1-9.6.1

SuSE Linux 42.3
x86_64
cross-hppa64-binutils-2.29.1-13.1
cross-ppc64le-binutils-2.29.1-13.1
cross-i386-binutils-debugsource-2.29.1-13.1
cross-ppc64-binutils-debuginfo-2.29.1-13.1
cross-spu-binutils-2.29.1-13.1
cross-avr-binutils-2.29.1-13.1
cross-m68k-binutils-2.29.1-13.1
binutils-debugsource-2.29.1-13.1
cross-i386-binutils-debuginfo-2.29.1-13.1
cross-hppa-binutils-2.29.1-13.1
cross-ppc64-binutils-debugsource-2.29.1-13.1
binutils-gold-debuginfo-2.29.1-13.1
cross-ppc64-binutils-2.29.1-13.1
cross-ppc64le-binutils-debugsource-2.29.1-13.1
cross-m68k-binutils-debugsource-2.29.1-13.1
cross-ppc-binutils-debuginfo-2.29.1-13.1

cross-sparc-binutils-2.29.1-13.1
cross-s390-binutils-debuginfo-2.29.1-13.1
cross-spu-binutils-debugsource-2.29.1-13.1
cross-sparc64-binutils-debuginfo-2.29.1-13.1
cross-hppa-binutils-debugsource-2.29.1-13.1
cross-ppc-binutils-debugsource-2.29.1-13.1
cross-s390x-binutils-debuginfo-2.29.1-13.1
binutils-debuginfo-2.29.1-13.1
cross-i386-binutils-2.29.1-13.1
cross-aarch64-binutils-debuginfo-2.29.1-13.1
binutils-devel-2.29.1-13.1
cross-arm-binutils-2.29.1-13.1
cross-arm-binutils-debugsource-2.29.1-13.1
cross-ppc-binutils-2.29.1-13.1
cross-m68k-binutils-debuginfo-2.29.1-13.1
cross-ia64-binutils-debuginfo-2.29.1-13.1
cross-hppa64-binutils-debugsource-2.29.1-13.1
cross-s390-binutils-debugsource-2.29.1-13.1
cross-sparc-binutils-debuginfo-2.29.1-13.1
cross-mips-binutils-2.29.1-13.1
cross-sparc-binutils-debugsource-2.29.1-13.1
cross-ppc64le-binutils-debuginfo-2.29.1-13.1
binutils-devel-32bit-2.29.1-13.1
cross-s390-binutils-2.29.1-13.1
cross-sparc64-binutils-debugsource-2.29.1-13.1
cross-s390x-binutils-2.29.1-13.1
binutils-2.29.1-13.1
cross-aarch64-binutils-2.29.1-13.1
cross-spu-binutils-debuginfo-2.29.1-13.1
cross-avr-binutils-debugsource-2.29.1-13.1
binutils-gold-2.29.1-13.1
cross-ia64-binutils-2.29.1-13.1
cross-arm-binutils-debuginfo-2.29.1-13.1
cross-mips-binutils-debugsource-2.29.1-13.1
cross-avr-binutils-debuginfo-2.29.1-13.1
cross-ia64-binutils-debugsource-2.29.1-13.1
cross-mips-binutils-debuginfo-2.29.1-13.1
cross-hppa-binutils-debuginfo-2.29.1-13.1
cross-aarch64-binutils-debugsource-2.29.1-13.1
cross-s390x-binutils-debugsource-2.29.1-13.1
cross-hppa64-binutils-debuginfo-2.29.1-13.1

146121 - SuSE SLES 11 SP4 SUSE-SU-2017:3165-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000253, CVE-2017-13080, CVE-2017-14489, CVE-2017-15265, CVE-2017-15274

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3165-1

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/003459.html

SuSE SLES 11 SP4
x86_64
kernel-syms-rt-3.0.101.rt130-69.11.1
kernel-rt_trace-base-3.0.101.rt130-69.11.1
kernel-rt-base-3.0.101.rt130-69.11.1
kernel-rt_trace-devel-3.0.101.rt130-69.11.1
kernel-rt_trace-3.0.101.rt130-69.11.1
kernel-source-rt-3.0.101.rt130-69.11.1
kernel-rt-3.0.101.rt130-69.11.1
kernel-rt-devel-3.0.101.rt130-69.11.1

146122 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:3155-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12150, CVE-2017-12151, CVE-2017-12163, CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3155-1

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/003453.html

SuSE SLED 12 SP3
x86_64
libnetapi0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libwbclient0-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbclient0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc-binding0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libnetapi0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbldap0-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbclient0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-winbind-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc-binding0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-errors0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-errors0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-hostconfig0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbclient0-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-standard0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbconf0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbldap0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-nbt0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr0-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-krb5pac0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-passdb0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-winbind-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-errors0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-hostconfig0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libnetapi0-4.6.9+git.59.c2cff9cea4c-3.17.1
libwbclient0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-util0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-krb5pac0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-libs-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-libs-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1

libsamba-credentials0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-krb5pac0-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libtevent-util0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-client-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-hostconfig0-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-util0-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-winbind-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-libs-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-krb5pac0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-nbt0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libtevent-util0-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-util0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-passdb0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc-binding0-4.6.9+git.59.c2cff9cea4c-3.17.1
libtevent-util0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-credentials0-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamdb0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-winbind-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbconf0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-nbt0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamdb0-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-credentials0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamdb0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbldap0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc0-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-client-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbclient0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-standard0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libwbclient0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc-binding0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-errors0-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-client-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamdb0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-standard0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-debugsource-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-credentials0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-passdb0-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-client-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libwbclient0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbldap0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbconf0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-standard0-4.6.9+git.59.c2cff9cea4c-3.17.1
libtevent-util0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-nbt0-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-libs-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libnetapi0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-util0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbconf0-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-hostconfig0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-passdb0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1

noarch

samba-doc-4.6.9+git.59.c2cff9cea4c-3.17.1

SuSE SLES 12 SP3
noarch
samba-doc-4.6.9+git.59.c2cff9cea4c-3.17.1

x86_64
libnetapi0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-passdb0-4.6.9+git.59.c2cff9cea4c-3.17.1
libwbclient0-4.6.9+git.59.c2cff9cea4c-3.17.1
libnetapi0-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc-binding0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libnetapi0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libwbclient0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbclient0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-winbind-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc-binding0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-errors0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-hostconfig0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbclient0-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-standard0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-passdb0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbldap0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-nbt0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr0-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-hostconfig0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-winbind-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-errors0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libwbclient0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsmbldap0-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-errors0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-libs-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-libs-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-credentials0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-krb5pac0-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr0-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libtevent-util0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-client-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-hostconfig0-4.6.9+git.59.c2cff9cea4c-3.17.1
libdcerpc0-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libsamba-util0-4.6.9+git.59.c2cff9cea4c-3.17.1
samba-libs-debuginfo-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-krb5pac0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1
libndr-nbt0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-3.17.1

146123 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3223-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11640, CVE-2017-13737, CVE-2017-14341, CVE-2017-14342, CVE-2017-16545, CVE-2017-16546, CVE-2017-16669

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3223-1

Observation

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

For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00026.html

SuSE Linux 42.2
x86_64
perl-GraphicsMagick-debuginfo-1.3.25-11.44.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.44.1
perl-GraphicsMagick-1.3.25-11.44.1
libGraphicsMagick++-Q16-12-1.3.25-11.44.1
libGraphicsMagickWand-Q16-2-1.3.25-11.44.1
libGraphicsMagick++-devel-1.3.25-11.44.1
GraphicsMagick-debugsource-1.3.25-11.44.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.44.1
GraphicsMagick-debuginfo-1.3.25-11.44.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.44.1
GraphicsMagick-devel-1.3.25-11.44.1
libGraphicsMagick3-config-1.3.25-11.44.1
libGraphicsMagick-Q16-3-1.3.25-11.44.1
GraphicsMagick-1.3.25-11.44.1

i586
perl-GraphicsMagick-debuginfo-1.3.25-11.44.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.44.1
perl-GraphicsMagick-1.3.25-11.44.1
libGraphicsMagick++-Q16-12-1.3.25-11.44.1
libGraphicsMagickWand-Q16-2-1.3.25-11.44.1
libGraphicsMagick++-devel-1.3.25-11.44.1
GraphicsMagick-debugsource-1.3.25-11.44.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.44.1
GraphicsMagick-debuginfo-1.3.25-11.44.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.44.1
GraphicsMagick-devel-1.3.25-11.44.1
libGraphicsMagick3-config-1.3.25-11.44.1
libGraphicsMagick-Q16-3-1.3.25-11.44.1
GraphicsMagick-1.3.25-11.44.1

SuSE Linux 42.3
x86_64
libGraphicsMagick-Q16-3-debuginfo-1.3.25-44.1
GraphicsMagick-debuginfo-1.3.25-44.1
libGraphicsMagickWand-Q16-2-1.3.25-44.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-44.1
GraphicsMagick-1.3.25-44.1
libGraphicsMagick++-devel-1.3.25-44.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-44.1
perl-GraphicsMagick-debuginfo-1.3.25-44.1
libGraphicsMagick-Q16-3-1.3.25-44.1
GraphicsMagick-devel-1.3.25-44.1
perl-GraphicsMagick-1.3.25-44.1
GraphicsMagick-debugsource-1.3.25-44.1
libGraphicsMagick++-Q16-12-1.3.25-44.1
libGraphicsMagick3-config-1.3.25-44.1

i586
libGraphicsMagick-Q16-3-debuginfo-1.3.25-44.1
GraphicsMagick-debuginfo-1.3.25-44.1
libGraphicsMagickWand-Q16-2-1.3.25-44.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-44.1
GraphicsMagick-1.3.25-44.1

libGraphicsMagick++-devel-1.3.25-44.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-44.1
perl-GraphicsMagick-debuginfo-1.3.25-44.1
libGraphicsMagick-Q16-3-1.3.25-44.1
GraphicsMagick-devel-1.3.25-44.1
perl-GraphicsMagick-1.3.25-44.1
GraphicsMagick-debugsource-1.3.25-44.1
libGraphicsMagick++-Q16-12-1.3.25-44.1
libGraphicsMagick3-config-1.3.25-44.1

146124 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3221-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15091

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3221-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00024.html

SuSE Linux 42.2
x86_64
pdns-backend-mydns-debuginfo-3.4.9-5.3.1
pdns-backend-postgresql-debuginfo-3.4.9-5.3.1
pdns-backend-mydns-3.4.9-5.3.1
pdns-backend-lua-3.4.9-5.3.1
pdns-debugsource-3.4.9-5.3.1
pdns-backend-ldap-3.4.9-5.3.1
pdns-debuginfo-3.4.9-5.3.1
pdns-backend-sqlite3-3.4.9-5.3.1
pdns-3.4.9-5.3.1
pdns-backend-postgresql-3.4.9-5.3.1
pdns-backend-ldap-debuginfo-3.4.9-5.3.1
pdns-backend-lua-debuginfo-3.4.9-5.3.1
pdns-backend-mysql-debuginfo-3.4.9-5.3.1
pdns-backend-mysql-3.4.9-5.3.1
pdns-backend-sqlite3-debuginfo-3.4.9-5.3.1

SuSE Linux 42.3
x86_64
pdns-backend-sqlite3-4.0.3-9.1
pdns-backend-mysql-debuginfo-4.0.3-9.1
pdns-backend-postgresql-debuginfo-4.0.3-9.1
pdns-backend-geoip-4.0.3-9.1
pdns-backend-godbc-debuginfo-4.0.3-9.1
pdns-backend-ldap-debuginfo-4.0.3-9.1
pdns-backend-sqlite3-debuginfo-4.0.3-9.1
pdns-backend-mydns-4.0.3-9.1
pdns-backend-lua-debuginfo-4.0.3-9.1
pdns-backend-lua-4.0.3-9.1
pdns-backend-remote-debuginfo-4.0.3-9.1
pdns-4.0.3-9.1

pdns-debugsource-4.0.3-9.1
pdns-debuginfo-4.0.3-9.1
pdns-backend-mydns-debuginfo-4.0.3-9.1
pdns-backend-mysql-4.0.3-9.1
pdns-backend-ldap-4.0.3-9.1
pdns-backend-remote-4.0.3-9.1
pdns-backend-postgresql-4.0.3-9.1
pdns-backend-godbc-4.0.3-9.1
pdns-backend-geoip-debuginfo-4.0.3-9.1

146125 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3222-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9157

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3222-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00025.html

SuSE Linux 42.2
x86_64
graphviz-python-2.38.0-4.5.3
graphviz-gnome-debuginfo-2.38.0-4.5.3
graphviz-debuginfo-2.38.0-4.5.1
graphviz-gd-2.38.0-4.5.3
graphviz-ruby-debuginfo-2.38.0-4.5.3
graphviz-php-2.38.0-4.5.3
graphviz-gd-debuginfo-2.38.0-4.5.3
graphviz-gvedit-debugsource-2.38.0-4.5.1
graphviz-perl-debuginfo-2.38.0-4.5.3
graphviz-tcl-debuginfo-2.38.0-4.5.3
graphviz-guile-debuginfo-2.38.0-4.5.3
graphviz-python-debuginfo-2.38.0-4.5.3
graphviz-java-2.38.0-4.5.3
graphviz-doc-2.38.0-4.5.3
graphviz-smyrna-debuginfo-2.38.0-4.5.1
graphviz-ruby-2.38.0-4.5.3
graphviz-gvedit-debuginfo-2.38.0-4.5.1
graphviz-smyrna-2.38.0-4.5.1
graphviz-java-debuginfo-2.38.0-4.5.3
graphviz-tcl-2.38.0-4.5.3
graphviz-lua-debuginfo-2.38.0-4.5.3
graphviz-php-debuginfo-2.38.0-4.5.3
graphviz-gvedit-2.38.0-4.5.1
graphviz-plugins-debugsource-2.38.0-4.5.3
graphviz-lua-2.38.0-4.5.3
graphviz-gnome-2.38.0-4.5.3
graphviz-devel-2.38.0-4.5.1
graphviz-perl-2.38.0-4.5.3
graphviz-debugsource-2.38.0-4.5.1
graphviz-smyrna-debugsource-2.38.0-4.5.1

graphviz-2.38.0-4.5.1
graphviz-guile-2.38.0-4.5.3

i586
graphviz-python-2.38.0-4.5.3
graphviz-gnome-debuginfo-2.38.0-4.5.3
graphviz-debuginfo-2.38.0-4.5.1
graphviz-gd-2.38.0-4.5.3
graphviz-ruby-debuginfo-2.38.0-4.5.3
graphviz-php-2.38.0-4.5.3
graphviz-gd-debuginfo-2.38.0-4.5.3
graphviz-gvedit-debugsource-2.38.0-4.5.1
graphviz-perl-debuginfo-2.38.0-4.5.3
graphviz-tcl-debuginfo-2.38.0-4.5.3
graphviz-guile-debuginfo-2.38.0-4.5.3
graphviz-python-debuginfo-2.38.0-4.5.3
graphviz-java-2.38.0-4.5.3
graphviz-doc-2.38.0-4.5.3
graphviz-ruby-2.38.0-4.5.3
graphviz-gvedit-debuginfo-2.38.0-4.5.1
graphviz-java-debuginfo-2.38.0-4.5.3
graphviz-tcl-2.38.0-4.5.3
graphviz-lua-debuginfo-2.38.0-4.5.3
graphviz-php-debuginfo-2.38.0-4.5.3
graphviz-gvedit-2.38.0-4.5.1
graphviz-plugins-debugsource-2.38.0-4.5.3
graphviz-lua-2.38.0-4.5.3
graphviz-gnome-2.38.0-4.5.3
graphviz-devel-2.38.0-4.5.1
graphviz-perl-2.38.0-4.5.3
graphviz-debugsource-2.38.0-4.5.1
graphviz-2.38.0-4.5.1
graphviz-guile-2.38.0-4.5.3

SuSE Linux 42.3
x86_64
graphviz-php-2.38.0-9.3
graphviz-debuginfo-2.38.0-9.1
graphviz-tcl-2.38.0-9.3
graphviz-smyrna-debuginfo-2.38.0-9.1
graphviz-gd-2.38.0-9.3
graphviz-gnome-debuginfo-2.38.0-9.3
graphviz-ruby-debuginfo-2.38.0-9.3
graphviz-perl-2.38.0-9.3
graphviz-guile-debuginfo-2.38.0-9.3
graphviz-debugsource-2.38.0-9.1
graphviz-gnome-2.38.0-9.3
graphviz-smyrna-2.38.0-9.1
graphviz-php-debuginfo-2.38.0-9.3
graphviz-gvedit-debuginfo-2.38.0-9.1
graphviz-java-2.38.0-9.3
graphviz-lua-2.38.0-9.3
graphviz-python-debuginfo-2.38.0-9.3
graphviz-ruby-2.38.0-9.3
graphviz-doc-2.38.0-9.3
graphviz-perl-debuginfo-2.38.0-9.3
graphviz-gd-debuginfo-2.38.0-9.3
graphviz-tcl-debuginfo-2.38.0-9.3
graphviz-gvedit-2.38.0-9.1
graphviz-2.38.0-9.1

graphviz-plugins-debugsource-2.38.0-9.3
graphviz-smyrna-debugsource-2.38.0-9.1
graphviz-guile-2.38.0-9.3
graphviz-java-debuginfo-2.38.0-9.3
graphviz-lua-debuginfo-2.38.0-9.3
graphviz-python-2.38.0-9.3
graphviz-devel-2.38.0-9.1
graphviz-gvedit-debugsource-2.38.0-9.1

i586
graphviz-php-2.38.0-9.3
graphviz-debuginfo-2.38.0-9.1
graphviz-tcl-2.38.0-9.3
graphviz-gd-2.38.0-9.3
graphviz-gnome-debuginfo-2.38.0-9.3
graphviz-ruby-debuginfo-2.38.0-9.3
graphviz-perl-2.38.0-9.3
graphviz-guile-debuginfo-2.38.0-9.3
graphviz-debugsource-2.38.0-9.1
graphviz-gnome-2.38.0-9.3
graphviz-php-debuginfo-2.38.0-9.3
graphviz-gvedit-debuginfo-2.38.0-9.1
graphviz-java-2.38.0-9.3
graphviz-lua-2.38.0-9.3
graphviz-python-debuginfo-2.38.0-9.3
graphviz-ruby-2.38.0-9.3
graphviz-doc-2.38.0-9.3
graphviz-perl-debuginfo-2.38.0-9.3
graphviz-gd-debuginfo-2.38.0-9.3
graphviz-tcl-debuginfo-2.38.0-9.3
graphviz-gvedit-2.38.0-9.1
graphviz-2.38.0-9.1
graphviz-plugins-debugsource-2.38.0-9.3
graphviz-guile-2.38.0-9.3
graphviz-java-debuginfo-2.38.0-9.3
graphviz-lua-debuginfo-2.38.0-9.3
graphviz-python-2.38.0-9.3
graphviz-devel-2.38.0-9.1
graphviz-gvedit-debugsource-2.38.0-9.1

146126 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3213-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3213-1

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-December/003471.html

SuSE SLES 12 SP2
x86_64

MozillaFirefox-debugsource-52.5.0esr-109.9.1
MozillaFirefox-debuginfo-52.5.0esr-109.9.1
MozillaFirefox-translations-52.5.0esr-109.9.1
MozillaFirefox-52.5.0esr-109.9.1

SuSE SLED 12 SP3
x86_64
MozillaFirefox-debugsource-52.5.0esr-109.9.1
MozillaFirefox-debuginfo-52.5.0esr-109.9.1
MozillaFirefox-translations-52.5.0esr-109.9.1
MozillaFirefox-52.5.0esr-109.9.1

SuSE SLED 12 SP2
x86_64
MozillaFirefox-debugsource-52.5.0esr-109.9.1
MozillaFirefox-debuginfo-52.5.0esr-109.9.1
MozillaFirefox-translations-52.5.0esr-109.9.1
MozillaFirefox-52.5.0esr-109.9.1

SuSE SLES 12 SP3
x86_64
MozillaFirefox-debugsource-52.5.0esr-109.9.1
MozillaFirefox-debuginfo-52.5.0esr-109.9.1
MozillaFirefox-translations-52.5.0esr-109.9.1
MozillaFirefox-52.5.0esr-109.9.1

146128 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3214-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16612

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3214-1

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-December/003472.html

SuSE SLES 12 SP2
x86_64
libXcursor-debugsource-1.1.14-4.3.1
libXcursor1-debuginfo-1.1.14-4.3.1
libXcursor1-debuginfo-32bit-1.1.14-4.3.1
libXcursor1-32bit-1.1.14-4.3.1
libXcursor1-1.1.14-4.3.1

SuSE SLED 12 SP3
x86_64
libXcursor-debugsource-1.1.14-4.3.1
libXcursor1-debuginfo-1.1.14-4.3.1
libXcursor1-debuginfo-32bit-1.1.14-4.3.1
libXcursor1-32bit-1.1.14-4.3.1
libXcursor1-1.1.14-4.3.1

SuSE SLED 12 SP2
x86_64
libXcursor-debugsource-1.1.14-4.3.1
libXcursor1-debuginfo-1.1.14-4.3.1
libXcursor1-debuginfo-32bit-1.1.14-4.3.1
libXcursor1-32bit-1.1.14-4.3.1
libXcursor1-1.1.14-4.3.1

SuSE SLES 12 SP3
x86_64
libXcursor-debugsource-1.1.14-4.3.1
libXcursor1-debuginfo-1.1.14-4.3.1
libXcursor1-debuginfo-32bit-1.1.14-4.3.1
libXcursor1-32bit-1.1.14-4.3.1
libXcursor1-1.1.14-4.3.1

146129 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3220-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16943

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3220-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00023.html

SuSE Linux 42.2
x86_64
exim-debugsource-4.86.2-10.9.1
eximstats-html-4.86.2-10.9.1
eximon-4.86.2-10.9.1
exim-4.86.2-10.9.1
exim-debuginfo-4.86.2-10.9.1
eximon-debuginfo-4.86.2-10.9.1

SuSE Linux 42.3
x86_64
eximon-debuginfo-4.86.2-17.1
exim-4.86.2-17.1
exim-debuginfo-4.86.2-17.1
eximon-4.86.2-17.1
eximstats-html-4.86.2-17.1
exim-debugsource-4.86.2-17.1

146130 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3215-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16852

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3215-1

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-December/003473.html

SuSE SLES 12 SP3
x86_64
libshibsp6-debuginfo-2.5.5-6.3.1
libshibsp6-2.5.5-6.3.1
libshibsp-lite6-2.5.5-6.3.1
shibboleth-sp-2.5.5-6.3.1
shibboleth-sp-debuginfo-2.5.5-6.3.1
libshibsp-lite6-debuginfo-2.5.5-6.3.1
shibboleth-sp-debugsource-2.5.5-6.3.1

SuSE SLES 12 SP2
x86_64
libshibsp6-debuginfo-2.5.5-6.3.1
libshibsp6-2.5.5-6.3.1
libshibsp-lite6-2.5.5-6.3.1
shibboleth-sp-2.5.5-6.3.1
shibboleth-sp-debuginfo-2.5.5-6.3.1
libshibsp-lite6-debuginfo-2.5.5-6.3.1
shibboleth-sp-debugsource-2.5.5-6.3.1

146131 - SuSE Linux 42.2 openSUSE-SU-2017:3141-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3141-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-11/msg00093.html

SuSE Linux 42.2
i586
libndr-standard0-4.4.2-11.15.1
samba-core-devel-4.4.2-11.15.1
libsmbldap0-debuginfo-4.4.2-11.15.1
samba-client-4.4.2-11.15.1
libsamba-passdb-devel-4.4.2-11.15.1
libndr0-4.4.2-11.15.1
libtevent-util-devel-4.4.2-11.15.1
libndr-standard0-debuginfo-4.4.2-11.15.1
libsmbldap0-4.4.2-11.15.1
ctdb-debuginfo-4.4.2-11.15.1

libsamdb-devel-4.4.2-11.15.1
libwbclient0-debuginfo-4.4.2-11.15.1
libsmbconf-devel-4.4.2-11.15.1
libsamba-hostconfig0-debuginfo-4.4.2-11.15.1
libsmbconf0-4.4.2-11.15.1
samba-winbind-4.4.2-11.15.1
libndr-nbt0-debuginfo-4.4.2-11.15.1
libsamba-credentials0-4.4.2-11.15.1
libsamba-credentials0-debuginfo-4.4.2-11.15.1
libdcerpc0-debuginfo-4.4.2-11.15.1
libdcerpc-binding0-4.4.2-11.15.1
libsamba-util0-debuginfo-4.4.2-11.15.1
libndr-nbt0-4.4.2-11.15.1
libnetapi0-4.4.2-11.15.1
samba-4.4.2-11.15.1
libsamba-credentials-devel-4.4.2-11.15.1
samba-debugsource-4.4.2-11.15.1
libndr-krb5pac0-debuginfo-4.4.2-11.15.1
samba-libs-4.4.2-11.15.1
libdcerpc-devel-4.4.2-11.15.1
libsamba-hostconfig0-4.4.2-11.15.1
samba-debuginfo-4.4.2-11.15.1
samba-pidl-4.4.2-11.15.1
libndr-krb5pac-devel-4.4.2-11.15.1
libsmbclient0-debuginfo-4.4.2-11.15.1
samba-test-4.4.2-11.15.1
libsmbclient0-4.4.2-11.15.1
libsamdb0-debuginfo-4.4.2-11.15.1
libndr-devel-4.4.2-11.15.1
libnetapi0-debuginfo-4.4.2-11.15.1
libsamba-policy0-debuginfo-4.4.2-11.15.1
libsmbconf0-debuginfo-4.4.2-11.15.1
libsamba-policy0-4.4.2-11.15.1
libsamba-passdb0-debuginfo-4.4.2-11.15.1
libndr-krb5pac0-4.4.2-11.15.1
libsamba-hostconfig-devel-4.4.2-11.15.1
ctdb-tests-debuginfo-4.4.2-11.15.1
samba-winbind-debuginfo-4.4.2-11.15.1
libdcerpc-binding0-debuginfo-4.4.2-11.15.1
libwbclient-devel-4.4.2-11.15.1
libdcerpc-samr0-4.4.2-11.15.1
libndr-standard-devel-4.4.2-11.15.1
libdcerpc-samr-devel-4.4.2-11.15.1
libsamba-util-devel-4.4.2-11.15.1
libsamba-util0-4.4.2-11.15.1
ctdb-tests-4.4.2-11.15.1
libwbclient0-4.4.2-11.15.1
samba-libs-debuginfo-4.4.2-11.15.1
samba-python-debuginfo-4.4.2-11.15.1
libdcerpc0-4.4.2-11.15.1
libsamba-errors0-4.4.2-11.15.1
samba-test-debuginfo-4.4.2-11.15.1
libtevent-util0-4.4.2-11.15.1
libndr0-debuginfo-4.4.2-11.15.1
libsamdb0-4.4.2-11.15.1
libsmbldap-devel-4.4.2-11.15.1
libnetapi-devel-4.4.2-11.15.1
libsamba-passdb0-4.4.2-11.15.1
libsamba-errors0-debuginfo-4.4.2-11.15.1
libsmbclient-devel-4.4.2-11.15.1

libtevent-util0-debuginfo-4.4.2-11.15.1
libsamba-errors-devel-4.4.2-11.15.1
samba-python-4.4.2-11.15.1
samba-client-debuginfo-4.4.2-11.15.1
ctdb-4.4.2-11.15.1
libdcerpc-samr0-debuginfo-4.4.2-11.15.1
libndr-nbt-devel-4.4.2-11.15.1
libsamba-policy-devel-4.4.2-11.15.1

noarch
samba-doc-4.4.2-11.15.1

x86_64
libndr-standard0-4.4.2-11.15.1
samba-core-devel-4.4.2-11.15.1
libsmbldap0-debuginfo-4.4.2-11.15.1
libwbclient0-32bit-4.4.2-11.15.1
libsamba-policy0-32bit-4.4.2-11.15.1
samba-client-4.4.2-11.15.1
libsamba-passdb-devel-4.4.2-11.15.1
libndr0-4.4.2-11.15.1
libtevent-util-devel-4.4.2-11.15.1
libdcerpc-samr0-debuginfo-32bit-4.4.2-11.15.1
libndr-standard0-debuginfo-4.4.2-11.15.1
libtevent-util0-32bit-4.4.2-11.15.1
libsmbldap0-4.4.2-11.15.1
libdcerpc-samr0-32bit-4.4.2-11.15.1
ctdb-debuginfo-4.4.2-11.15.1
libsamdb-devel-4.4.2-11.15.1
libwbclient0-debuginfo-4.4.2-11.15.1
libsmbconf-devel-4.4.2-11.15.1
libsamba-util0-debuginfo-32bit-4.4.2-11.15.1
libsamba-hostconfig0-debuginfo-4.4.2-11.15.1
libsmbconf0-4.4.2-11.15.1
libndr-nbt0-32bit-4.4.2-11.15.1
samba-winbind-4.4.2-11.15.1
libsamba-util0-32bit-4.4.2-11.15.1
libndr-nbt0-debuginfo-4.4.2-11.15.1
libsamba-credentials0-4.4.2-11.15.1
libsamba-credentials0-debuginfo-4.4.2-11.15.1
libdcerpc0-debuginfo-4.4.2-11.15.1
libndr-standard0-32bit-4.4.2-11.15.1
libdcerpc-binding0-4.4.2-11.15.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-11.15.1
libsamba-util0-debuginfo-4.4.2-11.15.1
libndr-nbt0-4.4.2-11.15.1
libnetapi0-4.4.2-11.15.1
samba-4.4.2-11.15.1
libsamba-credentials-devel-4.4.2-11.15.1
samba-debugsource-4.4.2-11.15.1
libndr-krb5pac0-debuginfo-4.4.2-11.15.1
samba-libs-4.4.2-11.15.1
libsamba-errors0-32bit-4.4.2-11.15.1
libndr-standard0-debuginfo-32bit-4.4.2-11.15.1
libdcerpc-devel-4.4.2-11.15.1
libsamdb0-debuginfo-32bit-4.4.2-11.15.1
libsamba-hostconfig0-4.4.2-11.15.1
libsamdb0-32bit-4.4.2-11.15.1
libndr-krb5pac0-32bit-4.4.2-11.15.1
samba-debuginfo-4.4.2-11.15.1

libdcerpc0-32bit-4.4.2-11.15.1
samba-pidl-4.4.2-11.15.1
libndr-krb5pac-devel-4.4.2-11.15.1
libsmbclient0-debuginfo-4.4.2-11.15.1
samba-test-4.4.2-11.15.1
libsmbclient0-4.4.2-11.15.1
libsamdb0-debuginfo-4.4.2-11.15.1
libndr0-debuginfo-32bit-4.4.2-11.15.1
libndr-nbt0-debuginfo-32bit-4.4.2-11.15.1
libndr-devel-4.4.2-11.15.1
samba-client-debuginfo-32bit-4.4.2-11.15.1
libsamba-passdb0-32bit-4.4.2-11.15.1
libnetapi0-debuginfo-4.4.2-11.15.1
libsamba-policy0-debuginfo-4.4.2-11.15.1
libsmbconf0-debuginfo-4.4.2-11.15.1
libsamba-policy0-4.4.2-11.15.1
libsamba-passdb0-debuginfo-4.4.2-11.15.1
libsamba-credentials0-32bit-4.4.2-11.15.1
libndr-krb5pac0-4.4.2-11.15.1
libsmbclient0-32bit-4.4.2-11.15.1
libsamba-policy0-debuginfo-32bit-4.4.2-11.15.1
libsmbconf0-32bit-4.4.2-11.15.1
libsamba-hostconfig-devel-4.4.2-11.15.1
libsamba-passdb0-debuginfo-32bit-4.4.2-11.15.1
ctdb-tests-debuginfo-4.4.2-11.15.1
samba-winbind-debuginfo-32bit-4.4.2-11.15.1
samba-libs-32bit-4.4.2-11.15.1
libdcerpc0-debuginfo-32bit-4.4.2-11.15.1
samba-client-32bit-4.4.2-11.15.1
libsmbldap0-32bit-4.4.2-11.15.1
samba-libs-debuginfo-32bit-4.4.2-11.15.1
libndr-krb5pac0-debuginfo-32bit-4.4.2-11.15.1
samba-winbind-debuginfo-4.4.2-11.15.1
libwbclient0-debuginfo-32bit-4.4.2-11.15.1
libdcerpc-binding0-debuginfo-4.4.2-11.15.1
libtevent-util0-debuginfo-32bit-4.4.2-11.15.1
libsamba-hostconfig0-debuginfo-32bit-4.4.2-11.15.1
libwbclient-devel-4.4.2-11.15.1
libdcerpc-samr0-4.4.2-11.15.1
libndr-standard-devel-4.4.2-11.15.1
libdcerpc-samr-devel-4.4.2-11.15.1
libsamba-util-devel-4.4.2-11.15.1
libsamba-errors0-debuginfo-32bit-4.4.2-11.15.1
libsamba-util0-4.4.2-11.15.1
ctdb-tests-4.4.2-11.15.1
libndr0-32bit-4.4.2-11.15.1
libwbclient0-4.4.2-11.15.1
libsamba-hostconfig0-32bit-4.4.2-11.15.1
samba-libs-debuginfo-4.4.2-11.15.1
samba-python-debuginfo-4.4.2-11.15.1
libdcerpc0-4.4.2-11.15.1
libsamba-errors0-4.4.2-11.15.1
samba-test-debuginfo-4.4.2-11.15.1
libtevent-util0-4.4.2-11.15.1
libndr0-debuginfo-4.4.2-11.15.1
libsamdb0-4.4.2-11.15.1
libsmbldap-devel-4.4.2-11.15.1
libsmbconf0-debuginfo-32bit-4.4.2-11.15.1
libsamba-credentials0-debuginfo-32bit-4.4.2-11.15.1
libnetapi-devel-4.4.2-11.15.1

libsamba-passdb0-4.4.2-11.15.1
libsamba-errors0-debuginfo-4.4.2-11.15.1
libnetapi0-debuginfo-32bit-4.4.2-11.15.1
libsmbclient-devel-4.4.2-11.15.1
libtevent-util0-debuginfo-4.4.2-11.15.1
libdcerpc-binding0-32bit-4.4.2-11.15.1
libsamba-errors-devel-4.4.2-11.15.1
samba-python-4.4.2-11.15.1
libsmbldap0-debuginfo-32bit-4.4.2-11.15.1
samba-client-debuginfo-4.4.2-11.15.1
ctdb-4.4.2-11.15.1
libdcerpc-samr0-debuginfo-4.4.2-11.15.1

146133 - SuSE Linux 42.3 openSUSE-SU-2017:3143-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12150, CVE-2017-12151, CVE-2017-12163, CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3143-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-11/msg00095.html

SuSE Linux 42.3
i586
samba-libs-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-client-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-passdb0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-hostconfig0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libtevent-util0-4.6.9+git.59.c2cff9cea4c-9.1
libsmbclient-devel-4.6.9+git.59.c2cff9cea4c-9.1
samba-winbind-4.6.9+git.59.c2cff9cea4c-9.1
samba-winbind-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsmbconf0-4.6.9+git.59.c2cff9cea4c-9.1
libsmbclient0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-util0-4.6.9+git.59.c2cff9cea4c-9.1
ctdb-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-credentials-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-passdb-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-passdb0-4.6.9+git.59.c2cff9cea4c-9.1
samba-python-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-binding0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamdb0-4.6.9+git.59.c2cff9cea4c-9.1
libsmbldap0-4.6.9+git.59.c2cff9cea4c-9.1
libsmbldap-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-errors-devel-4.6.9+git.59.c2cff9cea4c-9.1
libndr-nbt0-4.6.9+git.59.c2cff9cea4c-9.1
libnetapi0-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-hostconfig0-4.6.9+git.59.c2cff9cea4c-9.1
ctdb-tests-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-util-devel-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc0-4.6.9+git.59.c2cff9cea4c-9.1

ctdb-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libndr-krb5pac0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-client-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-devel-4.6.9+git.59.c2cff9cea4c-9.1
libnetapi0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-debugsource-4.6.9+git.59.c2cff9cea4c-9.1
libsmbconf0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-python-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libndr-nbt0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsmbldap0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-libs-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-hostconfig-devel-4.6.9+git.59.c2cff9cea4c-9.1
samba-pidl-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-util0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libnetapi-devel-4.6.9+git.59.c2cff9cea4c-9.1
libtevent-util0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
ctdb-tests-4.6.9+git.59.c2cff9cea4c-9.1
samba-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-test-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-errors0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamdb0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-4.6.9+git.59.c2cff9cea4c-9.1
samba-core-devel-4.6.9+git.59.c2cff9cea4c-9.1
libndr-standard0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libwbclient-devel-4.6.9+git.59.c2cff9cea4c-9.1
libndr-standard-devel-4.6.9+git.59.c2cff9cea4c-9.1
libndr-standard0-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-policy0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libwbclient0-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-samr0-4.6.9+git.59.c2cff9cea4c-9.1
libtevent-util-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsamdb-devel-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-samr0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsmbconf-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-policy0-4.6.9+git.59.c2cff9cea4c-9.1
libndr-krb5pac0-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-binding0-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-policy-devel-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-samr-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsmbclient0-4.6.9+git.59.c2cff9cea4c-9.1
libndr0-4.6.9+git.59.c2cff9cea4c-9.1
libndr-devel-4.6.9+git.59.c2cff9cea4c-9.1
libndr-krb5pac-devel-4.6.9+git.59.c2cff9cea4c-9.1
samba-test-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-credentials0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libwbclient0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-credentials0-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-errors0-4.6.9+git.59.c2cff9cea4c-9.1
libndr0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libndr-nbt-devel-4.6.9+git.59.c2cff9cea4c-9.1

noarch
samba-doc-4.6.9+git.59.c2cff9cea4c-9.1

x86_64
samba-ceph-4.6.9+git.59.c2cff9cea4c-9.1
samba-libs-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-client-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libwbclient0-32bit-4.6.9+git.59.c2cff9cea4c-9.1

libdcerpc-binding0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-passdb0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-hostconfig0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-libs-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libtevent-util0-4.6.9+git.59.c2cff9cea4c-9.1
libsamdb0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsmbclient-devel-4.6.9+git.59.c2cff9cea4c-9.1
samba-winbind-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-errors0-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libtevent-util0-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsmbconf0-32bit-4.6.9+git.59.c2cff9cea4c-9.1
samba-winbind-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-util0-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsmbconf0-4.6.9+git.59.c2cff9cea4c-9.1
libsmbclient0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libwbclient0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-util0-4.6.9+git.59.c2cff9cea4c-9.1
ctdb-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-binding0-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-credentials-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-passdb-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-passdb0-4.6.9+git.59.c2cff9cea4c-9.1
samba-python-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-binding0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamdb0-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-policy0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-passdb0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsmbldap0-4.6.9+git.59.c2cff9cea4c-9.1
libtevent-util0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsmbclient0-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-credentials0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libsmbldap-devel-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-errors-devel-4.6.9+git.59.c2cff9cea4c-9.1
libndr-nbt0-4.6.9+git.59.c2cff9cea4c-9.1
samba-client-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libnetapi0-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-hostconfig0-4.6.9+git.59.c2cff9cea4c-9.1
libndr-standard0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libndr-standard0-32bit-4.6.9+git.59.c2cff9cea4c-9.1
ctdb-tests-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-util-devel-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc0-4.6.9+git.59.c2cff9cea4c-9.1
ctdb-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libndr-krb5pac0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-client-4.6.9+git.59.c2cff9cea4c-9.1
libndr0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc-devel-4.6.9+git.59.c2cff9cea4c-9.1
libnetapi0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-debugsource-4.6.9+git.59.c2cff9cea4c-9.1
libsmbconf0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-python-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsmbldap0-32bit-4.6.9+git.59.c2cff9cea4c-9.1
libndr-nbt0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsmbldap0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
samba-libs-4.6.9+git.59.c2cff9cea4c-9.1
libdcerpc0-debuginfo-4.6.9+git.59.c2cff9cea4c-9.1
libsamba-errors0-debuginfo-32bit-4.6.9+git.59.c2cff9cea4c-9.1

146137 - SuSE SLES 11 SP4 SUSE-SU-2017:3114-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-5118

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3114-1

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/003421.html

SuSE SLES 11 SP4
x86_64
tboot-20120115_1.7.0-0.5.5.1

i586
tboot-20120115_1.7.0-0.5.5.1

163503 - Oracle Enterprise Linux ELSA-2017-3372 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
ELSA-2017-3372

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-December/007391.html
http://oss.oracle.com/pipermail/el-errata/2017-December/007390.html

OEL7
x86_64
thunderbird-52.5.0-1.0.1.el7_4

OEL6
x86_64
thunderbird-52.5.0-1.0.1.el6_9

i386
thunderbird-52.5.0-1.0.1.el6_9

163504 - Oracle Enterprise Linux ELSA-2017-3382 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7843

Description

The scan detected that the host is missing the following update:
ELSA-2017-3382

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-December/007398.html
http://oss.oracle.com/pipermail/el-errata/2017-December/007397.html

OEL7
x86_64
firefox-52.5.1-1.0.1.el7_4

OEL6
x86_64
firefox-52.5.1-1.0.1.el6_9

i386
firefox-52.5.1-1.0.1.el6_9

163505 - Oracle Enterprise Linux ELSA-2017-3368 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14167, CVE-2017-15289

Description

The scan detected that the host is missing the following update:
ELSA-2017-3368

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/007362.html

OEL7
x86_64
qemu-img-1.5.3-141.el7_4.4
qemu-kvm-tools-1.5.3-141.el7_4.4
qemu-kvm-1.5.3-141.el7_4.4
qemu-kvm-common-1.5.3-141.el7_4.4

163506 - Oracle Enterprise Linux ELSA-2017-3278 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
ELSA-2017-3278

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/007360.html

OEL6
x86_64
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

i386
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

175291 - Scientific Linux Security ERRATA Important: samba4 on SL6.x i386/x86_64 (1711-7740)

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: samba4 on SL6.x i386/x86_64 (1711-7740)

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=7740

SL6
x86_64
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9

samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-debuginfo-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

i386
samba4-pidl-4.2.10-12.el6_9
samba4-dc-libs-4.2.10-12.el6_9
samba4-dc-4.2.10-12.el6_9
samba4-winbind-4.2.10-12.el6_9
samba4-libs-4.2.10-12.el6_9
samba4-debuginfo-4.2.10-12.el6_9
samba4-client-4.2.10-12.el6_9
samba4-devel-4.2.10-12.el6_9
samba4-winbind-krb5-locator-4.2.10-12.el6_9
samba4-winbind-clients-4.2.10-12.el6_9
samba4-4.2.10-12.el6_9
samba4-common-4.2.10-12.el6_9
samba4-test-4.2.10-12.el6_9
samba4-python-4.2.10-12.el6_9

175293 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86_64 (1712-758)

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

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86_64 (1712-758)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=758

SL7
x86_64
thunderbird-52.5.0-1.el7_4
thunderbird-debuginfo-52.5.0-1.el7_4

SL6
x86_64
thunderbird-52.5.0-1.el6_9
thunderbird-debuginfo-52.5.0-1.el6_9

i386
thunderbird-52.5.0-1.el6_9
thunderbird-debuginfo-52.5.0-1.el6_9

175294 - Scientific Linux Security ERRATA Important: firefox on SL6.x, SL7.x i386/x86_64 (1712-1795)

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

Risk Level: High

CVE: CVE-2017-7843

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: firefox on SL6.x, SL7.x i386/x86_64 (1712-1795)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=1795

SL7
x86_64
firefox-debuginfo-52.5.1-1.el7_4
firefox-52.5.1-1.el7_4

SL6
x86_64
firefox-debuginfo-52.5.1-1.el6_9
firefox-52.5.1-1.el6_9

i386
firefox-debuginfo-52.5.1-1.el6_9
firefox-52.5.1-1.el6_9

175296 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1712-415)

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

Risk Level: High

CVE: CVE-2017-14167, CVE-2017-15289

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1712-415)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=415

SL7
x86_64
qemu-img-1.5.3-141.el7_4.4
qemu-kvm-debuginfo-1.5.3-141.el7_4.4
qemu-kvm-tools-1.5.3-141.el7_4.4
qemu-kvm-1.5.3-141.el7_4.4
qemu-kvm-common-1.5.3-141.el7_4.4

193001 - Fedora Linux 25 FEDORA-2017-905bb449bc Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16644, CVE-2017-16647, CVE-2017-16649, CVE-2017-16650, CVE-2017-16994

Description

The scan detected that the host is missing the following update:
FEDORA-2017-905bb449bc

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/2017/12/?count=200&page=1

Fedora Core 25

kernel-4.13.16-100.fc25

193017 - Fedora Linux 26 FEDORA-2017-f9f3d80442 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16644, CVE-2017-16647, CVE-2017-16649, CVE-2017-16650, CVE-2017-16994

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f9f3d80442

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/2017/12/?count=200&page=1

Fedora Core 26

kernel-4.13.16-200.fc26

193020 - Fedora Linux 27 FEDORA-2017-92a0ae09aa Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16644, CVE-2017-16647, CVE-2017-16649, CVE-2017-16650, CVE-2017-16994

Description

The scan detected that the host is missing the following update:
FEDORA-2017-92a0ae09aa

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/2017/12/?count=200&page=1

Fedora Core 27

kernel-4.13.16-300.fc27

193021 - Fedora Linux 27 FEDORA-2017-195e7ea9a8 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-2017-195e7ea9a8

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 27

lucene4-4.10.4-11.fc27

193028 - Fedora Linux 25 FEDORA-2017-6be762ea64 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6be762ea64

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/2017/12/?count=200&page=1

Fedora Core 25

python-2.7.13-3.fc25

146132 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3162-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000229, CVE-2017-16938

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3162-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-11/msg00097.html

SuSE Linux 42.2
x86_64
optipng-debuginfo-0.7.5-9.5.1
optipng-0.7.5-9.5.1
optipng-debugsource-0.7.5-9.5.1

i586
optipng-debuginfo-0.7.5-9.5.1
optipng-0.7.5-9.5.1
optipng-debugsource-0.7.5-9.5.1

SuSE Linux 42.3
x86_64
optipng-debugsource-0.7.5-14.1
optipng-debuginfo-0.7.5-14.1
optipng-0.7.5-14.1

i586
optipng-debugsource-0.7.5-14.1
optipng-debuginfo-0.7.5-14.1
optipng-0.7.5-14.1

182537 - FreeBSD varnish Information Disclosure Vulnerability (17133e7e-d764-11e7-b5af-a4badb2f4699)

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

Risk Level: Medium

CVE: CVE-2017-8807

Description

The scan detected that the host is missing the following update:
varnish -- information disclosure vulnerability (17133e7e-d764-11e7-b5af-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/17133e7e-d764-11e7-b5af-a4badb2f4699.html

Affected packages:
varnish4 < 4.1.9
varnish5 < 5.2.1

185997 - Ubuntu Linux 14.04 USN-3497-1 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-3497-1

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/004168.html

Ubuntu 14.04

openjdk-7-jre-lib_7u151-2.6.11-2ubuntu0.14.04.1
openjdk-7-jre_7u151-2.6.11-2ubuntu0.14.04.1
openjdk-7-jre-headless_7u151-2.6.11-2ubuntu0.14.04.1
openjdk-7-jre-zero_7u151-2.6.11-2ubuntu0.14.04.1
icedtea-7-jre-jamvm_7u151-2.6.11-2ubuntu0.14.04.1

193002 - Fedora Linux 27 FEDORA-2017-a1ad512b22 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14685, CVE-2017-14686, CVE-2017-14687, CVE-2017-15369, CVE-2017-15587, CVE-2017-9216

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a1ad512b22

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 27

mupdf-1.11-9.fc27

193010 - Fedora Linux 26 FEDORA-2017-267f37c544 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14685, CVE-2017-14686, CVE-2017-14687, CVE-2017-15369, CVE-2017-15587, CVE-2017-9216

Description

The scan detected that the host is missing the following update:
FEDORA-2017-267f37c544

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/2017/12/?count=200&page=1

Fedora Core 26

mupdf-1.11-9.fc26

22799 - (K21905460) F5 BIG-IP SSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6168

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in client SSL profiles with RSA key exchange enabled. Successful exploitation could allow an attacker to obtain sensitive information and perform unauthorized actions.

22802 - Wireshark Multiple Vulnerabilities Prior To 2.4.3

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

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

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

141787 - Red Hat Enterprise Linux RHSA-2017-3384 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8184, CVE-2017-15101

Description

The scan detected that the host is missing the following update:
RHSA-2017-3384

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00005.html

RHEL7D
x86_64
liblouis-debuginfo-2.5.2-12.el7_4
liblouis-utils-2.5.2-12.el7_4

liblouis-2.5.2-12.el7_4
liblouis-devel-2.5.2-12.el7_4

noarch
liblouis-doc-2.5.2-12.el7_4
liblouis-python-2.5.2-12.el7_4

RHEL7S
noarch
liblouis-doc-2.5.2-12.el7_4
liblouis-python-2.5.2-12.el7_4

x86_64
liblouis-debuginfo-2.5.2-12.el7_4
liblouis-utils-2.5.2-12.el7_4
liblouis-2.5.2-12.el7_4
liblouis-devel-2.5.2-12.el7_4

RHEL7WS
x86_64
liblouis-debuginfo-2.5.2-12.el7_4
liblouis-utils-2.5.2-12.el7_4
liblouis-2.5.2-12.el7_4
liblouis-devel-2.5.2-12.el7_4

noarch
liblouis-doc-2.5.2-12.el7_4
liblouis-python-2.5.2-12.el7_4

141793 - Red Hat Enterprise Linux RHSA-2017-3379 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
RHSA-2017-3379

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00003.html

RHEL7D
x86_64
sssd-dbus-1.15.2-50.el7_4.8
sssd-krb5-common-1.15.2-50.el7_4.8
sssd-polkit-rules-1.15.2-50.el7_4.8
sssd-libwbclient-devel-1.15.2-50.el7_4.8
sssd-ipa-1.15.2-50.el7_4.8
sssd-common-1.15.2-50.el7_4.8
python-sss-murmur-1.15.2-50.el7_4.8
libsss_simpleifp-1.15.2-50.el7_4.8
libsss_idmap-1.15.2-50.el7_4.8
python-sss-1.15.2-50.el7_4.8
libsss_certmap-1.15.2-50.el7_4.8

libipa_hbac-devel-1.15.2-50.el7_4.8
sssd-client-1.15.2-50.el7_4.8
sssd-ldap-1.15.2-50.el7_4.8
sssd-debuginfo-1.15.2-50.el7_4.8
libsss_certmap-devel-1.15.2-50.el7_4.8
libipa_hbac-1.15.2-50.el7_4.8
libsss_nss_idmap-devel-1.15.2-50.el7_4.8
libsss_autofs-1.15.2-50.el7_4.8
sssd-winbind-idmap-1.15.2-50.el7_4.8
libsss_simpleifp-devel-1.15.2-50.el7_4.8
sssd-tools-1.15.2-50.el7_4.8
sssd-1.15.2-50.el7_4.8
libsss_sudo-1.15.2-50.el7_4.8
libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-ad-1.15.2-50.el7_4.8
sssd-krb5-1.15.2-50.el7_4.8
sssd-libwbclient-1.15.2-50.el7_4.8
sssd-proxy-1.15.2-50.el7_4.8
sssd-common-pac-1.15.2-50.el7_4.8
python-libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-kcm-1.15.2-50.el7_4.8
python-libipa_hbac-1.15.2-50.el7_4.8
libsss_idmap-devel-1.15.2-50.el7_4.8

noarch
python-sssdconfig-1.15.2-50.el7_4.8

RHEL7S
noarch
python-sssdconfig-1.15.2-50.el7_4.8

x86_64
python-libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-polkit-rules-1.15.2-50.el7_4.8
sssd-libwbclient-devel-1.15.2-50.el7_4.8
sssd-ipa-1.15.2-50.el7_4.8
sssd-common-1.15.2-50.el7_4.8
python-sss-murmur-1.15.2-50.el7_4.8
libsss_simpleifp-1.15.2-50.el7_4.8
libsss_idmap-1.15.2-50.el7_4.8
python-sss-1.15.2-50.el7_4.8
libsss_certmap-1.15.2-50.el7_4.8
libipa_hbac-devel-1.15.2-50.el7_4.8
sssd-client-1.15.2-50.el7_4.8
sssd-ldap-1.15.2-50.el7_4.8
sssd-debuginfo-1.15.2-50.el7_4.8
libsss_certmap-devel-1.15.2-50.el7_4.8
libipa_hbac-1.15.2-50.el7_4.8
libsss_nss_idmap-devel-1.15.2-50.el7_4.8
libsss_autofs-1.15.2-50.el7_4.8
sssd-winbind-idmap-1.15.2-50.el7_4.8
libsss_simpleifp-devel-1.15.2-50.el7_4.8
sssd-dbus-1.15.2-50.el7_4.8
sssd-1.15.2-50.el7_4.8
libsss_sudo-1.15.2-50.el7_4.8
sssd-krb5-common-1.15.2-50.el7_4.8
libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-ad-1.15.2-50.el7_4.8
sssd-tools-1.15.2-50.el7_4.8
sssd-krb5-1.15.2-50.el7_4.8

sssd-libwbclient-1.15.2-50.el7_4.8
sssd-proxy-1.15.2-50.el7_4.8
sssd-common-pac-1.15.2-50.el7_4.8
sssd-kcm-1.15.2-50.el7_4.8
python-libipa_hbac-1.15.2-50.el7_4.8
libsss_idmap-devel-1.15.2-50.el7_4.8

RHEL7WS
x86_64
python-libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-polkit-rules-1.15.2-50.el7_4.8
sssd-libwbclient-devel-1.15.2-50.el7_4.8
sssd-ipa-1.15.2-50.el7_4.8
sssd-common-1.15.2-50.el7_4.8
python-sss-murmur-1.15.2-50.el7_4.8
libsss_simpleifp-1.15.2-50.el7_4.8
libsss_idmap-1.15.2-50.el7_4.8
python-sss-1.15.2-50.el7_4.8
libsss_certmap-1.15.2-50.el7_4.8
libipa_hbac-devel-1.15.2-50.el7_4.8
sssd-client-1.15.2-50.el7_4.8
sssd-ldap-1.15.2-50.el7_4.8
sssd-debuginfo-1.15.2-50.el7_4.8
libsss_certmap-devel-1.15.2-50.el7_4.8
libipa_hbac-1.15.2-50.el7_4.8
libsss_nss_idmap-devel-1.15.2-50.el7_4.8
libsss_autofs-1.15.2-50.el7_4.8
sssd-winbind-idmap-1.15.2-50.el7_4.8
libsss_simpleifp-devel-1.15.2-50.el7_4.8
sssd-dbus-1.15.2-50.el7_4.8
sssd-1.15.2-50.el7_4.8
libsss_sudo-1.15.2-50.el7_4.8
sssd-krb5-common-1.15.2-50.el7_4.8
libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-ad-1.15.2-50.el7_4.8
sssd-tools-1.15.2-50.el7_4.8
sssd-krb5-1.15.2-50.el7_4.8
sssd-libwbclient-1.15.2-50.el7_4.8
sssd-proxy-1.15.2-50.el7_4.8
sssd-common-pac-1.15.2-50.el7_4.8
sssd-kcm-1.15.2-50.el7_4.8
python-libipa_hbac-1.15.2-50.el7_4.8
libsss_idmap-devel-1.15.2-50.el7_4.8

noarch
python-sssdconfig-1.15.2-50.el7_4.8

146112 - SuSE SLES 11 SP4 SUSE-SU-2017:3176-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000254

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3176-1

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-December/003464.html

SuSE SLES 11 SP4
i586
curl-7.19.7-1.70.8.1
libcurl4-7.19.7-1.70.8.1

x86_64
curl-7.19.7-1.70.8.1
libcurl4-7.19.7-1.70.8.1
libcurl4-32bit-7.19.7-1.70.8.1

146115 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3198-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000211

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3198-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00007.html

SuSE Linux 42.2
x86_64
lynx-2.8.7-8.3.1
lynx-debuginfo-2.8.7-8.3.1
lynx-debugsource-2.8.7-8.3.1

i586
lynx-2.8.7-8.3.1
lynx-debuginfo-2.8.7-8.3.1
lynx-debugsource-2.8.7-8.3.1

SuSE Linux 42.3
x86_64
lynx-2.8.7-11.1
lynx-debuginfo-2.8.7-11.1
lynx-debugsource-2.8.7-11.1

i586
lynx-2.8.7-11.1
lynx-debuginfo-2.8.7-11.1
lynx-debugsource-2.8.7-11.1

146119 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3169-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
SUSE-SU-2017:3169-1

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/003461.html

SuSE SLES 12 SP2
noarch
openssl-doc-1.0.2j-60.16.1

x86_64
openssl-1.0.2j-60.16.1
libopenssl1_0_0-hmac-1.0.2j-60.16.1
openssl-debugsource-1.0.2j-60.16.1
libopenssl1_0_0-32bit-1.0.2j-60.16.1
libopenssl-devel-1.0.2j-60.16.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.16.1
openssl-debuginfo-1.0.2j-60.16.1
libopenssl1_0_0-hmac-32bit-1.0.2j-60.16.1
libopenssl1_0_0-1.0.2j-60.16.1
libopenssl1_0_0-debuginfo-1.0.2j-60.16.1

SuSE SLED 12 SP3
x86_64
openssl-1.0.2j-60.16.1
libopenssl1_0_0-32bit-1.0.2j-60.16.1
openssl-debugsource-1.0.2j-60.16.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.16.1
libopenssl-devel-1.0.2j-60.16.1
openssl-debuginfo-1.0.2j-60.16.1
libopenssl1_0_0-1.0.2j-60.16.1
libopenssl1_0_0-debuginfo-1.0.2j-60.16.1

SuSE SLED 12 SP2
x86_64
openssl-1.0.2j-60.16.1
libopenssl1_0_0-32bit-1.0.2j-60.16.1
openssl-debugsource-1.0.2j-60.16.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.16.1
libopenssl-devel-1.0.2j-60.16.1
openssl-debuginfo-1.0.2j-60.16.1
libopenssl1_0_0-1.0.2j-60.16.1
libopenssl1_0_0-debuginfo-1.0.2j-60.16.1

SuSE SLES 12 SP3
noarch
openssl-doc-1.0.2j-60.16.1

x86_64
openssl-1.0.2j-60.16.1
libopenssl1_0_0-hmac-1.0.2j-60.16.1
openssl-debugsource-1.0.2j-60.16.1
libopenssl1_0_0-32bit-1.0.2j-60.16.1

libopenssl-devel-1.0.2j-60.16.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.16.1
openssl-debuginfo-1.0.2j-60.16.1
libopenssl1_0_0-hmac-32bit-1.0.2j-60.16.1
libopenssl1_0_0-1.0.2j-60.16.1
libopenssl1_0_0-debuginfo-1.0.2j-60.16.1

146127 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3192-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE 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:
openSUSE-SU-2017:3192-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00001.html

SuSE Linux 42.2
i586
libopenssl1_0_0-debuginfo-1.0.2j-6.6.1
openssl-cavs-1.0.2j-6.6.1
libopenssl1_0_0-hmac-1.0.2j-6.6.1
openssl-debuginfo-1.0.2j-6.6.1
libopenssl-devel-1.0.2j-6.6.1
openssl-cavs-debuginfo-1.0.2j-6.6.1
libopenssl1_0_0-1.0.2j-6.6.1
openssl-debugsource-1.0.2j-6.6.1
openssl-1.0.2j-6.6.1

noarch
openssl-doc-1.0.2j-6.6.1

x86_64
libopenssl1_0_0-1.0.2j-6.6.1
libopenssl-devel-1.0.2j-6.6.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-6.6.1
openssl-1.0.2j-6.6.1
openssl-debuginfo-1.0.2j-6.6.1
libopenssl1_0_0-hmac-1.0.2j-6.6.1
libopenssl1_0_0-debuginfo-1.0.2j-6.6.1
openssl-debugsource-1.0.2j-6.6.1
libopenssl-devel-32bit-1.0.2j-6.6.1
libopenssl1_0_0-hmac-32bit-1.0.2j-6.6.1
openssl-cavs-1.0.2j-6.6.1
openssl-cavs-debuginfo-1.0.2j-6.6.1
libopenssl1_0_0-32bit-1.0.2j-6.6.1

SuSE Linux 42.3
i586
libopenssl1_0_0-debuginfo-1.0.2j-13.1
openssl-debugsource-1.0.2j-13.1
openssl-cavs-1.0.2j-13.1

openssl-1.0.2j-13.1
libopenssl1_0_0-hmac-1.0.2j-13.1
openssl-debuginfo-1.0.2j-13.1
libopenssl1_0_0-1.0.2j-13.1
libopenssl-devel-1.0.2j-13.1
openssl-cavs-debuginfo-1.0.2j-13.1

noarch
openssl-doc-1.0.2j-13.1

x86_64
libopenssl1_0_0-hmac-1.0.2j-13.1
openssl-cavs-1.0.2j-13.1
openssl-cavs-debuginfo-1.0.2j-13.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-13.1
openssl-debuginfo-1.0.2j-13.1
libopenssl1_0_0-1.0.2j-13.1
libopenssl1_0_0-hmac-32bit-1.0.2j-13.1
libopenssl1_0_0-32bit-1.0.2j-13.1
openssl-1.0.2j-13.1
libopenssl-devel-1.0.2j-13.1
libopenssl-devel-32bit-1.0.2j-13.1
libopenssl1_0_0-debuginfo-1.0.2j-13.1
openssl-debugsource-1.0.2j-13.1

163500 - Oracle Enterprise Linux ELSA-2017-3379 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
ELSA-2017-3379

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-December/007396.html

OEL7
x86_64
sssd-krb5-common-1.15.2-50.el7_4.8
sssd-polkit-rules-1.15.2-50.el7_4.8
sssd-ldap-1.15.2-50.el7_4.8
sssd-libwbclient-devel-1.15.2-50.el7_4.8
sssd-ipa-1.15.2-50.el7_4.8
sssd-common-1.15.2-50.el7_4.8
python-sss-murmur-1.15.2-50.el7_4.8
python-sssdconfig-1.15.2-50.el7_4.8
libsss_simpleifp-1.15.2-50.el7_4.8
libsss_idmap-1.15.2-50.el7_4.8
python-sss-1.15.2-50.el7_4.8
libsss_certmap-1.15.2-50.el7_4.8
libipa_hbac-devel-1.15.2-50.el7_4.8
sssd-client-1.15.2-50.el7_4.8
python-libsss_nss_idmap-1.15.2-50.el7_4.8

sssd-winbind-idmap-1.15.2-50.el7_4.8
libsss_certmap-devel-1.15.2-50.el7_4.8
libipa_hbac-1.15.2-50.el7_4.8
libsss_nss_idmap-devel-1.15.2-50.el7_4.8
libsss_autofs-1.15.2-50.el7_4.8
sssd-dbus-1.15.2-50.el7_4.8
sssd-1.15.2-50.el7_4.8
libsss_sudo-1.15.2-50.el7_4.8
sssd-tools-1.15.2-50.el7_4.8
libsss_simpleifp-devel-1.15.2-50.el7_4.8
sssd-ad-1.15.2-50.el7_4.8
sssd-krb5-1.15.2-50.el7_4.8
sssd-libwbclient-1.15.2-50.el7_4.8
libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-common-pac-1.15.2-50.el7_4.8
sssd-proxy-1.15.2-50.el7_4.8
sssd-kcm-1.15.2-50.el7_4.8
python-libipa_hbac-1.15.2-50.el7_4.8
libsss_idmap-devel-1.15.2-50.el7_4.8

163508 - Oracle Enterprise Linux ELSA-2017-3384 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15101

Description

The scan detected that the host is missing the following update:
ELSA-2017-3384

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-December/007399.html

OEL7
x86_64
liblouis-python-2.5.2-12.el7_4
liblouis-2.5.2-12.el7_4
liblouis-utils-2.5.2-12.el7_4
liblouis-devel-2.5.2-12.el7_4
liblouis-doc-2.5.2-12.el7_4

175290 - Scientific Linux Security ERRATA Moderate: liblouis on SL7.x x86_64 (1712-1137)

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

Risk Level: Medium

CVE: CVE-2014-8184, CVE-2017-15101

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: liblouis on SL7.x x86_64 (1712-1137)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=1137

SL7
x86_64
liblouis-debuginfo-2.5.2-12.el7_4
liblouis-utils-2.5.2-12.el7_4
liblouis-2.5.2-12.el7_4
liblouis-devel-2.5.2-12.el7_4

noarch
liblouis-doc-2.5.2-12.el7_4
liblouis-python-2.5.2-12.el7_4

175298 - Scientific Linux Security ERRATA Moderate: sssd on SL7.x x86_64 (1712-1464)

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

Risk Level: Medium

CVE: CVE-2017-12173

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: sssd on SL7.x x86_64 (1712-1464)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=1464

SL7
x86_64
sssd-dbus-1.15.2-50.el7_4.8
sssd-krb5-common-1.15.2-50.el7_4.8
sssd-polkit-rules-1.15.2-50.el7_4.8
sssd-libwbclient-devel-1.15.2-50.el7_4.8
sssd-ipa-1.15.2-50.el7_4.8
sssd-common-1.15.2-50.el7_4.8
python-sss-murmur-1.15.2-50.el7_4.8
libsss_simpleifp-1.15.2-50.el7_4.8
libsss_idmap-1.15.2-50.el7_4.8
python-sss-1.15.2-50.el7_4.8
libsss_certmap-1.15.2-50.el7_4.8
libipa_hbac-devel-1.15.2-50.el7_4.8
sssd-client-1.15.2-50.el7_4.8
sssd-ldap-1.15.2-50.el7_4.8
sssd-debuginfo-1.15.2-50.el7_4.8
libsss_certmap-devel-1.15.2-50.el7_4.8
libipa_hbac-1.15.2-50.el7_4.8
libsss_nss_idmap-devel-1.15.2-50.el7_4.8
libsss_autofs-1.15.2-50.el7_4.8
sssd-winbind-idmap-1.15.2-50.el7_4.8
libsss_simpleifp-devel-1.15.2-50.el7_4.8
sssd-tools-1.15.2-50.el7_4.8
sssd-1.15.2-50.el7_4.8
libsss_sudo-1.15.2-50.el7_4.8
libsss_nss_idmap-1.15.2-50.el7_4.8

sssd-ad-1.15.2-50.el7_4.8
sssd-krb5-1.15.2-50.el7_4.8
sssd-libwbclient-1.15.2-50.el7_4.8
sssd-proxy-1.15.2-50.el7_4.8
sssd-common-pac-1.15.2-50.el7_4.8
python-libsss_nss_idmap-1.15.2-50.el7_4.8
sssd-kcm-1.15.2-50.el7_4.8
python-libipa_hbac-1.15.2-50.el7_4.8
libsss_idmap-devel-1.15.2-50.el7_4.8

noarch
python-sssdconfig-1.15.2-50.el7_4.8

193003 - Fedora Linux 27 FEDORA-2017-87142683f1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15923

Description

The scan detected that the host is missing the following update:
FEDORA-2017-87142683f1

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 27

konversation-1.7.4-1.fc27

193011 - Fedora Linux 27 FEDORA-2017-c15b709e32 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16762

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c15b709e32

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/2017/12/?count=200&page=1

Fedora Core 27

python-sanic-0.6.0-1.fc27

193012 - Fedora Linux 27 FEDORA-2017-7d25605e98 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16227

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7d25605e98

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 27

quagga-1.2.2-1.fc27

193024 - Fedora Linux 26 FEDORA-2017-5808f488a5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16762

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5808f488a5

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/2017/12/?count=200&page=1

Fedora Core 26

python-sanic-0.6.0-1.fc26

22689 - (K13421245) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6162

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 lies in Traffic Management Microkernel (TMM). Successful exploitation could allow an attacker to cause a denial of service.

22790 - (K26738102) F5 BIG-IP APM SSO Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-3687

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 SSO_ORIG_URI parameter during multi-domain single sign-on. Successful exploitation could allow an attacker to redirect the user in a multi-domain SSO environment.

146134 - SuSE SLES 11 SP4 SUSE-SU-2017:3183-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-16879

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3183-1

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-December/003468.html

SuSE SLES 11 SP4
i586
tack-5.6-93.12.1
ncurses-devel-5.6-93.12.1
libncurses5-5.6-93.12.1
libncurses6-5.6-93.12.1
terminfo-5.6-93.12.1
terminfo-base-5.6-93.12.1
ncurses-utils-5.6-93.12.1

x86_64
tack-5.6-93.12.1
libncurses6-32bit-5.6-93.12.1
ncurses-devel-5.6-93.12.1
libncurses5-32bit-5.6-93.12.1
libncurses5-5.6-93.12.1
libncurses6-5.6-93.12.1
ncurses-devel-32bit-5.6-93.12.1
terminfo-5.6-93.12.1
terminfo-base-5.6-93.12.1
ncurses-utils-5.6-93.12.1

193000 - Fedora Linux 27 FEDORA-2017-654136ee16 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10516

Description

The scan detected that the host is missing the following update:
FEDORA-2017-654136ee16

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 27

python-werkzeug-0.12.2-1.fc27

193006 - Fedora Linux 27 FEDORA-2017-5dd46193e1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9847

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5dd46193e1

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/2017/12/?count=200&page=1

Fedora Core 27

qbittorrent-4.0.1-1.fc27
rb_libtorrent-1.1.5-1.fc27

193009 - Fedora Linux 25 FEDORA-2017-4994d364de Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9847

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4994d364de

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/2017/12/?count=200&page=1

Fedora Core 25

qbittorrent-4.0.1-1.fc25
rb_libtorrent-1.1.5-1.fc25

193014 - Fedora Linux 26 FEDORA-2017-23c3f02995 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10516

Description

The scan detected that the host is missing the following update:
FEDORA-2017-23c3f02995

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/2017/12/?count=200&page=1

Fedora Core 26

python-werkzeug-0.12.2-1.fc26

193023 - Fedora Linux 26 FEDORA-2017-b2f4db4def Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9847

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b2f4db4def

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/2017/12/?count=200&page=1

Fedora Core 26

rb_libtorrent-1.1.5-1.fc26
qbittorrent-4.0.1-1.fc26

22784 - (SYM17-014) Install Norton Security Certificate Spoof Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2017-15528

Description

A spoofing vulnerability is present in some versions of Symantec Install Norton Security.

Observation

Symantec Install Norton Security is Symantec software installer for all-in-one Symantec antivirus software.

A spoofing vulnerability is present in some versions of Symantec Install Norton Security. The flaw is due to improper handling of certificates when downloading the Norton Security for Mac product. Successful exploitation could allow an attack to launch a Man in the Middle attack.

88901 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-333-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16612

Description

The scan detected that the host is missing the following update:
SSA:2017-333-01

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.618566

Slackware 14.0
x86_64
libXcursor-1.1.15-x86_64-1

Slackware 13.37
x86_64
libXcursor-1.1.15-x86_64-1

Slackware 14.1
x86_64
libXcursor-1.1.15-x86_64-1

Slackware 13.1
x86_64
libXcursor-1.1.15-x86_64-1

Slackware 14.2
x86_64
libXcursor-1.1.15-x86_64-1

i586
libXcursor-1.1.15-i586-1

Slackware 13.0
x86_64
libXcursor-1.1.15-x86_64-1

88902 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-333-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8816, CVE-2017-8817, CVE-2017-8818

Description

The scan detected that the host is missing the following update:
SSA:2017-333-03

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.440895

Slackware 14.0
x86_64
curl-7.57.0-x86_64-1

Slackware 14.2
x86_64
curl-7.57.0-x86_64-1

i586
curl-7.57.0-i586-1

Slackware 14.1
x86_64
curl-7.57.0-x86_64-1

88903 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-333-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16611

Description

The scan detected that the host is missing the following update:
SSA:2017-333-02

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.527017

Slackware 14.0
x86_64
libXfont-1.4.7-x86_64-2

Slackware 13.37
x86_64
libXfont-1.4.7-x86_64-2

Slackware 14.1
x86_64
libXfont-1.4.7-x86_64-2

Slackware 13.1

x86_64
libXfont-1.4.7-x86_64-2

Slackware 14.2
x86_64
libXfont-1.5.1-x86_64-2

Slackware 13.0
x86_64
libXfont-1.4.7-x86_64-2

130958 - Debian Linux 8.0, 9.0 DSA-4052-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14176

Description

The scan detected that the host is missing the following update:
DSA-4052-1

Observation

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

http://www.debian.org/security/2017/dsa-4052

Debian 8.0
all
bzr_2.6.0+bzr6595-6+deb8u1

Debian 9.0
all
bzr_2.7.0+bzr6619-7+deb9u1

130959 - Debian Linux 8.0, 9.0 DSA-4051-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8816, CVE-2017-8817

Description

The scan detected that the host is missing the following update:
DSA-4051-1

Observation

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

http://www.debian.org/security/2017/dsa-4051

Debian 8.0
all
curl_7.38.0-4+deb8u8

Debian 9.0

all
curl_7.52.1-5+deb9u3

130961 - Debian Linux 8.0, 9.0 DSA-4054-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8819, CVE-2017-8820, CVE-2017-8821, CVE-2017-8822, CVE-2017-8823

Description

The scan detected that the host is missing the following update:
DSA-4054-1

Observation

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

http://www.debian.org/security/2017/dsa-4054

Debian 8.0
all
tor_0.2.5.16-1

Debian 9.0
all
tor_0.2.9.14-1

130962 - Debian Linux 9.0 DSA-4053-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16943, CVE-2017-16944

Description

The scan detected that the host is missing the following update:
DSA-4053-1

Observation

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

http://www.debian.org/security/2017/dsa-4053

Debian 9.0
all
exim4_4.89-2+deb9u2

141790 - Red Hat Enterprise Linux RHSA-2017-3335 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-3335

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/msg00041.html

RHEL6_2S
x86_64
redhat-release-server-6Server-6.2.0.8.el6_2.1

141792 - Red Hat Enterprise Linux RHSA-2017-3375 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-3375

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00002.html

RHEL7_2S
x86_64
redhat-release-server-7.2-9.el7_2.4
redhat-release-computenode-7.2-8.el7_2.4

141797 - Red Hat Enterprise Linux RHSA-2017-3376 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-3376

Observation

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

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00001.html

RHEL6_5S
x86_64
redhat-release-server-6Server-6.5.0.3.el6_5.4

146113 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3196-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3196-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00005.html

SuSE Linux 42.2
i586
libcrypto41-2.5.3-5.6.1
libtls15-debuginfo-2.5.3-5.6.1
libressl-devel-2.5.3-5.6.1
libtls15-2.5.3-5.6.1
libcrypto41-debuginfo-2.5.3-5.6.1
libressl-debuginfo-2.5.3-5.6.1
libressl-debugsource-2.5.3-5.6.1
libssl43-debuginfo-2.5.3-5.6.1
libssl43-2.5.3-5.6.1
libressl-2.5.3-5.6.1

noarch
libressl-devel-doc-2.5.3-5.6.1

x86_64
libcrypto41-32bit-2.5.3-5.6.1
libressl-debuginfo-2.5.3-5.6.1
libtls15-2.5.3-5.6.1
libssl43-debuginfo-32bit-2.5.3-5.6.1
libssl43-32bit-2.5.3-5.6.1
libressl-debugsource-2.5.3-5.6.1
libressl-2.5.3-5.6.1
libcrypto41-2.5.3-5.6.1
libssl43-2.5.3-5.6.1
libressl-devel-32bit-2.5.3-5.6.1
libtls15-32bit-2.5.3-5.6.1
libcrypto41-debuginfo-2.5.3-5.6.1
libressl-devel-2.5.3-5.6.1
libtls15-debuginfo-2.5.3-5.6.1
libtls15-debuginfo-32bit-2.5.3-5.6.1
libcrypto41-debuginfo-32bit-2.5.3-5.6.1
libssl43-debuginfo-2.5.3-5.6.1

SuSE Linux 42.3
i586
libressl-debugsource-2.5.3-8.1
libressl-devel-2.5.3-8.1
libressl-2.5.3-8.1
libressl-debuginfo-2.5.3-8.1
libssl43-debuginfo-2.5.3-8.1
libtls15-debuginfo-2.5.3-8.1

libcrypto41-debuginfo-2.5.3-8.1
libtls15-2.5.3-8.1
libssl43-2.5.3-8.1
libcrypto41-2.5.3-8.1

noarch
libressl-devel-doc-2.5.3-8.1

x86_64
libcrypto41-debuginfo-2.5.3-8.1
libressl-devel-32bit-2.5.3-8.1
libressl-debuginfo-2.5.3-8.1
libressl-devel-2.5.3-8.1
libcrypto41-debuginfo-32bit-2.5.3-8.1
libtls15-32bit-2.5.3-8.1
libssl43-2.5.3-8.1
libressl-2.5.3-8.1
libtls15-debuginfo-32bit-2.5.3-8.1
libtls15-debuginfo-2.5.3-8.1
libressl-debugsource-2.5.3-8.1
libssl43-debuginfo-2.5.3-8.1
libssl43-32bit-2.5.3-8.1
libtls15-2.5.3-8.1
libcrypto41-2.5.3-8.1
libcrypto41-32bit-2.5.3-8.1
libssl43-debuginfo-32bit-2.5.3-8.1

146118 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3202-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17083, CVE-2017-17084, CVE-2017-17085

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3202-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00011.html

SuSE Linux 42.2
x86_64
wireshark-ui-gtk-debuginfo-2.2.11-14.20.1
wireshark-debuginfo-2.2.11-14.20.1
wireshark-debugsource-2.2.11-14.20.1
wireshark-ui-qt-2.2.11-14.20.1
wireshark-ui-gtk-2.2.11-14.20.1
wireshark-ui-qt-debuginfo-2.2.11-14.20.1
wireshark-2.2.11-14.20.1
wireshark-devel-2.2.11-14.20.1

SuSE Linux 42.3
x86_64
wireshark-ui-gtk-debuginfo-2.2.11-28.1
wireshark-debugsource-2.2.11-28.1

wireshark-devel-2.2.11-28.1
wireshark-ui-qt-2.2.11-28.1
wireshark-ui-qt-debuginfo-2.2.11-28.1
wireshark-ui-gtk-2.2.11-28.1
wireshark-2.2.11-28.1
wireshark-debuginfo-2.2.11-28.1

160328 - CentOS 6, 7 CESA-2017-3270 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12613

Description

The scan detected that the host is missing the following update:
CESA-2017-3270

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/022645.html
http://lists.centos.org/pipermail/centos-announce/2017-November/022646.html

CentOS 7
x86_64
apr-1.4.8-3.el7_4.1
apr-devel-1.4.8-3.el7_4.1

i686
apr-1.4.8-3.el7_4.1
apr-devel-1.4.8-3.el7_4.1

CentOS 6
x86_64
apr-devel-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

i686
apr-devel-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

163501 - Oracle Enterprise Linux ELSA-2017-3270 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12613

Description

The scan detected that the host is missing the following update:
ELSA-2017-3270

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/007359.html
http://oss.oracle.com/pipermail/el-errata/2017-November/007358.html

OEL7
x86_64
apr-1.4.8-3.el7_4.1
apr-devel-1.4.8-3.el7_4.1

OEL6
x86_64
apr-devel-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

i386
apr-devel-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

175295 - Scientific Linux Security ERRATA Important: apr on SL6.x, SL7.x i386/x86_64 (1711-7409)

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

Risk Level: Low

CVE: CVE-2017-12613

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: apr on SL6.x, SL7.x i386/x86_64 (1711-7409)

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=7409

SL7
x86_64
apr-1.4.8-3.el7_4.1
apr-debuginfo-1.4.8-3.el7_4.1
apr-devel-1.4.8-3.el7_4.1

SL6
x86_64
apr-devel-1.3.9-5.el6_9.1
apr-debuginfo-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

i386
apr-devel-1.3.9-5.el6_9.1
apr-debuginfo-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

182531 - FreeBSD cURL Multiple Vulnerabilities (301a01b7-d50e-11e7-ac58-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-8816, CVE-2017-8817, CVE-2017-8818

Description

The scan detected that the host is missing the following update:
cURL -- Multiple vulnerabilities (301a01b7-d50e-11e7-ac58-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/301a01b7-d50e-11e7-ac58-b499baebfeaf.html

Affected packages:
7.21.0 < curl < 7.57.0

182532 - FreeBSD xrdp Local User Can Cause A Denial Of Service (a66f9be2-d519-11e7-9866-c85b763a2f96)

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

Risk Level: Low

CVE: CVE-2017-16927

Description

The scan detected that the host is missing the following update:
xrdp -- local user can cause a denial of service (a66f9be2-d519-11e7-9866-c85b763a2f96)

Observation

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

http://www.vuxml.org/freebsd/a66f9be2-d519-11e7-9866-c85b763a2f96.html

Affected packages:
xrdp-devel <= 0.9.3,1
0.9.3_1,1 < xrdp-devel <= 0.9.4,1

182533 - FreeBSD wordpress Multiple Issues (a2589511-d6ba-11e7-88dd-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 (a2589511-d6ba-11e7-88dd-00e04c1ea73d)

Observation

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

http://www.vuxml.org/freebsd/a2589511-d6ba-11e7-88dd-00e04c1ea73d.html

Affected packages:
wordpress < 4.9.1,1
fr-wordpress < 4.9.1,1
de-wordpress < 4.9.1
zh_CN-wordpress < 4.9.1
zh_TW-wordpress < 4.9.1
ja-wordpress < 4.9.1

ru_RU-wordpress < 4.9.1

182534 - FreeBSD asterisk DOS Vulnerability In Asterisk Chan_skinny (e91cf90c-d6dd-11e7-9d10-001999f8d30b)

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:
asterisk -- DOS Vulnerability in Asterisk chan_skinny (e91cf90c-d6dd-11e7-9d10-001999f8d30b)

Observation

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

http://www.vuxml.org/freebsd/e91cf90c-d6dd-11e7-9d10-001999f8d30b.html

Affected packages:
asterisk13 < 13.18.3

182535 - FreeBSD exim Remote DoS Attack In BDAT Processing (75dd622c-d5fd-11e7-b9fe-c13eb7bcbf4f)

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

Risk Level: Low

CVE: CVE-2017-16944

Description

The scan detected that the host is missing the following update:
exim -- remote DoS attack in BDAT processing (75dd622c-d5fd-11e7-b9fe-c13eb7bcbf4f)

Observation

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

http://www.vuxml.org/freebsd/75dd622c-d5fd-11e7-b9fe-c13eb7bcbf4f.html

Affected packages:
4.88 <= exim < 4.89.1

182536 - FreeBSD mozilla Multiple Vulnerabilities (b7e23050-2d5d-4e61-9b48-62e89db222ca)

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

Risk Level: Low

CVE: CVE-2017-7843, CVE-2017-7844

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (b7e23050-2d5d-4e61-9b48-62e89db222ca)

Observation

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

http://www.vuxml.org/freebsd/b7e23050-2d5d-4e61-9b48-62e89db222ca.html

Affected packages:
57.0,1 <= firefox < 57.0.1,1
firefox < 56.0.2_11,1
waterfox < 56.0.s20171130
seamonkey < 2.49.2
linux-seamonkey < 2.49.2
firefox-esr < 52.5.1,1
linux-firefox < 52.5.1,2

182538 - FreeBSD mybb Multiple Vulnerabilities (addad6de-d752-11e7-99bf-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:
mybb -- multiple vulnerabilities (addad6de-d752-11e7-99bf-00e04c1ea73d)

Observation

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

http://www.vuxml.org/freebsd/addad6de-d752-11e7-99bf-00e04c1ea73d.html

Affected packages:
mybb < 1.8.14

182539 - FreeBSD borgbackup Remote Users Can Override Repository Restrictions (0d369972-d4ba-11e7-bfca-005056925db4)

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

Risk Level: Low

CVE: CVE-2017-15914

Description

The scan detected that the host is missing the following update:
borgbackup -- remote users can override repository restrictions (0d369972-d4ba-11e7-bfca-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/0d369972-d4ba-11e7-bfca-005056925db4.html

Affected packages:
1.1.0 <= py34-borgbackup < 1.1.3
1.1.0 <= py35-borgbackup < 1.1.3
1.1.0 <= py36-borgbackup < 1.1.3

185995 - Ubuntu Linux 17.04, 17.10 USN-3499-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16944

Description

The scan detected that the host is missing the following update:
USN-3499-1

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/004171.html

Ubuntu 17.10

exim4-daemon-heavy_4.89-5ubuntu1.2
exim4-daemon-light_4.89-5ubuntu1.2

Ubuntu 17.04

exim4-daemon-light_4.88-5ubuntu1.3
exim4-daemon-heavy_4.88-5ubuntu1.3

185996 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3501-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16612

Description

The scan detected that the host is missing the following update:
USN-3501-1

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/004173.html

Ubuntu 16.04

libxcursor1_1.1.14-1ubuntu0.16.04.1

Ubuntu 14.04

libxcursor1_1.1.14-1ubuntu0.14.04.1

Ubuntu 17.04

libxcursor1_1.1.14-1ubuntu0.17.04.1

Ubuntu 17.10

libxcursor1_1.1.14-3ubuntu0.1

185999 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3498-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8816, CVE-2017-8817

Description

The scan detected that the host is missing the following update:
USN-3498-1

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/004169.html

Ubuntu 16.04

libcurl3_7.47.0-1ubuntu2.5
libcurl3-gnutls_7.47.0-1ubuntu2.5
libcurl3-nss_7.47.0-1ubuntu2.5
curl_7.47.0-1ubuntu2.5

Ubuntu 14.04

libcurl3-gnutls_7.35.0-1ubuntu2.13
libcurl3_7.35.0-1ubuntu2.13
libcurl3-nss_7.35.0-1ubuntu2.13
curl_7.35.0-1ubuntu2.13

Ubuntu 17.04

libcurl3_7.52.1-4ubuntu1.4
curl_7.52.1-4ubuntu1.4
libcurl3-nss_7.52.1-4ubuntu1.4
libcurl3-gnutls_7.52.1-4ubuntu1.4

Ubuntu 17.10

libcurl3-gnutls_7.55.1-1ubuntu2.2
libcurl3_7.55.1-1ubuntu2.2
curl_7.55.1-1ubuntu2.2
libcurl3-nss_7.55.1-1ubuntu2.2

186000 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3500-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16611

Description

The scan detected that the host is missing the following update:
USN-3500-1

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/004172.html

Ubuntu 16.04

libxfont1_1.5.1-1ubuntu0.16.04.4
libxfont2_2.0.1-3~ubuntu16.04.3

Ubuntu 14.04

libxfont1_1.4.7-1ubuntu0.4

Ubuntu 17.04

libxfont2_2.0.1-3ubuntu0.2
libxfont1_1.5.2-4ubuntu0.2

Ubuntu 17.10

libxfont1_1.5.2-4ubuntu1.1
libxfont2_2.0.1-3ubuntu1.1

186001 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3477-3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7826, CVE-2017-7827, CVE-2017-7828, CVE-2017-7830, CVE-2017-7831, CVE-2017-7832, CVE-2017-7833, CVE-2017-7834, CVE-2017-7835, CVE-2017-7837, CVE-2017-7838, CVE-2017-7839, CVE-2017-7840, CVE-2017-7842

Description

The scan detected that the host is missing the following update:
USN-3477-3

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004175.html

Ubuntu 16.04

firefox_57.0.1+build2-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_57.0.1+build2-0ubuntu0.14.04.1

Ubuntu 17.04

firefox_57.0.1+build2-0ubuntu0.17.04.1

Ubuntu 17.10

firefox_57.0.1+build2-0ubuntu0.17.10.1

186003 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3490-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
USN-3490-1

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-December/004174.html

Ubuntu 16.04

thunderbird_52.5.0+build1-0ubuntu0.16.04.1

Ubuntu 14.04

thunderbird_52.5.0+build1-0ubuntu0.14.04.1

Ubuntu 17.04

thunderbird_52.5.0+build1-0ubuntu0.17.04.1

Ubuntu 17.10

thunderbird_52.5.0+build1-0ubuntu0.17.10.1

186006 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3503-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000159

Description

The scan detected that the host is missing the following update:
USN-3503-1

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-December/004176.html

Ubuntu 16.04

evince_3.18.2-1ubuntu4.3
evince-common_3.18.2-1ubuntu4.3

Ubuntu 14.04

evince-common_3.10.3-0ubuntu10.4
evince_3.10.3-0ubuntu10.4

Ubuntu 17.04

evince_3.24.0-0ubuntu1.3
evince-common_3.24.0-0ubuntu1.3

193004 - Fedora Linux 26 FEDORA-2017-9ea11e444d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000405

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9ea11e444d

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/2017/12/?count=200&page=1

Fedora Core 26

kernel-4.13.16-202.fc26

193005 - Fedora Linux 25 FEDORA-2017-9015553e3d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15390, CVE-2017-15392, CVE-2017-15394, CVE-2017-15396, CVE-2017-15398, CVE-2017-5124, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5132, CVE-2017-5133

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9015553e3d

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/2017/12/?count=200&page=1

Fedora Core 25

qt5-qtwebengine-5.9.3-1.fc25

193007 - Fedora Linux 27 FEDORA-2017-612d3e009f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15110

Description

The scan detected that the host is missing the following update:
FEDORA-2017-612d3e009f

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 27

moodle-3.3.3-1.fc27

193008 - Fedora Linux 27 FEDORA-2017-15b815b9b7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15390, CVE-2017-15392, CVE-2017-15394, CVE-2017-15396, CVE-2017-15398, CVE-2017-5124, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5132, CVE-2017-5133

Description

The scan detected that the host is missing the following update:
FEDORA-2017-15b815b9b7

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/2017/12/?count=200&page=1

Fedora Core 27

qt5-qtwebengine-5.9.3-1.fc27

193013 - Fedora Linux 25 FEDORA-2017-e40e02e0dd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15110

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e40e02e0dd

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/2017/12/?count=200&page=1

Fedora Core 25

moodle-3.1.9-1.fc25

193015 - Fedora Linux 27 FEDORA-2017-f76bf63612 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-0203

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f76bf63612

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/2017/12/?count=200&page=1

Fedora Core 27

qpid-cpp-1.36.0-8.fc27

193016 - Fedora Linux 27 FEDORA-2017-9e775c0d06 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-2017-9e775c0d06

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 27

slurm-17.02.9-3.fc27

193018 - Fedora Linux 27 FEDORA-2017-b0c1f44130 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000405

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b0c1f44130

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/2017/12/?count=200&page=1

Fedora Core 27

kernel-4.13.16-302.fc27

193019 - Fedora Linux 26 FEDORA-2017-e7938fd7d7 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-e7938fd7d7

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/2017/12/?count=200&page=1

Fedora Core 26

java-9-openjdk-9.0.1.11-4.fc26

193022 - Fedora Linux 27 FEDORA-2017-78a4610238 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-2017-78a4610238

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 27

mediawiki-1.29.2-2.fc27

193025 - Fedora Linux 26 FEDORA-2017-475529a26a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15110

Description

The scan detected that the host is missing the following update:
FEDORA-2017-475529a26a

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/2017/12/?count=200&page=1

Fedora Core 26

moodle-3.2.6-1.fc26

193026 - Fedora Linux 26 FEDORA-2017-2522df3526 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-2017-2522df3526

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/2017/12/?count=200&page=1

Fedora Core 26

nodejs-brace-expansion-1.1.7-1.fc26
nodejs-balanced-match-0.4.2-4.fc26

193027 - Fedora Linux 26 FEDORA-2017-4d90e9fc97 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15390, CVE-2017-15392, CVE-2017-15394, CVE-2017-15396, CVE-2017-15398, CVE-2017-5124, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5132, CVE-2017-5133

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4d90e9fc97

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/2017/12/?count=200&page=1

Fedora Core 26

qt5-qtwebengine-5.9.3-1.fc26

141791 - Red Hat Enterprise Linux RHSA-2017-3315 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000380

Description

The scan detected that the host is missing the following update:
RHSA-2017-3315

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/msg00048.html

RHEL7D
x86_64
kernel-debug-debuginfo-3.10.0-693.11.1.el7
kernel-debuginfo-common-x86_64-3.10.0-693.11.1.el7
kernel-debug-3.10.0-693.11.1.el7
kernel-3.10.0-693.11.1.el7
kernel-tools-libs-devel-3.10.0-693.11.1.el7
kernel-debug-devel-3.10.0-693.11.1.el7
python-perf-debuginfo-3.10.0-693.11.1.el7
kernel-headers-3.10.0-693.11.1.el7
kernel-tools-3.10.0-693.11.1.el7
python-perf-3.10.0-693.11.1.el7
kernel-tools-libs-3.10.0-693.11.1.el7
kernel-tools-debuginfo-3.10.0-693.11.1.el7
kernel-debuginfo-3.10.0-693.11.1.el7
perf-3.10.0-693.11.1.el7
kernel-devel-3.10.0-693.11.1.el7
perf-debuginfo-3.10.0-693.11.1.el7

noarch
kernel-abi-whitelists-3.10.0-693.11.1.el7
kernel-doc-3.10.0-693.11.1.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-693.11.1.el7
kernel-doc-3.10.0-693.11.1.el7

x86_64
kernel-debug-debuginfo-3.10.0-693.11.1.el7
kernel-debuginfo-common-x86_64-3.10.0-693.11.1.el7
kernel-debug-3.10.0-693.11.1.el7
kernel-3.10.0-693.11.1.el7
kernel-tools-libs-devel-3.10.0-693.11.1.el7
kernel-debug-devel-3.10.0-693.11.1.el7
python-perf-debuginfo-3.10.0-693.11.1.el7
kernel-headers-3.10.0-693.11.1.el7
kernel-tools-3.10.0-693.11.1.el7
python-perf-3.10.0-693.11.1.el7
kernel-tools-libs-3.10.0-693.11.1.el7
kernel-tools-debuginfo-3.10.0-693.11.1.el7
kernel-debuginfo-3.10.0-693.11.1.el7
perf-3.10.0-693.11.1.el7
kernel-devel-3.10.0-693.11.1.el7
perf-debuginfo-3.10.0-693.11.1.el7

RHEL7WS
x86_64
kernel-debug-debuginfo-3.10.0-693.11.1.el7
kernel-debuginfo-common-x86_64-3.10.0-693.11.1.el7
kernel-debug-3.10.0-693.11.1.el7
kernel-3.10.0-693.11.1.el7
kernel-tools-libs-devel-3.10.0-693.11.1.el7
kernel-debug-devel-3.10.0-693.11.1.el7
python-perf-debuginfo-3.10.0-693.11.1.el7
kernel-headers-3.10.0-693.11.1.el7
kernel-tools-3.10.0-693.11.1.el7
python-perf-3.10.0-693.11.1.el7
kernel-tools-libs-3.10.0-693.11.1.el7
kernel-tools-debuginfo-3.10.0-693.11.1.el7
kernel-debuginfo-3.10.0-693.11.1.el7
perf-3.10.0-693.11.1.el7
kernel-devel-3.10.0-693.11.1.el7
perf-debuginfo-3.10.0-693.11.1.el7

noarch
kernel-abi-whitelists-3.10.0-693.11.1.el7
kernel-doc-3.10.0-693.11.1.el7

146135 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3144-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13080, CVE-2017-13081

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3144-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-11/msg00096.html

SuSE Linux 42.2
noarch
ucode-amd-20170530-7.9.1
kernel-firmware-20170530-7.9.1

SuSE Linux 42.3
noarch
ucode-amd-20170530-11.1
kernel-firmware-20170530-11.1

163502 - Oracle Enterprise Linux ELSA-2017-3315 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000380

Description

The scan detected that the host is missing the following update:
ELSA-2017-3315

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/007363.html
http://oss.oracle.com/pipermail/el-errata/2017-November/007361.html

OEL7
x86_64
kernel-tools-libs-devel-3.10.0-693.11.1.0.1.el7
kernel-devel-3.10.0-693.11.1.0.1.el7
kernel-3.10.0-693.11.1.el7
kernel-tools-libs-devel-3.10.0-693.11.1.el7
perf-3.10.0-693.11.1.0.1.el7
kernel-debug-devel-3.10.0-693.11.1.el7
kernel-debug-devel-3.10.0-693.11.1.0.1.el7
kernel-headers-3.10.0-693.11.1.el7
kernel-doc-3.10.0-693.11.1.0.1.el7
python-perf-3.10.0-693.11.1.0.1.el7
kernel-abi-whitelists-3.10.0-693.11.1.el7
python-perf-3.10.0-693.11.1.el7
kernel-debug-3.10.0-693.11.1.0.1.el7
kernel-abi-whitelists-3.10.0-693.11.1.0.1.el7
kernel-tools-libs-3.10.0-693.11.1.el7
kernel-debug-3.10.0-693.11.1.el7
kernel-headers-3.10.0-693.11.1.0.1.el7
kernel-tools-3.10.0-693.11.1.el7
kernel-3.10.0-693.11.1.0.1.el7
kernel-tools-3.10.0-693.11.1.0.1.el7
kernel-tools-libs-3.10.0-693.11.1.0.1.el7
perf-3.10.0-693.11.1.el7
kernel-devel-3.10.0-693.11.1.el7
kernel-doc-3.10.0-693.11.1.el7

175297 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1712-79)

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

Risk Level: Low

CVE: CVE-2017-1000380

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1712-79)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=79

SL7
x86_64
kernel-debug-debuginfo-3.10.0-693.11.1.el7
kernel-debuginfo-common-x86_64-3.10.0-693.11.1.el7

kernel-debug-3.10.0-693.11.1.el7
kernel-3.10.0-693.11.1.el7
kernel-tools-libs-devel-3.10.0-693.11.1.el7
kernel-debug-devel-3.10.0-693.11.1.el7
python-perf-debuginfo-3.10.0-693.11.1.el7
kernel-headers-3.10.0-693.11.1.el7
kernel-tools-3.10.0-693.11.1.el7
python-perf-3.10.0-693.11.1.el7
kernel-tools-libs-3.10.0-693.11.1.el7
kernel-tools-debuginfo-3.10.0-693.11.1.el7
kernel-debuginfo-3.10.0-693.11.1.el7
perf-3.10.0-693.11.1.el7
kernel-devel-3.10.0-693.11.1.el7
perf-debuginfo-3.10.0-693.11.1.el7

noarch
kernel-abi-whitelists-3.10.0-693.11.1.el7
kernel-doc-3.10.0-693.11.1.el7

186005 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3505-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13080, CVE-2017-13081

Description

The scan detected that the host is missing the following update:
USN-3505-1

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-December/004180.html

Ubuntu 16.04

linux-firmware_1.157.14

Ubuntu 14.04

linux-firmware_1.127.24

Ubuntu 17.04

linux-firmware_1.164.2

Ubuntu 17.10

linux-firmware_1.169.1

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.

141771 - Red Hat Enterprise Linux RHSA-2017-3190 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15095, CVE-2017-7525

Update Details

FASLScript is updated

141786 - Red Hat Enterprise Linux RHSA-2017-3265 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux 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

Update Details

FASLScript is updated

33307 - Oracle Solaris 151934-04 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

70046 - macosx.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com/

Multi-National Phone Support available here:

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

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