2016-APR-13
FSL version 7.5.810

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

141158 - Red Hat Enterprise Linux RHSA-2016-0610 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1006, CVE-2016-1011, CVE-2016-1012, CVE-2016-1013, CVE-2016-1014, CVE-2016-1015, CVE-2016-1016, CVE-2016-1017, CVE-2016-1018, CVE-2016-1019, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1030, CVE-2016-1031, CVE-2016-1032, CVE-2016-1033

Description

The scan detected that the host is missing the following update:
RHSA-2016-0610

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0610.html

RHEL5S
x86_64
flash-plugin-11.2.202.616-1.el5

i386
flash-plugin-11.2.202.616-1.el5

RHEL6D
x86_64
flash-plugin-11.2.202.616-1.el6_7

i386
flash-plugin-11.2.202.616-1.el6_7

RHEL6S
x86_64
flash-plugin-11.2.202.616-1.el6_7

i386
flash-plugin-11.2.202.616-1.el6_7

RHEL6WS
x86_64
flash-plugin-11.2.202.616-1.el6_7

i386
flash-plugin-11.2.202.616-1.el6_7

RHEL5D
x86_64
flash-plugin-11.2.202.616-1.el5

i386
flash-plugin-11.2.202.616-1.el5

144525 - SuSE Linux 13.2 openSUSE-SU-2016:0995-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4529, CVE-2013-4530, CVE-2013-4533, CVE-2013-4534, CVE-2013-4537, CVE-2013-4538, CVE-2013-4539, CVE-2014-0222, CVE-2014-3689, CVE-2014-7815, CVE-2014-9718, CVE-2015-1779, CVE-2015-5239, CVE-2015-5278, CVE-2015-6815, CVE-2015-6855, CVE-2015-7512, CVE-2015-8345, CVE-2015-8613, CVE-2015-8619, CVE-2015-8743, CVE-2015-8744, CVE-2015-8745, CVE-2016-1568, CVE-2016-1570, CVE-2016-1571, CVE-2016-1714, CVE-2016-1981, CVE-2016-2198, CVE-2016-2270, CVE-2016-2271, CVE-2016-2392, CVE-2016-2538

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:0995-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-04/msg00023.html

SuSE Linux 13.2
x86_64
xen-tools-debuginfo-4.4.4_02-43.1
xen-kmp-desktop-debuginfo-4.4.4_02_k3.16.7_35-43.1
xen-tools-domU-4.4.4_02-43.1
xen-tools-domU-debuginfo-4.4.4_02-43.1
xen-doc-html-4.4.4_02-43.1
xen-kmp-default-4.4.4_02_k3.16.7_35-43.1
xen-libs-debuginfo-4.4.4_02-43.1
xen-devel-4.4.4_02-43.1
xen-tools-4.4.4_02-43.1
xen-libs-32bit-4.4.4_02-43.1
xen-libs-4.4.4_02-43.1
xen-kmp-desktop-4.4.4_02_k3.16.7_35-43.1
xen-4.4.4_02-43.1
xen-libs-debuginfo-32bit-4.4.4_02-43.1
xen-kmp-default-debuginfo-4.4.4_02_k3.16.7_35-43.1
xen-debugsource-4.4.4_02-43.1

i586
xen-devel-4.4.4_02-43.1
xen-tools-domU-4.4.4_02-43.1
xen-libs-debuginfo-4.4.4_02-43.1
xen-libs-4.4.4_02-43.1
xen-tools-domU-debuginfo-4.4.4_02-43.1
xen-debugsource-4.4.4_02-43.1

144526 - SuSE SLED 12, 12 SP1 SUSE-SU-2016:0990-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1019

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:0990-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-April/001992.html

SuSE SLED 12
x86_64
flash-player-gnome-11.2.202.616-126.1
flash-player-11.2.202.616-126.1

SuSE SLED 12 SP1
x86_64
flash-player-gnome-11.2.202.616-126.1
flash-player-11.2.202.616-126.1

185239 - Ubuntu Linux 12.04, 14.04, 15.10 USN-2917-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1950, CVE-2016-1952, CVE-2016-1953, CVE-2016-1954, CVE-2016-1955, CVE-2016-1956, CVE-2016-1957, CVE-2016-1958, CVE-2016-1959, CVE-2016-1960, CVE-2016-1961, CVE-2016-1962, CVE-2016-1963, CVE-2016-1964, CVE-2016-1965, CVE-2016-1966, CVE-2016-1967, CVE-2016-1968, CVE-2016-1973, CVE-2016-1974, CVE-2016-1977, CVE-2016-2790, CVE-2016-2791, CVE-2016-2792, CVE-2016-2793, CVE-2016-2794, CVE-2016-2795, CVE-2016-2796, CVE-2016-2797, CVE-2016-2798, CVE-2016-2799, CVE-2016-2800, CVE-2016-2801, CVE-2016-2802

Description

The scan detected that the host is missing the following update:
USN-2917-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-April/003380.html

Ubuntu 12.04

firefox_45.0.1+build1-0ubuntu0.12.04.2

Ubuntu 15.10

firefox_45.0.1+build1-0ubuntu0.15.10.2

Ubuntu 14.04

firefox_45.0.1+build1-0ubuntu0.14.04.2

141151 - Red Hat Enterprise Linux RHSA-2016-0619 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
RHSA-2016-0619

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0619.html

RHEL6_2S
x86_64
samba-doc-3.6.23-30.el6_2
libsmbclient-devel-3.6.23-30.el6_2
samba-domainjoin-gui-3.6.23-30.el6_2
samba-swat-3.6.23-30.el6_2
samba-debuginfo-3.6.23-30.el6_2
samba-winbind-devel-3.6.23-30.el6_2
samba-winbind-krb5-locator-3.6.23-30.el6_2

RHEL6_6S
i386
libsmbclient-3.6.23-30.el6_6
samba-3.6.23-30.el6_6
samba-debuginfo-3.6.23-30.el6_6
samba-winbind-clients-3.6.23-30.el6_6
samba-winbind-3.6.23-30.el6_6
samba-common-3.6.23-30.el6_6
samba-client-3.6.23-30.el6_6

x86_64
libsmbclient-3.6.23-30.el6_6
samba-3.6.23-30.el6_6
samba-debuginfo-3.6.23-30.el6_6
samba-winbind-clients-3.6.23-30.el6_6
samba-winbind-3.6.23-30.el6_6
samba-common-3.6.23-30.el6_6
samba-client-3.6.23-30.el6_6

141152 - Red Hat Enterprise Linux RHSA-2016-0613 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
RHSA-2016-0613

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0613.html

RHEL5D
x86_64
samba3x-debuginfo-3.6.23-12.el5_11
samba3x-doc-3.6.23-12.el5_11
samba3x-domainjoin-gui-3.6.23-12.el5_11
samba3x-swat-3.6.23-12.el5_11
samba3x-winbind-3.6.23-12.el5_11
samba3x-3.6.23-12.el5_11
samba3x-common-3.6.23-12.el5_11
samba3x-client-3.6.23-12.el5_11

i386
samba3x-debuginfo-3.6.23-12.el5_11
samba3x-doc-3.6.23-12.el5_11
samba3x-domainjoin-gui-3.6.23-12.el5_11
samba3x-swat-3.6.23-12.el5_11
samba3x-winbind-3.6.23-12.el5_11
samba3x-3.6.23-12.el5_11
samba3x-common-3.6.23-12.el5_11
samba3x-client-3.6.23-12.el5_11

RHEL5S
i386
samba3x-debuginfo-3.6.23-12.el5_11
samba3x-doc-3.6.23-12.el5_11
samba3x-winbind-devel-3.6.23-12.el5_11
samba3x-domainjoin-gui-3.6.23-12.el5_11
samba3x-swat-3.6.23-12.el5_11
samba3x-winbind-3.6.23-12.el5_11
samba3x-3.6.23-12.el5_11
samba3x-common-3.6.23-12.el5_11
samba3x-client-3.6.23-12.el5_11

x86_64
samba3x-debuginfo-3.6.23-12.el5_11
samba3x-doc-3.6.23-12.el5_11
samba3x-winbind-devel-3.6.23-12.el5_11
samba3x-domainjoin-gui-3.6.23-12.el5_11
samba3x-swat-3.6.23-12.el5_11
samba3x-winbind-3.6.23-12.el5_11
samba3x-3.6.23-12.el5_11
samba3x-common-3.6.23-12.el5_11
samba3x-client-3.6.23-12.el5_11

141154 - Red Hat Enterprise Linux RHSA-2016-0611 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
RHSA-2016-0611

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0611.html

RHEL6D
x86_64
samba-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-winbind-krb5-locator-3.6.23-30.el6_7
samba-debuginfo-3.6.23-30.el6_7
samba-swat-3.6.23-30.el6_7
samba-glusterfs-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
libsmbclient-devel-3.6.23-30.el6_7
samba-winbind-devel-3.6.23-30.el6_7
samba-doc-3.6.23-30.el6_7
samba-common-3.6.23-30.el6_7
samba-domainjoin-gui-3.6.23-30.el6_7

i386
samba-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-winbind-krb5-locator-3.6.23-30.el6_7
samba-debuginfo-3.6.23-30.el6_7
samba-swat-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
libsmbclient-devel-3.6.23-30.el6_7
samba-winbind-devel-3.6.23-30.el6_7
samba-doc-3.6.23-30.el6_7
samba-common-3.6.23-30.el6_7
samba-domainjoin-gui-3.6.23-30.el6_7

RHEL6S
i386
samba-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-winbind-krb5-locator-3.6.23-30.el6_7
samba-debuginfo-3.6.23-30.el6_7
samba-swat-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
libsmbclient-devel-3.6.23-30.el6_7
samba-winbind-devel-3.6.23-30.el6_7
samba-doc-3.6.23-30.el6_7
samba-common-3.6.23-30.el6_7
samba-domainjoin-gui-3.6.23-30.el6_7

x86_64
samba-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-winbind-krb5-locator-3.6.23-30.el6_7
samba-debuginfo-3.6.23-30.el6_7

samba-swat-3.6.23-30.el6_7
samba-glusterfs-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
libsmbclient-devel-3.6.23-30.el6_7
samba-winbind-devel-3.6.23-30.el6_7
samba-doc-3.6.23-30.el6_7
samba-common-3.6.23-30.el6_7
samba-domainjoin-gui-3.6.23-30.el6_7

RHEL6WS
x86_64
samba-common-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-3.6.23-30.el6_7
samba-debuginfo-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7

i386
samba-common-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-3.6.23-30.el6_7
samba-debuginfo-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7

141157 - Red Hat Enterprise Linux RHSA-2016-0612 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
RHSA-2016-0612

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0612.html

RHEL7S
noarch
samba-pidl-4.2.10-6.el7_2
openchange-devel-docs-2.0-10.el7_2
samba-common-4.2.10-6.el7_2

RHEL6S
i386
libtalloc-debuginfo-2.1.5-1.el6_7
ipa-admintools-3.0.0-47.el6_7.2
openchange-devel-1.0-7.el6_7
libldb-debuginfo-1.1.25-2.el6_7
libldb-devel-1.1.25-2.el6_7

samba4-winbind-clients-4.2.10-6.el6_7
ipa-server-3.0.0-47.el6_7.2
ipa-python-3.0.0-47.el6_7.2
ipa-client-3.0.0-47.el6_7.2
libtevent-0.9.26-2.el6_7
samba4-debuginfo-4.2.10-6.el6_7
python-tevent-0.9.26-2.el6_7
libtdb-debuginfo-1.3.8-1.el6_7
openchange-client-1.0-7.el6_7
ldb-tools-1.1.25-2.el6_7
pytalloc-devel-2.1.5-1.el6_7
pyldb-devel-1.1.25-2.el6_7
ipa-server-selinux-3.0.0-47.el6_7.2
ipa-server-trust-ad-3.0.0-47.el6_7.2
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
openchange-devel-docs-1.0-7.el6_7
libtdb-devel-1.3.8-1.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
ipa-debuginfo-3.0.0-47.el6_7.2
samba4-dc-4.2.10-6.el6_7
samba4-common-4.2.10-6.el6_7
openchange-1.0-7.el6_7
samba4-libs-4.2.10-6.el6_7
libtalloc-devel-2.1.5-1.el6_7
libtevent-debuginfo-0.9.26-2.el6_7
samba4-client-4.2.10-6.el6_7
openchange-debuginfo-1.0-7.el6_7
libldb-1.1.25-2.el6_7
samba4-devel-4.2.10-6.el6_7
samba4-test-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

x86_64
libtalloc-debuginfo-2.1.5-1.el6_7
ipa-admintools-3.0.0-47.el6_7.2
openchange-devel-1.0-7.el6_7
libldb-debuginfo-1.1.25-2.el6_7
libldb-devel-1.1.25-2.el6_7
samba4-winbind-clients-4.2.10-6.el6_7
ipa-server-3.0.0-47.el6_7.2
ipa-python-3.0.0-47.el6_7.2
ipa-client-3.0.0-47.el6_7.2
libtevent-0.9.26-2.el6_7
samba4-debuginfo-4.2.10-6.el6_7
python-tevent-0.9.26-2.el6_7
libtdb-debuginfo-1.3.8-1.el6_7
openchange-client-1.0-7.el6_7
ldb-tools-1.1.25-2.el6_7
pytalloc-devel-2.1.5-1.el6_7
pyldb-devel-1.1.25-2.el6_7

ipa-server-selinux-3.0.0-47.el6_7.2
ipa-server-trust-ad-3.0.0-47.el6_7.2
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
openchange-devel-docs-1.0-7.el6_7
libtdb-devel-1.3.8-1.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
ipa-debuginfo-3.0.0-47.el6_7.2
samba4-dc-4.2.10-6.el6_7
samba4-common-4.2.10-6.el6_7
openchange-1.0-7.el6_7
samba4-libs-4.2.10-6.el6_7
libtalloc-devel-2.1.5-1.el6_7
libtevent-debuginfo-0.9.26-2.el6_7
samba4-client-4.2.10-6.el6_7
openchange-debuginfo-1.0-7.el6_7
libldb-1.1.25-2.el6_7
samba4-devel-4.2.10-6.el6_7
samba4-test-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

RHEL6WS
x86_64
libtalloc-debuginfo-2.1.5-1.el6_7
ipa-admintools-3.0.0-47.el6_7.2
libldb-debuginfo-1.1.25-2.el6_7
libldb-devel-1.1.25-2.el6_7
samba4-winbind-clients-4.2.10-6.el6_7
ipa-server-3.0.0-47.el6_7.2
ipa-python-3.0.0-47.el6_7.2
ipa-client-3.0.0-47.el6_7.2
libtevent-0.9.26-2.el6_7
samba4-debuginfo-4.2.10-6.el6_7
python-tevent-0.9.26-2.el6_7
libtdb-debuginfo-1.3.8-1.el6_7
ipa-server-selinux-3.0.0-47.el6_7.2
ipa-server-trust-ad-3.0.0-47.el6_7.2
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
libtdb-devel-1.3.8-1.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
ipa-debuginfo-3.0.0-47.el6_7.2
samba4-dc-4.2.10-6.el6_7

samba4-common-4.2.10-6.el6_7
openchange-1.0-7.el6_7
samba4-libs-4.2.10-6.el6_7
libtalloc-devel-2.1.5-1.el6_7
libtevent-debuginfo-0.9.26-2.el6_7
samba4-client-4.2.10-6.el6_7
openchange-debuginfo-1.0-7.el6_7
libldb-1.1.25-2.el6_7
samba4-devel-4.2.10-6.el6_7
samba4-test-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

i386
libtalloc-debuginfo-2.1.5-1.el6_7
ipa-admintools-3.0.0-47.el6_7.2
libldb-debuginfo-1.1.25-2.el6_7
libldb-devel-1.1.25-2.el6_7
samba4-winbind-clients-4.2.10-6.el6_7
ipa-server-3.0.0-47.el6_7.2
ipa-python-3.0.0-47.el6_7.2
ipa-client-3.0.0-47.el6_7.2
libtevent-0.9.26-2.el6_7
samba4-debuginfo-4.2.10-6.el6_7
python-tevent-0.9.26-2.el6_7
libtdb-debuginfo-1.3.8-1.el6_7
ipa-server-selinux-3.0.0-47.el6_7.2
ipa-server-trust-ad-3.0.0-47.el6_7.2
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
libtdb-devel-1.3.8-1.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
ipa-debuginfo-3.0.0-47.el6_7.2
samba4-dc-4.2.10-6.el6_7
samba4-common-4.2.10-6.el6_7
openchange-1.0-7.el6_7
samba4-libs-4.2.10-6.el6_7
libtalloc-devel-2.1.5-1.el6_7
libtevent-debuginfo-0.9.26-2.el6_7
samba4-client-4.2.10-6.el6_7
openchange-debuginfo-1.0-7.el6_7
libldb-1.1.25-2.el6_7
samba4-devel-4.2.10-6.el6_7
samba4-test-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

RHEL7D
x86_64
libtdb-1.3.8-1.el7_2
ipa-server-trust-ad-4.2.0-15.el7_2.6.1
samba-winbind-clients-4.2.10-6.el7_2

libtevent-debuginfo-0.9.26-1.el7_2
samba-test-libs-4.2.10-6.el7_2
samba-client-libs-4.2.10-6.el7_2
python-tevent-0.9.26-1.el7_2
openchange-devel-2.0-10.el7_2
samba-dc-libs-4.2.10-6.el7_2
pyldb-devel-1.1.25-1.el7_2
samba-debuginfo-4.2.10-6.el7_2
libtevent-0.9.26-1.el7_2
libldb-devel-1.1.25-1.el7_2
libsmbclient-4.2.10-6.el7_2
libsmbclient-devel-4.2.10-6.el7_2
ipa-server-dns-4.2.0-15.el7_2.6.1
samba-client-4.2.10-6.el7_2
pytalloc-2.1.5-1.el7_2
libtalloc-2.1.5-1.el7_2
pyldb-1.1.25-1.el7_2
libtdb-debuginfo-1.3.8-1.el7_2
openchange-debuginfo-2.0-10.el7_2
samba-4.2.10-6.el7_2
libtalloc-devel-2.1.5-1.el7_2
samba-common-libs-4.2.10-6.el7_2
pytalloc-devel-2.1.5-1.el7_2
ipa-debuginfo-4.2.0-15.el7_2.6.1
libldb-1.1.25-1.el7_2
ipa-client-4.2.0-15.el7_2.6.1
tdb-tools-1.3.8-1.el7_2
samba-common-tools-4.2.10-6.el7_2
openchange-2.0-10.el7_2
samba-devel-4.2.10-6.el7_2
libtdb-devel-1.3.8-1.el7_2
samba-dc-4.2.10-6.el7_2
libwbclient-4.2.10-6.el7_2
samba-winbind-modules-4.2.10-6.el7_2
libtalloc-debuginfo-2.1.5-1.el7_2
samba-test-4.2.10-6.el7_2
ipa-python-4.2.0-15.el7_2.6.1
samba-vfs-glusterfs-4.2.10-6.el7_2
samba-test-devel-4.2.10-6.el7_2
ldb-tools-1.1.25-1.el7_2
python-tdb-1.3.8-1.el7_2
samba-winbind-krb5-locator-4.2.10-6.el7_2
libwbclient-devel-4.2.10-6.el7_2
samba-libs-4.2.10-6.el7_2
ipa-admintools-4.2.0-15.el7_2.6.1
samba-winbind-4.2.10-6.el7_2
samba-python-4.2.10-6.el7_2
ipa-server-4.2.0-15.el7_2.6.1
libtevent-devel-0.9.26-1.el7_2
libldb-debuginfo-1.1.25-1.el7_2
openchange-client-2.0-10.el7_2

RHEL6D
x86_64
ipa-server-selinux-3.0.0-47.el6_7.2

RHEL7WS
x86_64
libtdb-1.3.8-1.el7_2

141159 - Red Hat Enterprise Linux RHSA-2016-0620 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
RHSA-2016-0620

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0620.html

RHEL6_2S
x86_64
samba4-pidl-4.2.10-6.el6_2
openchange-devel-docs-1.0-1.el6_2
libipa_hbac-devel-1.5.1-66.el6_2.5
openchange-client-1.0-1.el6_2
evolution-mapi-0.28.3-8.el6_2
samba4-debuginfo-4.2.10-6.el6_2
samba4-devel-4.2.10-6.el6_2
libldb-debuginfo-1.1.25-2.el6_2
ldb-tools-1.1.25-2.el6_2
pyldb-devel-1.1.25-2.el6_2
openchange-1.0-1.el6_2
samba4-libs-4.2.10-6.el6_2
evolution-mapi-devel-0.28.3-8.el6_2
libldb-devel-1.1.25-2.el6_2
evolution-mapi-debuginfo-0.28.3-8.el6_2
sssd-debuginfo-1.5.1-66.el6_2.5
openchange-devel-1.0-1.el6_2
openchange-debuginfo-1.0-1.el6_2
sssd-tools-1.5.1-66.el6_2.5
samba4-4.2.10-6.el6_2

RHEL6_6S
i386
samba4-devel-4.2.10-6.el6_6
samba4-libs-4.2.10-6.el6_6
samba4-dc-4.2.10-6.el6_6
ipa-debuginfo-3.0.0-42.el6_6.1
ipa-admintools-3.0.0-42.el6_6.1
libldb-1.1.25-2.el6_6
ipa-server-trust-ad-3.0.0-42.el6_6.1
samba4-dc-libs-4.2.10-6.el6_6
samba4-client-4.2.10-6.el6_6
samba4-debuginfo-4.2.10-6.el6_6
libldb-debuginfo-1.1.25-2.el6_6
samba4-winbind-krb5-locator-4.2.10-6.el6_6
pyldb-1.1.25-2.el6_6
samba4-winbind-clients-4.2.10-6.el6_6
ipa-python-3.0.0-42.el6_6.1
samba4-test-4.2.10-6.el6_6
ipa-server-selinux-3.0.0-42.el6_6.1

libldb-devel-1.1.25-2.el6_6
samba4-4.2.10-6.el6_6
samba4-common-4.2.10-6.el6_6
samba4-winbind-4.2.10-6.el6_6
ipa-client-3.0.0-42.el6_6.1
samba4-python-4.2.10-6.el6_6
ipa-server-3.0.0-42.el6_6.1
samba4-pidl-4.2.10-6.el6_6

x86_64
samba4-devel-4.2.10-6.el6_6
samba4-libs-4.2.10-6.el6_6
samba4-dc-4.2.10-6.el6_6
ipa-debuginfo-3.0.0-42.el6_6.1
ipa-admintools-3.0.0-42.el6_6.1
libldb-1.1.25-2.el6_6
ipa-server-trust-ad-3.0.0-42.el6_6.1
samba4-dc-libs-4.2.10-6.el6_6
samba4-client-4.2.10-6.el6_6
samba4-debuginfo-4.2.10-6.el6_6
libldb-debuginfo-1.1.25-2.el6_6
samba4-winbind-krb5-locator-4.2.10-6.el6_6
pyldb-1.1.25-2.el6_6
samba4-winbind-clients-4.2.10-6.el6_6
ipa-python-3.0.0-42.el6_6.1
samba4-test-4.2.10-6.el6_6
ipa-server-selinux-3.0.0-42.el6_6.1
libldb-devel-1.1.25-2.el6_6
samba4-4.2.10-6.el6_6
samba4-common-4.2.10-6.el6_6
samba4-winbind-4.2.10-6.el6_6
ipa-client-3.0.0-42.el6_6.1
samba4-python-4.2.10-6.el6_6
ipa-server-3.0.0-42.el6_6.1
samba4-pidl-4.2.10-6.el6_6

144520 - SuSE Linux 13.2 openSUSE-SU-2016:0971-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0636

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:0971-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-04/msg00014.html

SuSE Linux 13.2
i586
java-1_7_0-openjdk-headless-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-accessibility-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.99-19.1

java-1_7_0-openjdk-src-1.7.0.99-19.1
java-1_7_0-openjdk-demo-1.7.0.99-19.1
java-1_7_0-openjdk-devel-1.7.0.99-19.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.99-19.1
java-1_7_0-openjdk-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-headless-1.7.0.99-19.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.99-19.1
java-1_7_0-openjdk-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.99-19.1
java-1_7_0-openjdk-debugsource-1.7.0.99-19.1

noarch
java-1_7_0-openjdk-javadoc-1.7.0.99-19.1

x86_64
java-1_7_0-openjdk-headless-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-accessibility-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-src-1.7.0.99-19.1
java-1_7_0-openjdk-demo-1.7.0.99-19.1
java-1_7_0-openjdk-devel-1.7.0.99-19.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.99-19.1
java-1_7_0-openjdk-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-headless-1.7.0.99-19.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.99-19.1
java-1_7_0-openjdk-1.7.0.99-19.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.99-19.1
java-1_7_0-openjdk-debugsource-1.7.0.99-19.1

144524 - SuSE Linux 13.2 openSUSE-SU-2016:0983-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0636

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:0983-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-04/msg00016.html

SuSE Linux 13.2
i586
java-1_8_0-openjdk-demo-debuginfo-1.8.0.77-24.1
java-1_8_0-openjdk-demo-1.8.0.77-24.1

java-1_8_0-openjdk-headless-1.8.0.77-24.1
java-1_8_0-openjdk-src-1.8.0.77-24.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.77-24.1
java-1_8_0-openjdk-devel-1.8.0.77-24.1
java-1_8_0-openjdk-accessibility-1.8.0.77-24.1
java-1_8_0-openjdk-debuginfo-1.8.0.77-24.1
java-1_8_0-openjdk-1.8.0.77-24.1
java-1_8_0-openjdk-debugsource-1.8.0.77-24.1

noarch
java-1_8_0-openjdk-javadoc-1.8.0.77-24.1

x86_64
java-1_8_0-openjdk-demo-debuginfo-1.8.0.77-24.1
java-1_8_0-openjdk-demo-1.8.0.77-24.1
java-1_8_0-openjdk-headless-1.8.0.77-24.1
java-1_8_0-openjdk-src-1.8.0.77-24.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.77-24.1
java-1_8_0-openjdk-devel-1.8.0.77-24.1
java-1_8_0-openjdk-accessibility-1.8.0.77-24.1
java-1_8_0-openjdk-debuginfo-1.8.0.77-24.1
java-1_8_0-openjdk-1.8.0.77-24.1
java-1_8_0-openjdk-debugsource-1.8.0.77-24.1

160083 - CentOS 5 CESA-2016-0613 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
CESA-2016-0613

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-April/021821.html

CentOS 5
x86_64
samba3x-doc-3.6.23-12.el5_11
samba3x-winbind-devel-3.6.23-12.el5_11
samba3x-domainjoin-gui-3.6.23-12.el5_11
samba3x-swat-3.6.23-12.el5_11
samba3x-winbind-3.6.23-12.el5_11
samba3x-3.6.23-12.el5_11
samba3x-common-3.6.23-12.el5_11
samba3x-client-3.6.23-12.el5_11

i386
samba3x-doc-3.6.23-12.el5_11
samba3x-winbind-devel-3.6.23-12.el5_11
samba3x-domainjoin-gui-3.6.23-12.el5_11
samba3x-swat-3.6.23-12.el5_11
samba3x-winbind-3.6.23-12.el5_11
samba3x-3.6.23-12.el5_11

samba3x-common-3.6.23-12.el5_11
samba3x-client-3.6.23-12.el5_11

160084 - CentOS 6 CESA-2016-0611 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
CESA-2016-0611

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-April/021815.html

CentOS 6
x86_64
samba-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-winbind-krb5-locator-3.6.23-30.el6_7
samba-swat-3.6.23-30.el6_7
samba-glusterfs-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
libsmbclient-devel-3.6.23-30.el6_7
samba-winbind-devel-3.6.23-30.el6_7
samba-doc-3.6.23-30.el6_7
samba-common-3.6.23-30.el6_7
samba-domainjoin-gui-3.6.23-30.el6_7

i686
samba-common-3.6.23-30.el6_7
samba-swat-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-3.6.23-30.el6_7
samba-doc-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
samba-winbind-krb5-locator-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
samba-winbind-devel-3.6.23-30.el6_7
libsmbclient-devel-3.6.23-30.el6_7
samba-domainjoin-gui-3.6.23-30.el6_7

160086 - CentOS 6, 7 CESA-2016-0612 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
CESA-2016-0612

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-April/021820.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021816.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021827.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021825.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021818.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021829.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021817.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021822.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021819.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021824.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021828.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021814.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021830.html
http://lists.centos.org/pipermail/centos-announce/2016-April/021826.html

CentOS 7
i686
pyldb-devel-1.1.25-1.el7_2
python-tdb-1.3.8-1.el7_2
samba-devel-4.2.10-6.el7_2
libtalloc-2.1.5-1.el7_2
libtevent-0.9.26-1.el7_2
samba-libs-4.2.10-6.el7_2
pyldb-1.1.25-1.el7_2
libwbclient-devel-4.2.10-6.el7_2
samba-test-libs-4.2.10-6.el7_2
openchange-2.0-10.el7_2
pytalloc-2.1.5-1.el7_2
ctdb-devel-4.2.10-6.el7_2
libsmbclient-devel-4.2.10-6.el7_2
libsmbclient-4.2.10-6.el7_2
libtdb-1.3.8-1.el7_2
libtalloc-devel-2.1.5-1.el7_2
libwbclient-4.2.10-6.el7_2
libldb-devel-1.1.25-1.el7_2
libtdb-devel-1.3.8-1.el7_2
samba-client-libs-4.2.10-6.el7_2
libtevent-devel-0.9.26-1.el7_2
openchange-devel-2.0-10.el7_2
samba-winbind-modules-4.2.10-6.el7_2
pytalloc-devel-2.1.5-1.el7_2
libldb-1.1.25-1.el7_2

noarch
samba-pidl-4.2.10-6.el7_2
openchange-devel-docs-2.0-10.el7_2
samba-common-4.2.10-6.el7_2

x86_64
libwbclient-4.2.10-6.el7_2
python-tevent-0.9.26-1.el7_2
samba-winbind-clients-4.2.10-6.el7_2
samba-client-libs-4.2.10-6.el7_2

openchange-client-2.0-10.el7_2
openchange-devel-2.0-10.el7_2
ctdb-tests-4.2.10-6.el7_2
samba-dc-libs-4.2.10-6.el7_2
pyldb-devel-1.1.25-1.el7_2
samba-test-libs-4.2.10-6.el7_2
ipa-admintools-4.2.0-15.0.1.el7.centos.6.1
libtevent-0.9.26-1.el7_2
ipa-server-dns-4.2.0-15.0.1.el7.centos.6.1
libldb-devel-1.1.25-1.el7_2
libsmbclient-4.2.10-6.el7_2
samba-winbind-4.2.10-6.el7_2
samba-vfs-glusterfs-4.2.10-6.el7_2
samba-client-4.2.10-6.el7_2
pytalloc-2.1.5-1.el7_2
libtalloc-2.1.5-1.el7_2
pyldb-1.1.25-1.el7_2
libtalloc-devel-2.1.5-1.el7_2
samba-common-libs-4.2.10-6.el7_2
libsmbclient-devel-4.2.10-6.el7_2
libldb-1.1.25-1.el7_2
ctdb-devel-4.2.10-6.el7_2
samba-common-tools-4.2.10-6.el7_2
tdb-tools-1.3.8-1.el7_2
openchange-2.0-10.el7_2
ctdb-4.2.10-6.el7_2
samba-devel-4.2.10-6.el7_2
libtdb-devel-1.3.8-1.el7_2
samba-dc-4.2.10-6.el7_2
ipa-server-trust-ad-4.2.0-15.0.1.el7.centos.6.1
ipa-server-4.2.0-15.0.1.el7.centos.6.1
pytalloc-devel-2.1.5-1.el7_2
samba-winbind-modules-4.2.10-6.el7_2
samba-test-4.2.10-6.el7_2
libtdb-1.3.8-1.el7_2
ipa-client-4.2.0-15.0.1.el7.centos.6.1
ldb-tools-1.1.25-1.el7_2
python-tdb-1.3.8-1.el7_2
samba-winbind-krb5-locator-4.2.10-6.el7_2
libwbclient-devel-4.2.10-6.el7_2
ipa-python-4.2.0-15.0.1.el7.centos.6.1
samba-test-devel-4.2.10-6.el7_2
samba-libs-4.2.10-6.el7_2
samba-python-4.2.10-6.el7_2
libtevent-devel-0.9.26-1.el7_2
samba-4.2.10-6.el7_2

CentOS 6
x86_64
samba4-client-4.2.10-6.el6_7
libtevent-0.9.26-2.el6_7
ipa-client-3.0.0-47.el6.centos.2
libldb-devel-1.1.25-2.el6_7
samba4-winbind-clients-4.2.10-6.el6_7
libldb-1.1.25-2.el6_7
samba4-libs-4.2.10-6.el6_7
samba4-common-4.2.10-6.el6_7
libtdb-devel-1.3.8-1.el6_7
openchange-devel-docs-1.0-7.el6_7
python-tevent-0.9.26-2.el6_7

ipa-server-trust-ad-3.0.0-47.el6.centos.2
openchange-client-1.0-7.el6_7
ldb-tools-1.1.25-2.el6_7
pytalloc-devel-2.1.5-1.el6_7
pyldb-devel-1.1.25-2.el6_7
samba4-test-4.2.10-6.el6_7
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
ipa-admintools-3.0.0-47.el6.centos.2
ipa-python-3.0.0-47.el6.centos.2
ipa-server-selinux-3.0.0-47.el6.centos.2
ipa-server-3.0.0-47.el6.centos.2
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
openchange-devel-1.0-7.el6_7
openchange-1.0-7.el6_7
libtalloc-devel-2.1.5-1.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
samba4-dc-4.2.10-6.el6_7
samba4-devel-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

i686
samba4-client-4.2.10-6.el6_7
libtevent-0.9.26-2.el6_7
ipa-client-3.0.0-47.el6.centos.2
libldb-devel-1.1.25-2.el6_7
samba4-winbind-clients-4.2.10-6.el6_7
libldb-1.1.25-2.el6_7
samba4-libs-4.2.10-6.el6_7
samba4-common-4.2.10-6.el6_7
libtdb-devel-1.3.8-1.el6_7
openchange-devel-docs-1.0-7.el6_7
python-tevent-0.9.26-2.el6_7
ipa-server-trust-ad-3.0.0-47.el6.centos.2
openchange-client-1.0-7.el6_7
ldb-tools-1.1.25-2.el6_7
pytalloc-devel-2.1.5-1.el6_7
pyldb-devel-1.1.25-2.el6_7
samba4-test-4.2.10-6.el6_7
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
ipa-admintools-3.0.0-47.el6.centos.2
ipa-python-3.0.0-47.el6.centos.2
ipa-server-selinux-3.0.0-47.el6.centos.2
ipa-server-3.0.0-47.el6.centos.2
libtalloc-2.1.5-1.el6_7

samba4-python-4.2.10-6.el6_7
openchange-devel-1.0-7.el6_7
openchange-1.0-7.el6_7
libtalloc-devel-2.1.5-1.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
samba4-dc-4.2.10-6.el6_7
samba4-devel-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

163059 - Oracle Enterprise Linux ELSA-2016-0613 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
ELSA-2016-0613

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-April/005949.html

OEL5
i386
samba3x-swat-3.6.23-12.0.1.el5_11
samba3x-doc-3.6.23-12.0.1.el5_11
samba3x-winbind-devel-3.6.23-12.0.1.el5_11
samba3x-domainjoin-gui-3.6.23-12.0.1.el5_11
samba3x-common-3.6.23-12.0.1.el5_11
samba3x-3.6.23-12.0.1.el5_11
samba3x-winbind-3.6.23-12.0.1.el5_11
samba3x-client-3.6.23-12.0.1.el5_11

x86_64
samba3x-swat-3.6.23-12.0.1.el5_11
samba3x-doc-3.6.23-12.0.1.el5_11
samba3x-winbind-devel-3.6.23-12.0.1.el5_11
samba3x-domainjoin-gui-3.6.23-12.0.1.el5_11
samba3x-common-3.6.23-12.0.1.el5_11
samba3x-3.6.23-12.0.1.el5_11
samba3x-winbind-3.6.23-12.0.1.el5_11
samba3x-client-3.6.23-12.0.1.el5_11

163060 - Oracle Enterprise Linux ELSA-2016-0612 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

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

ELSA-2016-0612

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-April/005946.html
http://oss.oracle.com/pipermail/el-errata/2016-April/005947.html

OEL7
x86_64
ipa-server-dns-4.2.0-15.0.1.el7_2.6.1
libtdb-1.3.8-1.el7_2
python-tevent-0.9.26-1.el7_2
samba-winbind-clients-4.2.10-6.el7_2
samba-client-libs-4.2.10-6.el7_2
openchange-devel-2.0-10.el7_2
samba-dc-libs-4.2.10-6.el7_2
pyldb-devel-1.1.25-1.el7_2
samba-test-libs-4.2.10-6.el7_2
libtevent-0.9.26-1.el7_2
libldb-devel-1.1.25-1.el7_2
libsmbclient-4.2.10-6.el7_2
samba-winbind-4.2.10-6.el7_2
samba-vfs-glusterfs-4.2.10-6.el7_2
samba-client-4.2.10-6.el7_2
pytalloc-2.1.5-1.el7_2
libtalloc-2.1.5-1.el7_2
pyldb-1.1.25-1.el7_2
ipa-server-trust-ad-4.2.0-15.0.1.el7_2.6.1
samba-pidl-4.2.10-6.el7_2
samba-4.2.10-6.el7_2
libtalloc-devel-2.1.5-1.el7_2
samba-common-libs-4.2.10-6.el7_2
ipa-server-4.2.0-15.0.1.el7_2.6.1
pytalloc-devel-2.1.5-1.el7_2
libsmbclient-devel-4.2.10-6.el7_2
libldb-1.1.25-1.el7_2
samba-common-tools-4.2.10-6.el7_2
tdb-tools-1.3.8-1.el7_2
ipa-python-4.2.0-15.0.1.el7_2.6.1
openchange-2.0-10.el7_2
openchange-devel-docs-2.0-10.el7_2
libtdb-devel-1.3.8-1.el7_2
samba-dc-4.2.10-6.el7_2
libwbclient-4.2.10-6.el7_2
samba-winbind-modules-4.2.10-6.el7_2
samba-test-4.2.10-6.el7_2
ipa-admintools-4.2.0-15.0.1.el7_2.6.1
ipa-client-4.2.0-15.0.1.el7_2.6.1
samba-test-devel-4.2.10-6.el7_2
ldb-tools-1.1.25-1.el7_2
python-tdb-1.3.8-1.el7_2
samba-winbind-krb5-locator-4.2.10-6.el7_2
libwbclient-devel-4.2.10-6.el7_2
samba-common-4.2.10-6.el7_2
samba-libs-4.2.10-6.el7_2
samba-python-4.2.10-6.el7_2
libtevent-devel-0.9.26-1.el7_2
samba-devel-4.2.10-6.el7_2

openchange-client-2.0-10.el7_2

OEL6
x86_64
ipa-admintools-3.0.0-47.el6_7.2
libtevent-0.9.26-2.el6_7
samba4-libs-4.2.10-6.el6_7
libldb-devel-1.1.25-2.el6_7
samba4-winbind-clients-4.2.10-6.el6_7
ipa-server-3.0.0-47.el6_7.2
samba4-common-4.2.10-6.el6_7
ipa-python-3.0.0-47.el6_7.2
ipa-client-3.0.0-47.el6_7.2
openchange-devel-docs-1.0-7.el6_7
python-tevent-0.9.26-2.el6_7
openchange-client-1.0-7.el6_7
pytalloc-devel-2.1.5-1.el6_7
pyldb-devel-1.1.25-2.el6_7
ipa-server-selinux-3.0.0-47.el6_7.2
ipa-server-trust-ad-3.0.0-47.el6_7.2
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
libtdb-devel-1.3.8-1.el6_7
samba4-devel-4.2.10-6.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
samba4-dc-4.2.10-6.el6_7
openchange-devel-1.0-7.el6_7
openchange-1.0-7.el6_7
libtalloc-devel-2.1.5-1.el6_7
samba4-client-4.2.10-6.el6_7
libldb-1.1.25-2.el6_7
ldb-tools-1.1.25-2.el6_7
samba4-test-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

i386
ipa-admintools-3.0.0-47.el6_7.2
libtevent-0.9.26-2.el6_7
samba4-libs-4.2.10-6.el6_7
libldb-devel-1.1.25-2.el6_7
samba4-winbind-clients-4.2.10-6.el6_7
ipa-server-3.0.0-47.el6_7.2
samba4-common-4.2.10-6.el6_7
ipa-python-3.0.0-47.el6_7.2
ipa-client-3.0.0-47.el6_7.2
openchange-devel-docs-1.0-7.el6_7
python-tevent-0.9.26-2.el6_7
openchange-client-1.0-7.el6_7
pytalloc-devel-2.1.5-1.el6_7
pyldb-devel-1.1.25-2.el6_7
ipa-server-selinux-3.0.0-47.el6_7.2

ipa-server-trust-ad-3.0.0-47.el6_7.2
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
libtdb-devel-1.3.8-1.el6_7
samba4-devel-4.2.10-6.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
samba4-dc-4.2.10-6.el6_7
openchange-devel-1.0-7.el6_7
openchange-1.0-7.el6_7
libtalloc-devel-2.1.5-1.el6_7
samba4-client-4.2.10-6.el6_7
libldb-1.1.25-2.el6_7
ldb-tools-1.1.25-2.el6_7
samba4-test-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

163062 - Oracle Enterprise Linux ELSA-2016-0611 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
ELSA-2016-0611

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-April/005948.html

OEL6
x86_64
libsmbclient-devel-3.6.23-30.0.1.el6_7
samba-glusterfs-3.6.23-30.0.1.el6_7
samba-winbind-3.6.23-30.0.1.el6_7
samba-common-3.6.23-30.0.1.el6_7
samba-winbind-devel-3.6.23-30.0.1.el6_7
samba-domainjoin-gui-3.6.23-30.0.1.el6_7
samba-doc-3.6.23-30.0.1.el6_7
libsmbclient-3.6.23-30.0.1.el6_7
samba-swat-3.6.23-30.0.1.el6_7
samba-winbind-krb5-locator-3.6.23-30.0.1.el6_7
samba-winbind-clients-3.6.23-30.0.1.el6_7
samba-client-3.6.23-30.0.1.el6_7
samba-3.6.23-30.0.1.el6_7

i386

samba-winbind-devel-3.6.23-30.0.1.el6_7
samba-swat-3.6.23-30.0.1.el6_7
samba-winbind-3.6.23-30.0.1.el6_7
samba-common-3.6.23-30.0.1.el6_7
samba-domainjoin-gui-3.6.23-30.0.1.el6_7
samba-client-3.6.23-30.0.1.el6_7
samba-winbind-clients-3.6.23-30.0.1.el6_7
samba-3.6.23-30.0.1.el6_7
samba-doc-3.6.23-30.0.1.el6_7
samba-winbind-krb5-locator-3.6.23-30.0.1.el6_7
libsmbclient-3.6.23-30.0.1.el6_7
libsmbclient-devel-3.6.23-30.0.1.el6_7

174939 - Scientific Linux Security ERRATA Critical: samba on SL6.x i386/x86_64 (1604-7302)

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: samba on SL6.x i386/x86_64 (1604-7302)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=7302

SL6
x86_64
samba-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-winbind-krb5-locator-3.6.23-30.el6_7
samba-debuginfo-3.6.23-30.el6_7
samba-swat-3.6.23-30.el6_7
samba-glusterfs-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
libsmbclient-devel-3.6.23-30.el6_7
samba-winbind-devel-3.6.23-30.el6_7
samba-doc-3.6.23-30.el6_7
samba-common-3.6.23-30.el6_7
samba-domainjoin-gui-3.6.23-30.el6_7

i386
samba-3.6.23-30.el6_7
samba-winbind-clients-3.6.23-30.el6_7
samba-winbind-3.6.23-30.el6_7
samba-client-3.6.23-30.el6_7
samba-winbind-krb5-locator-3.6.23-30.el6_7
samba-debuginfo-3.6.23-30.el6_7
samba-swat-3.6.23-30.el6_7
libsmbclient-3.6.23-30.el6_7
libsmbclient-devel-3.6.23-30.el6_7
samba-winbind-devel-3.6.23-30.el6_7
samba-doc-3.6.23-30.el6_7

samba-common-3.6.23-30.el6_7
samba-domainjoin-gui-3.6.23-30.el6_7

174940 - Scientific Linux Security ERRATA Critical: samba3x on SL5.x i386/x86_64 (1604-6491)

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: samba3x on SL5.x i386/x86_64 (1604-6491)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=6491

SL5
x86_64
samba3x-debuginfo-3.6.23-12.el5_11
samba3x-doc-3.6.23-12.el5_11
samba3x-winbind-devel-3.6.23-12.el5_11
samba3x-domainjoin-gui-3.6.23-12.el5_11
samba3x-swat-3.6.23-12.el5_11
samba3x-winbind-3.6.23-12.el5_11
samba3x-3.6.23-12.el5_11
samba3x-common-3.6.23-12.el5_11
samba3x-client-3.6.23-12.el5_11

i386
samba3x-debuginfo-3.6.23-12.el5_11
samba3x-doc-3.6.23-12.el5_11
samba3x-winbind-devel-3.6.23-12.el5_11
samba3x-domainjoin-gui-3.6.23-12.el5_11
samba3x-swat-3.6.23-12.el5_11
samba3x-winbind-3.6.23-12.el5_11
samba3x-3.6.23-12.el5_11
samba3x-common-3.6.23-12.el5_11
samba3x-client-3.6.23-12.el5_11

174941 - Scientific Linux Security ERRATA Critical: samba and samba4 on SL6.x, SL7.x i386/x86_64 (1604-8117)

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: samba and samba4 on SL6.x, SL7.x i386/x86_64 (1604-8117)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=8117

SL7
x86_64
libtdb-1.3.8-1.el7_2
ipa-server-trust-ad-4.2.0-15.el7_2.6.1
samba-winbind-clients-4.2.10-6.el7_2
libtevent-debuginfo-0.9.26-1.el7_2
samba-test-libs-4.2.10-6.el7_2
samba-client-libs-4.2.10-6.el7_2
python-tevent-0.9.26-1.el7_2
openchange-devel-2.0-10.el7_2
samba-dc-libs-4.2.10-6.el7_2
pyldb-devel-1.1.25-1.el7_2
samba-debuginfo-4.2.10-6.el7_2
libtevent-0.9.26-1.el7_2
libldb-devel-1.1.25-1.el7_2
libsmbclient-4.2.10-6.el7_2
libsmbclient-devel-4.2.10-6.el7_2
ipa-server-dns-4.2.0-15.el7_2.6.1
samba-client-4.2.10-6.el7_2
pytalloc-2.1.5-1.el7_2
libtalloc-2.1.5-1.el7_2
pyldb-1.1.25-1.el7_2
libtdb-debuginfo-1.3.8-1.el7_2
openchange-debuginfo-2.0-10.el7_2
samba-4.2.10-6.el7_2
libtalloc-devel-2.1.5-1.el7_2
samba-common-libs-4.2.10-6.el7_2
pytalloc-devel-2.1.5-1.el7_2
ipa-debuginfo-4.2.0-15.el7_2.6.1
libldb-1.1.25-1.el7_2
ipa-client-4.2.0-15.el7_2.6.1
tdb-tools-1.3.8-1.el7_2
samba-common-tools-4.2.10-6.el7_2
openchange-2.0-10.el7_2
samba-devel-4.2.10-6.el7_2
libtdb-devel-1.3.8-1.el7_2
samba-dc-4.2.10-6.el7_2
libwbclient-4.2.10-6.el7_2
samba-winbind-modules-4.2.10-6.el7_2
libtalloc-debuginfo-2.1.5-1.el7_2
samba-test-4.2.10-6.el7_2
ipa-python-4.2.0-15.el7_2.6.1
samba-vfs-glusterfs-4.2.10-6.el7_2
samba-test-devel-4.2.10-6.el7_2
ldb-tools-1.1.25-1.el7_2
python-tdb-1.3.8-1.el7_2
samba-winbind-krb5-locator-4.2.10-6.el7_2
libwbclient-devel-4.2.10-6.el7_2
samba-libs-4.2.10-6.el7_2
ipa-admintools-4.2.0-15.el7_2.6.1
samba-winbind-4.2.10-6.el7_2
samba-python-4.2.10-6.el7_2
ipa-server-4.2.0-15.el7_2.6.1
libtevent-devel-0.9.26-1.el7_2
libldb-debuginfo-1.1.25-1.el7_2
openchange-client-2.0-10.el7_2

noarch

samba-pidl-4.2.10-6.el7_2
openchange-devel-docs-2.0-10.el7_2
samba-common-4.2.10-6.el7_2

SL6
x86_64
ipa-server-selinux-3.0.0-47.el6_7.2
libtalloc-debuginfo-2.1.5-1.el6_7
samba4-client-4.2.10-6.el6_7
openchange-devel-1.0-7.el6_7
libldb-debuginfo-1.1.25-2.el6_7
libldb-devel-1.1.25-2.el6_7
samba4-winbind-clients-4.2.10-6.el6_7
samba4-libs-4.2.10-6.el6_7
ipa-python-3.0.0-47.el6_7.2
ipa-client-3.0.0-47.el6_7.2
libtevent-0.9.26-2.el6_7
samba4-debuginfo-4.2.10-6.el6_7
python-tevent-0.9.26-2.el6_7
libtdb-debuginfo-1.3.8-1.el6_7
ipa-admintools-3.0.0-47.el6_7.2
openchange-client-1.0-7.el6_7
ldb-tools-1.1.25-2.el6_7
pytalloc-devel-2.1.5-1.el6_7
pyldb-devel-1.1.25-2.el6_7
ipa-server-3.0.0-47.el6_7.2
libldb-1.1.25-2.el6_7
ipa-server-trust-ad-3.0.0-47.el6_7.2
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
openchange-devel-docs-1.0-7.el6_7
libtdb-devel-1.3.8-1.el6_7
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
ipa-debuginfo-3.0.0-47.el6_7.2
samba4-common-4.2.10-6.el6_7
openchange-1.0-7.el6_7
libtalloc-devel-2.1.5-1.el6_7
libtevent-debuginfo-0.9.26-2.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
openchange-debuginfo-1.0-7.el6_7
samba4-dc-4.2.10-6.el6_7
samba4-devel-4.2.10-6.el6_7
samba4-test-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

i386
ipa-server-selinux-3.0.0-47.el6_7.2
libtalloc-debuginfo-2.1.5-1.el6_7
samba4-client-4.2.10-6.el6_7
openchange-devel-1.0-7.el6_7
libldb-debuginfo-1.1.25-2.el6_7
libldb-devel-1.1.25-2.el6_7

samba4-winbind-clients-4.2.10-6.el6_7
samba4-libs-4.2.10-6.el6_7
ipa-python-3.0.0-47.el6_7.2
ipa-client-3.0.0-47.el6_7.2
libtevent-0.9.26-2.el6_7
samba4-debuginfo-4.2.10-6.el6_7
python-tevent-0.9.26-2.el6_7
libtdb-debuginfo-1.3.8-1.el6_7
ipa-admintools-3.0.0-47.el6_7.2
openchange-client-1.0-7.el6_7
ldb-tools-1.1.25-2.el6_7
pytalloc-devel-2.1.5-1.el6_7
pyldb-devel-1.1.25-2.el6_7
ipa-server-3.0.0-47.el6_7.2
libldb-1.1.25-2.el6_7
ipa-server-trust-ad-3.0.0-47.el6_7.2
tdb-tools-1.3.8-1.el6_7
libtdb-1.3.8-1.el6_7
libtevent-devel-0.9.26-2.el6_7
samba4-dc-libs-4.2.10-6.el6_7
samba4-4.2.10-6.el6_7
pytalloc-2.1.5-1.el6_7
pyldb-1.1.25-2.el6_7
samba4-pidl-4.2.10-6.el6_7
openchange-devel-docs-1.0-7.el6_7
libtdb-devel-1.3.8-1.el6_7
libtalloc-2.1.5-1.el6_7
samba4-python-4.2.10-6.el6_7
ipa-debuginfo-3.0.0-47.el6_7.2
samba4-common-4.2.10-6.el6_7
openchange-1.0-7.el6_7
libtalloc-devel-2.1.5-1.el6_7
libtevent-debuginfo-0.9.26-2.el6_7
samba4-winbind-krb5-locator-4.2.10-6.el6_7
openchange-debuginfo-1.0-7.el6_7
samba4-dc-4.2.10-6.el6_7
samba4-devel-4.2.10-6.el6_7
samba4-test-4.2.10-6.el6_7
python-tdb-1.3.8-1.el6_7
samba4-winbind-4.2.10-6.el6_7

174943 - Scientific Linux Security ERRATA Important: graphite2 on SL7.x x86_64 (1604-6103)

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

Risk Level: High

CVE: CVE-2016-1521, CVE-2016-1522, CVE-2016-1523, CVE-2016-1526

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: graphite2 on SL7.x x86_64 (1604-6103)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=6103

SL7

x86_64
graphite2-debuginfo-1.3.6-1.el7_2
graphite2-1.3.6-1.el7_2
graphite2-devel-1.3.6-1.el7_2

130465 - Debian Linux 8.0 DSA-3545-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1899, CVE-2016-1900, CVE-2016-1901

Description

The scan detected that the host is missing the following update:
DSA-3545-1

Observation

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

http://www.debian.org/security/2016/dsa-3545

Debian 8.0
all
cgit_0.10.2.git2.0.1-3+deb8u1

141153 - Red Hat Enterprise Linux RHSA-2016-0617 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1805, CVE-2016-0774

Description

The scan detected that the host is missing the following update:
RHSA-2016-0617

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0617.html

RHEL6_6S
i386
kernel-debuginfo-common-i686-2.6.32-504.46.1.el6
kernel-headers-2.6.32-504.46.1.el6
perf-2.6.32-504.46.1.el6
perf-debuginfo-2.6.32-504.46.1.el6
python-perf-debuginfo-2.6.32-504.46.1.el6
kernel-2.6.32-504.46.1.el6
kernel-debug-debuginfo-2.6.32-504.46.1.el6
kernel-devel-2.6.32-504.46.1.el6
kernel-debuginfo-2.6.32-504.46.1.el6
kernel-debug-devel-2.6.32-504.46.1.el6
kernel-debug-2.6.32-504.46.1.el6

noarch

kernel-firmware-2.6.32-504.46.1.el6
kernel-doc-2.6.32-504.46.1.el6
kernel-abi-whitelists-2.6.32-504.46.1.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-504.46.1.el6
kernel-headers-2.6.32-504.46.1.el6
perf-2.6.32-504.46.1.el6
perf-debuginfo-2.6.32-504.46.1.el6
kernel-debuginfo-common-x86_64-2.6.32-504.46.1.el6
python-perf-debuginfo-2.6.32-504.46.1.el6
kernel-2.6.32-504.46.1.el6
kernel-debug-debuginfo-2.6.32-504.46.1.el6
kernel-devel-2.6.32-504.46.1.el6
kernel-debuginfo-2.6.32-504.46.1.el6
kernel-debug-devel-2.6.32-504.46.1.el6
kernel-debug-2.6.32-504.46.1.el6

141155 - Red Hat Enterprise Linux RHSA-2016-0621 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
RHSA-2016-0621

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0621.html

RHEL5D
x86_64
samba-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
samba-debuginfo-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

i386
samba-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
samba-debuginfo-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

RHEL5S
i386
samba-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
libsmbclient-devel-3.0.33-3.41.el5_11
samba-debuginfo-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11

libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

x86_64
samba-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
libsmbclient-devel-3.0.33-3.41.el5_11
samba-debuginfo-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

141156 - Red Hat Enterprise Linux RHSA-2016-0625 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
RHSA-2016-0625

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0625.html

RHEL4ES
x86_64
samba-swat-3.0.33-3.37.el4
samba-debuginfo-3.0.33-3.37.el4
samba-3.0.33-3.37.el4
samba-client-3.0.33-3.37.el4
samba-common-3.0.33-3.37.el4

i386
samba-swat-3.0.33-3.37.el4
samba-debuginfo-3.0.33-3.37.el4
samba-3.0.33-3.37.el4
samba-client-3.0.33-3.37.el4
samba-common-3.0.33-3.37.el4

RHEL4AS
i386
samba-swat-3.0.33-3.37.el4
samba-debuginfo-3.0.33-3.37.el4
samba-3.0.33-3.37.el4
samba-client-3.0.33-3.37.el4
samba-common-3.0.33-3.37.el4

x86_64
samba-swat-3.0.33-3.37.el4
samba-debuginfo-3.0.33-3.37.el4
samba-3.0.33-3.37.el4
samba-client-3.0.33-3.37.el4
samba-common-3.0.33-3.37.el4

144517 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1024-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1024-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-April/001999.html

SuSE SLES 12 SP1
noarch
samba-doc-4.2.4-16.1

x86_64
libsamba-credentials0-32bit-4.2.4-16.1
libsmbclient0-4.2.4-16.1
libsmbldap0-4.2.4-16.1
samba-libs-4.2.4-16.1
libndr-standard0-32bit-4.2.4-16.1
libtevent-util0-32bit-4.2.4-16.1
libsmbclient0-debuginfo-4.2.4-16.1
libndr0-4.2.4-16.1
samba-32bit-4.2.4-16.1
libsamba-credentials0-debuginfo-4.2.4-16.1
libnetapi0-debuginfo-4.2.4-16.1
libdcerpc-binding0-4.2.4-16.1
libsmbconf0-debuginfo-32bit-4.2.4-16.1
libdcerpc0-32bit-4.2.4-16.1
libsamba-util0-32bit-4.2.4-16.1
libgensec0-4.2.4-16.1
libndr-standard0-debuginfo-4.2.4-16.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-16.1
libdcerpc0-debuginfo-4.2.4-16.1
samba-winbind-32bit-4.2.4-16.1
libndr-krb5pac0-debuginfo-32bit-4.2.4-16.1
libsamdb0-4.2.4-16.1
libwbclient0-32bit-4.2.4-16.1
libsmbclient0-debuginfo-32bit-4.2.4-16.1
libsmbconf0-debuginfo-4.2.4-16.1
libnetapi0-debuginfo-32bit-4.2.4-16.1
libsamdb0-debuginfo-32bit-4.2.4-16.1
libndr0-debuginfo-4.2.4-16.1
samba-debuginfo-4.2.4-16.1
libsmbclient0-32bit-4.2.4-16.1
libsamba-passdb0-debuginfo-4.2.4-16.1
libsamba-util0-debuginfo-4.2.4-16.1
libregistry0-debuginfo-4.2.4-16.1
samba-client-32bit-4.2.4-16.1
libregistry0-4.2.4-16.1
libndr-krb5pac0-32bit-4.2.4-16.1
samba-winbind-debuginfo-32bit-4.2.4-16.1
samba-libs-32bit-4.2.4-16.1

libsmbconf0-4.2.4-16.1
libndr-nbt0-32bit-4.2.4-16.1
libdcerpc-binding0-debuginfo-4.2.4-16.1
libtevent-util0-4.2.4-16.1
libdcerpc0-debuginfo-32bit-4.2.4-16.1
libndr-krb5pac0-debuginfo-4.2.4-16.1
samba-libs-debuginfo-4.2.4-16.1
libsamba-hostconfig0-4.2.4-16.1
libsamba-hostconfig0-32bit-4.2.4-16.1
libsamba-hostconfig0-debuginfo-4.2.4-16.1
libtevent-util0-debuginfo-4.2.4-16.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-16.1
samba-client-4.2.4-16.1
libdcerpc0-4.2.4-16.1
libndr-standard0-4.2.4-16.1
samba-winbind-debuginfo-4.2.4-16.1
libsamba-credentials0-debuginfo-32bit-4.2.4-16.1
libsamba-util0-debuginfo-32bit-4.2.4-16.1
samba-debugsource-4.2.4-16.1
libgensec0-32bit-4.2.4-16.1
libsamdb0-32bit-4.2.4-16.1
libnetapi0-32bit-4.2.4-16.1
libgensec0-debuginfo-4.2.4-16.1
libsmbclient-raw0-debuginfo-4.2.4-16.1
libndr0-32bit-4.2.4-16.1
libndr-nbt0-debuginfo-32bit-4.2.4-16.1
libsamba-util0-4.2.4-16.1
libgensec0-debuginfo-32bit-4.2.4-16.1
libsmbldap0-debuginfo-4.2.4-16.1
libndr-nbt0-debuginfo-4.2.4-16.1
libnetapi0-4.2.4-16.1
libwbclient0-debuginfo-4.2.4-16.1
samba-client-debuginfo-4.2.4-16.1
libwbclient0-4.2.4-16.1
libndr-krb5pac0-4.2.4-16.1
libsmbclient-raw0-4.2.4-16.1
libndr-standard0-debuginfo-32bit-4.2.4-16.1
samba-winbind-4.2.4-16.1
libndr-nbt0-4.2.4-16.1
libsmbconf0-32bit-4.2.4-16.1
libsamba-passdb0-debuginfo-32bit-4.2.4-16.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-16.1
libdcerpc-binding0-32bit-4.2.4-16.1
libsamba-passdb0-32bit-4.2.4-16.1
samba-debuginfo-32bit-4.2.4-16.1
libsmbclient-raw0-32bit-4.2.4-16.1
libsamdb0-debuginfo-4.2.4-16.1
libsmbldap0-debuginfo-32bit-4.2.4-16.1
samba-libs-debuginfo-32bit-4.2.4-16.1
libsamba-credentials0-4.2.4-16.1
libndr0-debuginfo-32bit-4.2.4-16.1
libtevent-util0-debuginfo-32bit-4.2.4-16.1
samba-4.2.4-16.1
libsamba-passdb0-4.2.4-16.1
samba-client-debuginfo-32bit-4.2.4-16.1
libsmbldap0-32bit-4.2.4-16.1
libwbclient0-debuginfo-32bit-4.2.4-16.1

SuSE SLED 12 SP1
x86_64

libsamba-credentials0-32bit-4.2.4-16.1
libsmbclient0-4.2.4-16.1
libsmbldap0-4.2.4-16.1
libsamba-hostconfig0-32bit-4.2.4-16.1
libndr-standard0-32bit-4.2.4-16.1
libsmbclient0-debuginfo-4.2.4-16.1
samba-32bit-4.2.4-16.1
libsamba-credentials0-debuginfo-4.2.4-16.1
libnetapi0-debuginfo-4.2.4-16.1
libdcerpc-binding0-4.2.4-16.1
libsmbconf0-debuginfo-32bit-4.2.4-16.1
libdcerpc0-32bit-4.2.4-16.1
samba-client-debuginfo-4.2.4-16.1
libgensec0-4.2.4-16.1
libndr-standard0-debuginfo-4.2.4-16.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-16.1
libdcerpc0-debuginfo-4.2.4-16.1
samba-winbind-32bit-4.2.4-16.1
libndr-krb5pac0-debuginfo-32bit-4.2.4-16.1
libsamdb0-4.2.4-16.1
libwbclient0-32bit-4.2.4-16.1
libsmbconf0-debuginfo-4.2.4-16.1
libdcerpc0-4.2.4-16.1
libnetapi0-debuginfo-32bit-4.2.4-16.1
libsamdb0-debuginfo-32bit-4.2.4-16.1
libndr0-debuginfo-4.2.4-16.1
libsmbclient0-debuginfo-32bit-4.2.4-16.1
libsmbclient0-32bit-4.2.4-16.1
libsamba-passdb0-debuginfo-4.2.4-16.1
libsamba-util0-debuginfo-4.2.4-16.1
libregistry0-debuginfo-4.2.4-16.1
samba-client-32bit-4.2.4-16.1
libregistry0-4.2.4-16.1
libndr-krb5pac0-32bit-4.2.4-16.1
samba-winbind-debuginfo-32bit-4.2.4-16.1
libsmbconf0-4.2.4-16.1
libndr-nbt0-32bit-4.2.4-16.1
libdcerpc-binding0-debuginfo-4.2.4-16.1
libtevent-util0-4.2.4-16.1
samba-debuginfo-4.2.4-16.1
libdcerpc0-debuginfo-32bit-4.2.4-16.1
libndr-krb5pac0-debuginfo-4.2.4-16.1
libsamba-passdb0-32bit-4.2.4-16.1
samba-libs-debuginfo-4.2.4-16.1
libsamba-hostconfig0-4.2.4-16.1
libsamba-hostconfig0-debuginfo-4.2.4-16.1
samba-winbind-debuginfo-4.2.4-16.1
libtevent-util0-debuginfo-4.2.4-16.1
samba-libs-32bit-4.2.4-16.1
samba-client-4.2.4-16.1
libsmbldap0-32bit-4.2.4-16.1
libsmbclient-raw0-32bit-4.2.4-16.1
libndr0-4.2.4-16.1
libsamba-util0-debuginfo-32bit-4.2.4-16.1
samba-debugsource-4.2.4-16.1
libgensec0-32bit-4.2.4-16.1
libsamdb0-32bit-4.2.4-16.1
libnetapi0-32bit-4.2.4-16.1
libgensec0-debuginfo-4.2.4-16.1
libdcerpc-binding0-32bit-4.2.4-16.1

libsmbclient-raw0-debuginfo-4.2.4-16.1
libndr0-32bit-4.2.4-16.1
libndr-nbt0-debuginfo-32bit-4.2.4-16.1
libsamba-util0-4.2.4-16.1
libgensec0-debuginfo-32bit-4.2.4-16.1
libsmbldap0-debuginfo-4.2.4-16.1
libndr-nbt0-debuginfo-4.2.4-16.1
libnetapi0-4.2.4-16.1
libwbclient0-debuginfo-4.2.4-16.1
libtevent-util0-debuginfo-32bit-4.2.4-16.1
libsamba-util0-32bit-4.2.4-16.1
libndr-krb5pac0-4.2.4-16.1
libsmbclient-raw0-4.2.4-16.1
libndr-standard0-debuginfo-32bit-4.2.4-16.1
libsamba-credentials0-debuginfo-32bit-4.2.4-16.1
libndr-nbt0-4.2.4-16.1
libsmbconf0-32bit-4.2.4-16.1
libsamba-passdb0-debuginfo-32bit-4.2.4-16.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-16.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-16.1
libtevent-util0-32bit-4.2.4-16.1
samba-libs-4.2.4-16.1
samba-winbind-4.2.4-16.1
libwbclient0-4.2.4-16.1
samba-debuginfo-32bit-4.2.4-16.1
libsamdb0-debuginfo-4.2.4-16.1
libsmbldap0-debuginfo-32bit-4.2.4-16.1
libndr-standard0-4.2.4-16.1
samba-libs-debuginfo-32bit-4.2.4-16.1
libsamba-credentials0-4.2.4-16.1
libndr0-debuginfo-32bit-4.2.4-16.1
samba-4.2.4-16.1
libsamba-passdb0-4.2.4-16.1
samba-client-debuginfo-32bit-4.2.4-16.1
libwbclient0-debuginfo-32bit-4.2.4-16.1

noarch
samba-doc-4.2.4-16.1

144521 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1022-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1022-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-April/001997.html

SuSE SLED 12
x86_64
libwbclient0-32bit-4.2.4-18.17.1

samba-client-debuginfo-4.2.4-18.17.1
libsmbclient-raw0-32bit-4.2.4-18.17.1
libnetapi0-debuginfo-4.2.4-18.17.1
libgensec0-debuginfo-4.2.4-18.17.1
libndr-nbt0-32bit-4.2.4-18.17.1
libsmbldap0-debuginfo-32bit-4.2.4-18.17.1
samba-client-4.2.4-18.17.1
libtevent-util0-debuginfo-4.2.4-18.17.1
libndr-standard0-debuginfo-4.2.4-18.17.1
libtevent-util0-32bit-4.2.4-18.17.1
libsamba-util0-debuginfo-32bit-4.2.4-18.17.1
libsamba-credentials0-debuginfo-4.2.4-18.17.1
libregistry0-4.2.4-18.17.1
libnetapi0-32bit-4.2.4-18.17.1
libwbclient0-debuginfo-4.2.4-18.17.1
samba-winbind-4.2.4-18.17.1
libndr-krb5pac0-debuginfo-32bit-4.2.4-18.17.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-18.17.1
libsmbclient-raw0-debuginfo-4.2.4-18.17.1
libsamba-hostconfig0-4.2.4-18.17.1
libndr-krb5pac0-32bit-4.2.4-18.17.1
libsamdb0-debuginfo-32bit-4.2.4-18.17.1
samba-winbind-32bit-4.2.4-18.17.1
libwbclient0-4.2.4-18.17.1
libsmbclient-raw0-4.2.4-18.17.1
samba-libs-4.2.4-18.17.1
libnetapi0-4.2.4-18.17.1
libsamba-hostconfig0-32bit-4.2.4-18.17.1
libndr-nbt0-debuginfo-32bit-4.2.4-18.17.1
libndr-krb5pac0-4.2.4-18.17.1
libsamba-passdb0-32bit-4.2.4-18.17.1
libwbclient0-debuginfo-32bit-4.2.4-18.17.1
libsamba-passdb0-debuginfo-4.2.4-18.17.1
libdcerpc-binding0-4.2.4-18.17.1
libsmbconf0-4.2.4-18.17.1
samba-libs-32bit-4.2.4-18.17.1
libsmbclient0-debuginfo-4.2.4-18.17.1
libndr-standard0-32bit-4.2.4-18.17.1
samba-winbind-debuginfo-32bit-4.2.4-18.17.1
libsmbconf0-debuginfo-32bit-4.2.4-18.17.1
libsamba-hostconfig0-debuginfo-4.2.4-18.17.1
libsamdb0-32bit-4.2.4-18.17.1
libsmbconf0-debuginfo-4.2.4-18.17.1
libtevent-util0-debuginfo-32bit-4.2.4-18.17.1
samba-winbind-debuginfo-4.2.4-18.17.1
samba-debuginfo-32bit-4.2.4-18.17.1
libdcerpc0-4.2.4-18.17.1
samba-libs-debuginfo-4.2.4-18.17.1
libndr-krb5pac0-debuginfo-4.2.4-18.17.1
libgensec0-32bit-4.2.4-18.17.1
libsamba-passdb0-4.2.4-18.17.1
libndr0-32bit-4.2.4-18.17.1
samba-debuginfo-4.2.4-18.17.1
libndr0-4.2.4-18.17.1
libsmbclient0-4.2.4-18.17.1
libdcerpc-binding0-debuginfo-4.2.4-18.17.1
libsmbclient0-32bit-4.2.4-18.17.1
libndr0-debuginfo-32bit-4.2.4-18.17.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-18.17.1
libsamba-credentials0-debuginfo-32bit-4.2.4-18.17.1

libnetapi0-debuginfo-32bit-4.2.4-18.17.1
libdcerpc0-debuginfo-32bit-4.2.4-18.17.1
libsamba-credentials0-32bit-4.2.4-18.17.1
libsamba-passdb0-debuginfo-32bit-4.2.4-18.17.1
libsamdb0-4.2.4-18.17.1
libgensec0-debuginfo-32bit-4.2.4-18.17.1
samba-libs-debuginfo-32bit-4.2.4-18.17.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-18.17.1
libdcerpc-binding0-32bit-4.2.4-18.17.1
libsamba-util0-debuginfo-4.2.4-18.17.1
libndr-standard0-debuginfo-32bit-4.2.4-18.17.1
libndr-nbt0-debuginfo-4.2.4-18.17.1
libsmbldap0-4.2.4-18.17.1
libsamdb0-debuginfo-4.2.4-18.17.1
libdcerpc0-debuginfo-4.2.4-18.17.1
libsamba-util0-32bit-4.2.4-18.17.1
samba-4.2.4-18.17.1
libsmbldap0-debuginfo-4.2.4-18.17.1
libgensec0-4.2.4-18.17.1
libregistry0-debuginfo-4.2.4-18.17.1
libsmbconf0-32bit-4.2.4-18.17.1
libsamba-util0-4.2.4-18.17.1
libsmbclient0-debuginfo-32bit-4.2.4-18.17.1
samba-client-debuginfo-32bit-4.2.4-18.17.1
libndr0-debuginfo-4.2.4-18.17.1
samba-32bit-4.2.4-18.17.1
libdcerpc0-32bit-4.2.4-18.17.1
libtevent-util0-4.2.4-18.17.1
libsmbldap0-32bit-4.2.4-18.17.1
samba-debugsource-4.2.4-18.17.1
samba-client-32bit-4.2.4-18.17.1
libndr-standard0-4.2.4-18.17.1
libndr-nbt0-4.2.4-18.17.1
libsamba-credentials0-4.2.4-18.17.1

noarch
samba-doc-4.2.4-18.17.1

SuSE SLES 12
noarch
samba-doc-4.2.4-18.17.1

x86_64
libwbclient0-4.2.4-18.17.1
samba-client-debuginfo-4.2.4-18.17.1
libsmbclient-raw0-32bit-4.2.4-18.17.1
libnetapi0-debuginfo-4.2.4-18.17.1
libgensec0-debuginfo-4.2.4-18.17.1
libndr-nbt0-32bit-4.2.4-18.17.1
libsmbldap0-debuginfo-32bit-4.2.4-18.17.1
samba-winbind-debuginfo-4.2.4-18.17.1
libtevent-util0-debuginfo-4.2.4-18.17.1
libndr-standard0-debuginfo-4.2.4-18.17.1
libtevent-util0-32bit-4.2.4-18.17.1
libsamba-util0-debuginfo-32bit-4.2.4-18.17.1
libsamba-credentials0-debuginfo-4.2.4-18.17.1
libregistry0-4.2.4-18.17.1
libnetapi0-32bit-4.2.4-18.17.1
libwbclient0-debuginfo-4.2.4-18.17.1
samba-winbind-4.2.4-18.17.1

libndr-krb5pac0-debuginfo-32bit-4.2.4-18.17.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-18.17.1
libsmbclient-raw0-debuginfo-4.2.4-18.17.1
libsamba-hostconfig0-4.2.4-18.17.1
libndr-krb5pac0-32bit-4.2.4-18.17.1
libdcerpc0-debuginfo-32bit-4.2.4-18.17.1
samba-winbind-32bit-4.2.4-18.17.1
libsamba-passdb0-debuginfo-32bit-4.2.4-18.17.1
libsmbclient-raw0-4.2.4-18.17.1
libnetapi0-4.2.4-18.17.1
libsamba-hostconfig0-32bit-4.2.4-18.17.1
samba-debugsource-4.2.4-18.17.1
libndr-krb5pac0-4.2.4-18.17.1
samba-client-4.2.4-18.17.1
libwbclient0-debuginfo-32bit-4.2.4-18.17.1
libsamba-hostconfig0-debuginfo-4.2.4-18.17.1
libsamba-passdb0-debuginfo-4.2.4-18.17.1
libdcerpc-binding0-4.2.4-18.17.1
libsmbconf0-4.2.4-18.17.1
samba-libs-32bit-4.2.4-18.17.1
libsamdb0-debuginfo-32bit-4.2.4-18.17.1
libsmbclient0-debuginfo-4.2.4-18.17.1
libndr-standard0-32bit-4.2.4-18.17.1
samba-winbind-debuginfo-32bit-4.2.4-18.17.1
libsmbconf0-debuginfo-32bit-4.2.4-18.17.1
libndr-nbt0-debuginfo-32bit-4.2.4-18.17.1
libsamdb0-32bit-4.2.4-18.17.1
libsmbconf0-debuginfo-4.2.4-18.17.1
libtevent-util0-debuginfo-32bit-4.2.4-18.17.1
samba-debuginfo-32bit-4.2.4-18.17.1
libdcerpc0-4.2.4-18.17.1
samba-libs-debuginfo-4.2.4-18.17.1
libndr-krb5pac0-debuginfo-4.2.4-18.17.1
libgensec0-32bit-4.2.4-18.17.1
libsamba-passdb0-4.2.4-18.17.1
libndr0-32bit-4.2.4-18.17.1
samba-debuginfo-4.2.4-18.17.1
libwbclient0-32bit-4.2.4-18.17.1
libndr0-4.2.4-18.17.1
libsmbclient0-4.2.4-18.17.1
libdcerpc-binding0-debuginfo-4.2.4-18.17.1
libsmbclient0-32bit-4.2.4-18.17.1
libndr0-debuginfo-32bit-4.2.4-18.17.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-18.17.1
libsamba-credentials0-debuginfo-32bit-4.2.4-18.17.1
libnetapi0-debuginfo-32bit-4.2.4-18.17.1
libsamba-credentials0-32bit-4.2.4-18.17.1
libsamba-passdb0-32bit-4.2.4-18.17.1
libsamdb0-4.2.4-18.17.1
libgensec0-debuginfo-32bit-4.2.4-18.17.1
samba-libs-debuginfo-32bit-4.2.4-18.17.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-18.17.1
libdcerpc-binding0-32bit-4.2.4-18.17.1
libsamba-util0-debuginfo-4.2.4-18.17.1
libndr-standard0-debuginfo-32bit-4.2.4-18.17.1
libndr-nbt0-debuginfo-4.2.4-18.17.1
libsmbldap0-4.2.4-18.17.1
libsamdb0-debuginfo-4.2.4-18.17.1
libdcerpc0-debuginfo-4.2.4-18.17.1
libsamba-util0-32bit-4.2.4-18.17.1

samba-4.2.4-18.17.1
samba-libs-4.2.4-18.17.1
libgensec0-4.2.4-18.17.1
libregistry0-debuginfo-4.2.4-18.17.1
libsmbconf0-32bit-4.2.4-18.17.1
libsmbldap0-32bit-4.2.4-18.17.1
libsamba-util0-4.2.4-18.17.1
libsmbldap0-debuginfo-4.2.4-18.17.1
samba-client-debuginfo-32bit-4.2.4-18.17.1
libndr0-debuginfo-4.2.4-18.17.1
samba-32bit-4.2.4-18.17.1
libdcerpc0-32bit-4.2.4-18.17.1
libtevent-util0-4.2.4-18.17.1
libsmbclient0-debuginfo-32bit-4.2.4-18.17.1
samba-client-32bit-4.2.4-18.17.1

144522 - SuSE Linux 13.2 openSUSE-SU-2016:1007-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3190

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1007-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-04/msg00029.html

SuSE Linux 13.2
x86_64
libcairo-script-interpreter2-32bit-1.14.0-7.11.1
libcairo-gobject2-1.14.0-7.11.1
cairo-tools-debuginfo-1.14.0-7.11.1
cairo-devel-1.14.0-7.11.1
libcairo-script-interpreter2-debuginfo-1.14.0-7.11.1
cairo-devel-32bit-1.14.0-7.11.1
libcairo-script-interpreter2-debuginfo-32bit-1.14.0-7.11.1
libcairo-gobject2-debuginfo-32bit-1.14.0-7.11.1
cairo-tools-1.14.0-7.11.1
libcairo2-debuginfo-1.14.0-7.11.1
libcairo2-1.14.0-7.11.1
libcairo-gobject2-32bit-1.14.0-7.11.1
libcairo2-debuginfo-32bit-1.14.0-7.11.1
libcairo-script-interpreter2-1.14.0-7.11.1
cairo-debugsource-1.14.0-7.11.1
libcairo2-32bit-1.14.0-7.11.1
libcairo-gobject2-debuginfo-1.14.0-7.11.1

i586
libcairo2-1.14.0-7.11.1
cairo-tools-1.14.0-7.11.1
libcairo-gobject2-1.14.0-7.11.1
libcairo-gobject2-debuginfo-1.14.0-7.11.1
libcairo-script-interpreter2-debuginfo-1.14.0-7.11.1

libcairo-script-interpreter2-1.14.0-7.11.1
libcairo2-debuginfo-1.14.0-7.11.1
cairo-debugsource-1.14.0-7.11.1
cairo-tools-debuginfo-1.14.0-7.11.1
cairo-devel-1.14.0-7.11.1

144523 - SuSE SLES 11 SP4 SUSE-SU-2016:1023-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1023-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-April/001998.html

SuSE SLES 11 SP4
noarch
samba-doc-3.6.3-76.2

i586
ldapsmb-1.34b-76.1
samba-krb-printing-3.6.3-76.1
samba-winbind-3.6.3-76.1
libtalloc2-3.6.3-76.1
samba-3.6.3-76.1
samba-client-3.6.3-76.1
libtevent0-3.6.3-76.1
libldb1-3.6.3-76.1
libwbclient0-3.6.3-76.1
libsmbclient0-3.6.3-76.1
libtdb1-3.6.3-76.1

x86_64
libtevent0-32bit-3.6.3-76.1
libwbclient0-32bit-3.6.3-76.1
samba-krb-printing-3.6.3-76.1
libwbclient0-3.6.3-76.1
samba-winbind-32bit-3.6.3-76.1
ldapsmb-1.34b-76.1
libsmbclient0-32bit-3.6.3-76.1
libtalloc2-3.6.3-76.1
samba-3.6.3-76.1
samba-client-32bit-3.6.3-76.1
samba-client-3.6.3-76.1
libsmbclient0-3.6.3-76.1
libtevent0-3.6.3-76.1
libldb1-3.6.3-76.1
libtdb1-32bit-3.6.3-76.1
samba-winbind-3.6.3-76.1
libtdb1-3.6.3-76.1
libtalloc2-32bit-3.6.3-76.1

samba-32bit-3.6.3-76.1

144528 - SuSE Linux 13.2 openSUSE-SU-2016:1016-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3068, CVE-2016-3069, CVE-2016-3630

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1016-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-04/msg00036.html

SuSE Linux 13.2
i586
mercurial-3.1.2-7.1
mercurial-debugsource-3.1.2-7.1
mercurial-debuginfo-3.1.2-7.1

noarch
mercurial-lang-3.1.2-7.1

x86_64
mercurial-3.1.2-7.1
mercurial-debugsource-3.1.2-7.1
mercurial-debuginfo-3.1.2-7.1

144529 - SuSE Linux 13.2 openSUSE-SU-2016:0966-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0252, CVE-2016-0729

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:0966-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-04/msg00012.html

SuSE Linux 13.2
x86_64
libxerces-c-3_1-32bit-3.1.1-13.3.1
libxerces-c-3_1-debuginfo-32bit-3.1.1-13.3.1
libxerces-c-3_1-3.1.1-13.3.1
xerces-c-debuginfo-3.1.1-13.3.1
libxerces-c-3_1-debuginfo-3.1.1-13.3.1
libxerces-c-devel-3.1.1-13.3.1

xerces-c-debugsource-3.1.1-13.3.1
xerces-c-3.1.1-13.3.1

i586
libxerces-c-3_1-3.1.1-13.3.1
xerces-c-debuginfo-3.1.1-13.3.1
libxerces-c-3_1-debuginfo-3.1.1-13.3.1
libxerces-c-devel-3.1.1-13.3.1
xerces-c-debugsource-3.1.1-13.3.1
xerces-c-3.1.1-13.3.1

160085 - CentOS 5 CESA-2016-0621 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
CESA-2016-0621

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-April/021823.html

CentOS 5
x86_64
samba-3.0.33-3.41.el5_11
libsmbclient-devel-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

i386
samba-3.0.33-3.41.el5_11
libsmbclient-devel-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

163061 - Oracle Enterprise Linux ELSA-2016-0621 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
ELSA-2016-0621

Observation

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

For more information see:

http://oss.oracle.com/pipermail/el-errata/2016-April/005950.html

OEL5
i386
samba-3.0.33-3.41.el5_11
libsmbclient-devel-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

x86_64
samba-3.0.33-3.41.el5_11
libsmbclient-devel-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

170659 - Amazon Linux AMI ALAS-2016-684 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4766, CVE-2015-4791, CVE-2015-4792, CVE-2015-4800, CVE-2015-4802, CVE-2015-4807, CVE-2015-4815, CVE-2015-4819, CVE-2015-4826, CVE-2015-4830, CVE-2015-4833, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4862, CVE-2015-4864, CVE-2015-4866, CVE-2015-4870, CVE-2015-4879, CVE-2015-4890, CVE-2015-4895, CVE-2015-4904, CVE-2015-4905, CVE-2015-4910, CVE-2015-4913, CVE-2015-7744, CVE-2016-0502, CVE-2016-0503, CVE-2016-0504, CVE-2016-0505, CVE-2016-0546, CVE-2016-0594, CVE-2016-0595, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0599, CVE-2016-0600, CVE-2016-0601, CVE-2016-0605, CVE-2016-0606, CVE-2016-0607, CVE-2016-0608, CVE-2016-0609, CVE-2016-0610, CVE-2016-0611, CVE-2016-0616

Description

The scan detected that the host is missing the following update:
ALAS-2016-684

Observation

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

https://alas.aws.amazon.com/ALAS-2016-684.html

Amazon Linux AMI
x86_64
mysql56-errmsg-5.6.29-1.14.amzn1
mysql56-embedded-5.6.29-1.14.amzn1
mysql56-common-5.6.29-1.14.amzn1
mysql56-embedded-devel-5.6.29-1.14.amzn1
mysql56-test-5.6.29-1.14.amzn1
mysql56-5.6.29-1.14.amzn1
mysql56-debuginfo-5.6.29-1.14.amzn1
mysql56-devel-5.6.29-1.14.amzn1
mysql56-server-5.6.29-1.14.amzn1
mysql56-libs-5.6.29-1.14.amzn1
mysql56-bench-5.6.29-1.14.amzn1

i686

mysql56-errmsg-5.6.29-1.14.amzn1
mysql56-embedded-5.6.29-1.14.amzn1
mysql56-libs-5.6.29-1.14.amzn1
mysql56-test-5.6.29-1.14.amzn1
mysql56-5.6.29-1.14.amzn1
mysql56-debuginfo-5.6.29-1.14.amzn1
mysql56-devel-5.6.29-1.14.amzn1
mysql56-embedded-devel-5.6.29-1.14.amzn1
mysql56-server-5.6.29-1.14.amzn1
mysql56-common-5.6.29-1.14.amzn1
mysql56-bench-5.6.29-1.14.amzn1

174942 - Scientific Linux Security ERRATA Important: samba on SL5.x i386/x86_64 (1604-6906)

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

Risk Level: High

CVE: CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: samba on SL5.x i386/x86_64 (1604-6906)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1604&L=scientific-linux-errata&F=&S=&P=6906

SL5
x86_64
samba-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
libsmbclient-devel-3.0.33-3.41.el5_11
samba-debuginfo-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

i386
samba-3.0.33-3.41.el5_11
samba-swat-3.0.33-3.41.el5_11
libsmbclient-devel-3.0.33-3.41.el5_11
samba-debuginfo-3.0.33-3.41.el5_11
samba-client-3.0.33-3.41.el5_11
libsmbclient-3.0.33-3.41.el5_11
samba-common-3.0.33-3.41.el5_11

190490 - Fedora Linux 24 FEDORA-2016-9ff972ca42 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0729

Description

The scan detected that the host is missing the following update:
FEDORA-2016-9ff972ca42

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182062.html

Fedora Core 24

xerces-c-3.1.3-1.fc24

190515 - Fedora Linux 23 FEDORA-2016-ae9ac16cf3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0729

Description

The scan detected that the host is missing the following update:
FEDORA-2016-ae9ac16cf3

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182131.html

Fedora Core 23

xerces-c-3.1.3-1.fc23

144527 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1019-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8709, CVE-2015-8812, CVE-2015-8816, CVE-2016-2143, CVE-2016-2184, CVE-2016-2384, CVE-2016-2782, CVE-2016-3139, CVE-2016-3156

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1019-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-April/001996.html

SuSE SLES 12 SP1
noarch
kernel-source-3.12.57-60.35.1
kernel-macros-3.12.57-60.35.1
kernel-devel-3.12.57-60.35.1

x86_64
kernel-syms-3.12.57-60.35.1

kernel-default-debugsource-3.12.57-60.35.1
kernel-default-3.12.57-60.35.1
kernel-default-base-debuginfo-3.12.57-60.35.1
kernel-xen-debugsource-3.12.57-60.35.1
kernel-xen-devel-3.12.57-60.35.1
kernel-default-devel-3.12.57-60.35.1
kernel-xen-base-3.12.57-60.35.1
kernel-xen-base-debuginfo-3.12.57-60.35.1
kernel-default-debuginfo-3.12.57-60.35.1
kernel-default-base-3.12.57-60.35.1
kernel-xen-3.12.57-60.35.1
kernel-xen-debuginfo-3.12.57-60.35.1

SuSE SLED 12 SP1
x86_64
kernel-xen-debuginfo-3.12.57-60.35.1
kernel-default-debugsource-3.12.57-60.35.1
kernel-xen-debugsource-3.12.57-60.35.1
kernel-xen-devel-3.12.57-60.35.1
kernel-syms-3.12.57-60.35.1
kernel-default-extra-3.12.57-60.35.1
kernel-default-extra-debuginfo-3.12.57-60.35.1
kernel-default-devel-3.12.57-60.35.1
kernel-default-debuginfo-3.12.57-60.35.1
kernel-default-3.12.57-60.35.1
kernel-xen-3.12.57-60.35.1

noarch
kernel-source-3.12.57-60.35.1
kernel-macros-3.12.57-60.35.1
kernel-devel-3.12.57-60.35.1

144518 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:0963-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5276

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:0963-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-April/001987.html

SuSE SLED 12 SP1
x86_64
libstdc++6-5.3.1+r233831-9.1
libmpxwrappers0-5.3.1+r233831-9.1
libubsan0-debuginfo-5.3.1+r233831-9.1
libtsan0-5.3.1+r233831-9.1
libcilkrts5-5.3.1+r233831-9.1
libffi-gcc5-debugsource-5.3.1+r233831-9.1
libgfortran3-debuginfo-5.3.1+r233831-9.1
libtsan0-debuginfo-5.3.1+r233831-9.1

libcilkrts5-32bit-5.3.1+r233831-9.1
libasan2-debuginfo-5.3.1+r233831-9.1
libffi4-5.3.1+r233831-9.1
libstdc++6-debuginfo-5.3.1+r233831-9.1
libgomp1-5.3.1+r233831-9.1
liblsan0-debuginfo-5.3.1+r233831-9.1
libgomp1-debuginfo-5.3.1+r233831-9.1
libubsan0-5.3.1+r233831-9.1
libgfortran3-32bit-5.3.1+r233831-9.1
libasan2-32bit-5.3.1+r233831-9.1
libquadmath0-5.3.1+r233831-9.1
libgcc_s1-5.3.1+r233831-9.1
libasan2-5.3.1+r233831-9.1
libstdc++6-locale-5.3.1+r233831-9.1
libubsan0-32bit-5.3.1+r233831-9.1
libmpxwrappers0-debuginfo-5.3.1+r233831-9.1
libstdc++6-32bit-5.3.1+r233831-9.1
gcc5-debugsource-5.3.1+r233831-9.1
libitm1-debuginfo-5.3.1+r233831-9.1
libitm1-5.3.1+r233831-9.1
libitm1-32bit-5.3.1+r233831-9.1
libquadmath0-debuginfo-5.3.1+r233831-9.1
liblsan0-5.3.1+r233831-9.1
libmpx0-32bit-5.3.1+r233831-9.1
libgcc_s1-debuginfo-5.3.1+r233831-9.1
libmpxwrappers0-32bit-5.3.1+r233831-9.1
libatomic1-5.3.1+r233831-9.1
libmpx0-5.3.1+r233831-9.1
gcc5-debuginfo-5.3.1+r233831-9.1
libatomic1-debuginfo-5.3.1+r233831-9.1
libffi4-32bit-5.3.1+r233831-9.1
libquadmath0-32bit-5.3.1+r233831-9.1
libcilkrts5-debuginfo-5.3.1+r233831-9.1
libgfortran3-5.3.1+r233831-9.1
libffi4-debuginfo-5.3.1+r233831-9.1
libmpx0-debuginfo-5.3.1+r233831-9.1
libatomic1-32bit-5.3.1+r233831-9.1
libgcc_s1-32bit-5.3.1+r233831-9.1
libgomp1-32bit-5.3.1+r233831-9.1

SuSE SLED 12
x86_64
libmpxwrappers0-32bit-debuginfo-5.3.1+r233831-9.1
libmpxwrappers0-5.3.1+r233831-9.1
libubsan0-debuginfo-5.3.1+r233831-9.1
libtsan0-5.3.1+r233831-9.1
libcilkrts5-5.3.1+r233831-9.1
libffi-gcc5-debugsource-5.3.1+r233831-9.1
libasan2-32bit-debuginfo-5.3.1+r233831-9.1
libgfortran3-debuginfo-5.3.1+r233831-9.1
libtsan0-debuginfo-5.3.1+r233831-9.1
libcilkrts5-32bit-5.3.1+r233831-9.1
libasan2-debuginfo-5.3.1+r233831-9.1
libffi4-5.3.1+r233831-9.1
libstdc++6-debuginfo-5.3.1+r233831-9.1
libgomp1-5.3.1+r233831-9.1
liblsan0-debuginfo-5.3.1+r233831-9.1
libgomp1-debuginfo-5.3.1+r233831-9.1
libubsan0-5.3.1+r233831-9.1
libmpx0-32bit-debuginfo-5.3.1+r233831-9.1

libgfortran3-32bit-5.3.1+r233831-9.1
libcilkrts5-32bit-debuginfo-5.3.1+r233831-9.1
libgfortran3-32bit-debuginfo-5.3.1+r233831-9.1
libitm1-32bit-debuginfo-5.3.1+r233831-9.1
libgcc_s1-5.3.1+r233831-9.1
libasan2-5.3.1+r233831-9.1
libstdc++6-locale-5.3.1+r233831-9.1
libubsan0-32bit-5.3.1+r233831-9.1
libgomp1-32bit-debuginfo-5.3.1+r233831-9.1
libmpxwrappers0-debuginfo-5.3.1+r233831-9.1
libubsan0-32bit-debuginfo-5.3.1+r233831-9.1
libstdc++6-32bit-5.3.1+r233831-9.1
gcc5-debugsource-5.3.1+r233831-9.1
libffi4-32bit-debuginfo-5.3.1+r233831-9.1
libitm1-debuginfo-5.3.1+r233831-9.1
libitm1-5.3.1+r233831-9.1
libatomic1-debuginfo-5.3.1+r233831-9.1
libquadmath0-debuginfo-5.3.1+r233831-9.1
liblsan0-5.3.1+r233831-9.1
libstdc++6-5.3.1+r233831-9.1
libmpx0-32bit-5.3.1+r233831-9.1
libatomic1-32bit-debuginfo-5.3.1+r233831-9.1
libgcc_s1-debuginfo-5.3.1+r233831-9.1
libquadmath0-32bit-debuginfo-5.3.1+r233831-9.1
libmpxwrappers0-32bit-5.3.1+r233831-9.1
libitm1-32bit-5.3.1+r233831-9.1
libatomic1-5.3.1+r233831-9.1
libmpx0-5.3.1+r233831-9.1
libstdc++6-32bit-debuginfo-5.3.1+r233831-9.1
libffi4-32bit-5.3.1+r233831-9.1
libquadmath0-5.3.1+r233831-9.1
libgcc_s1-32bit-debuginfo-5.3.1+r233831-9.1
libcilkrts5-debuginfo-5.3.1+r233831-9.1
libgfortran3-5.3.1+r233831-9.1
libasan2-32bit-5.3.1+r233831-9.1
libquadmath0-32bit-5.3.1+r233831-9.1
libffi4-debuginfo-5.3.1+r233831-9.1
libmpx0-debuginfo-5.3.1+r233831-9.1
libatomic1-32bit-5.3.1+r233831-9.1
libgcc_s1-32bit-5.3.1+r233831-9.1
libgomp1-32bit-5.3.1+r233831-9.1

SuSE SLES 12 SP1
x86_64
libstdc++6-5.3.1+r233831-9.1
libmpxwrappers0-5.3.1+r233831-9.1
libubsan0-debuginfo-5.3.1+r233831-9.1
libtsan0-5.3.1+r233831-9.1
libcilkrts5-5.3.1+r233831-9.1
libffi-gcc5-debugsource-5.3.1+r233831-9.1
libgfortran3-debuginfo-5.3.1+r233831-9.1
libtsan0-debuginfo-5.3.1+r233831-9.1
libcilkrts5-32bit-5.3.1+r233831-9.1
libasan2-debuginfo-5.3.1+r233831-9.1
libffi4-5.3.1+r233831-9.1
libstdc++6-debuginfo-5.3.1+r233831-9.1
libgomp1-5.3.1+r233831-9.1
liblsan0-5.3.1+r233831-9.1
liblsan0-debuginfo-5.3.1+r233831-9.1
libgomp1-debuginfo-5.3.1+r233831-9.1

libgfortran3-32bit-5.3.1+r233831-9.1
libasan2-32bit-5.3.1+r233831-9.1
libquadmath0-5.3.1+r233831-9.1
libgcc_s1-5.3.1+r233831-9.1
libasan2-5.3.1+r233831-9.1
libubsan0-32bit-5.3.1+r233831-9.1
libmpxwrappers0-debuginfo-5.3.1+r233831-9.1
libstdc++6-32bit-5.3.1+r233831-9.1
gcc5-debugsource-5.3.1+r233831-9.1
libitm1-debuginfo-5.3.1+r233831-9.1
libitm1-5.3.1+r233831-9.1
libatomic1-debuginfo-5.3.1+r233831-9.1
libquadmath0-debuginfo-5.3.1+r233831-9.1
libstdc++6-locale-5.3.1+r233831-9.1
libmpx0-5.3.1+r233831-9.1
libmpx0-32bit-5.3.1+r233831-9.1
libgcc_s1-debuginfo-5.3.1+r233831-9.1
libmpxwrappers0-32bit-5.3.1+r233831-9.1
libitm1-32bit-5.3.1+r233831-9.1
libatomic1-5.3.1+r233831-9.1
libubsan0-5.3.1+r233831-9.1
gcc5-debuginfo-5.3.1+r233831-9.1
libffi4-32bit-5.3.1+r233831-9.1
libquadmath0-32bit-5.3.1+r233831-9.1
libcilkrts5-debuginfo-5.3.1+r233831-9.1
libgfortran3-5.3.1+r233831-9.1
libffi4-debuginfo-5.3.1+r233831-9.1
libmpx0-debuginfo-5.3.1+r233831-9.1
libatomic1-32bit-5.3.1+r233831-9.1
libgcc_s1-32bit-5.3.1+r233831-9.1
libgomp1-32bit-5.3.1+r233831-9.1

SuSE SLES 12
x86_64
libstdc++6-5.3.1+r233831-9.1
libmpxwrappers0-32bit-debuginfo-5.3.1+r233831-9.1
libubsan0-debuginfo-5.3.1+r233831-9.1
libtsan0-5.3.1+r233831-9.1
libcilkrts5-5.3.1+r233831-9.1
libffi-gcc5-debugsource-5.3.1+r233831-9.1
libasan2-32bit-debuginfo-5.3.1+r233831-9.1
libgfortran3-debuginfo-5.3.1+r233831-9.1
libtsan0-debuginfo-5.3.1+r233831-9.1
libcilkrts5-32bit-5.3.1+r233831-9.1
libasan2-debuginfo-5.3.1+r233831-9.1
libffi4-5.3.1+r233831-9.1
libstdc++6-debuginfo-5.3.1+r233831-9.1
libgomp1-5.3.1+r233831-9.1
liblsan0-5.3.1+r233831-9.1
liblsan0-debuginfo-5.3.1+r233831-9.1
libgomp1-debuginfo-5.3.1+r233831-9.1
libmpx0-32bit-debuginfo-5.3.1+r233831-9.1
libgfortran3-32bit-5.3.1+r233831-9.1
libcilkrts5-32bit-debuginfo-5.3.1+r233831-9.1
libgfortran3-32bit-debuginfo-5.3.1+r233831-9.1
libitm1-32bit-debuginfo-5.3.1+r233831-9.1
libgcc_s1-5.3.1+r233831-9.1
libasan2-5.3.1+r233831-9.1
libubsan0-32bit-5.3.1+r233831-9.1
libgomp1-32bit-debuginfo-5.3.1+r233831-9.1

libmpxwrappers0-debuginfo-5.3.1+r233831-9.1
libubsan0-32bit-debuginfo-5.3.1+r233831-9.1
libstdc++6-32bit-5.3.1+r233831-9.1
gcc5-debugsource-5.3.1+r233831-9.1
libitm1-debuginfo-5.3.1+r233831-9.1
libitm1-5.3.1+r233831-9.1
libatomic1-debuginfo-5.3.1+r233831-9.1
libquadmath0-debuginfo-5.3.1+r233831-9.1
libstdc++6-locale-5.3.1+r233831-9.1
libmpx0-5.3.1+r233831-9.1
libmpxwrappers0-5.3.1+r233831-9.1
libmpx0-32bit-5.3.1+r233831-9.1

170660 - Amazon Linux AMI ALAS-2016-683 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0787

Description

The scan detected that the host is missing the following update:
ALAS-2016-683

Observation

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

https://alas.aws.amazon.com/ALAS-2016-683.html

Amazon Linux AMI
x86_64
libssh2-debuginfo-1.4.2-2.13.amzn1
libssh2-1.4.2-2.13.amzn1
libssh2-devel-1.4.2-2.13.amzn1
libssh2-docs-1.4.2-2.13.amzn1

i686
libssh2-docs-1.4.2-2.13.amzn1
libssh2-1.4.2-2.13.amzn1
libssh2-devel-1.4.2-2.13.amzn1
libssh2-debuginfo-1.4.2-2.13.amzn1

170661 - Amazon Linux AMI ALAS-2016-682 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0293, CVE-2015-3197, CVE-2016-0703, CVE-2016-0704, CVE-2016-0800

Description

The scan detected that the host is missing the following update:
ALAS-2016-682

Observation

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

https://alas.aws.amazon.com/ALAS-2016-682.html

Amazon Linux AMI
x86_64
openssl098e-debuginfo-0.9.8e-29.19.amzn1
openssl098e-0.9.8e-29.19.amzn1

i686
openssl098e-debuginfo-0.9.8e-29.19.amzn1
openssl098e-0.9.8e-29.19.amzn1

185238 - Ubuntu Linux 14.04 USN-2948-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7566, CVE-2015-7833, CVE-2015-8812, CVE-2016-0723, CVE-2016-2085, CVE-2016-2550, CVE-2016-2782, CVE-2016-2847

Description

The scan detected that the host is missing the following update:
USN-2948-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-April/003381.html

Ubuntu 14.04

linux-image-3.16.0-70-powerpc64-smp_3.16.0-70.90~14.04.1
linux-image-3.16.0-70-powerpc-e500mc_3.16.0-70.90~14.04.1
linux-image-3.16.0-70-powerpc64-emb_3.16.0-70.90~14.04.1
linux-image-3.16.0-70-powerpc-smp_3.16.0-70.90~14.04.1
linux-image-3.16.0-70-generic_3.16.0-70.90~14.04.1
linux-image-3.16.0-70-generic-lpae_3.16.0-70.90~14.04.1
linux-image-3.16.0-70-lowlatency_3.16.0-70.90~14.04.1

130464 - Debian Linux 7.0, 8.0 DSA-3544-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2512, CVE-2016-2513

Description

The scan detected that the host is missing the following update:
DSA-3544-1

Observation

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

http://www.debian.org/security/2016/dsa-3544

Debian 8.0
all

python-django_1.7.7-1+deb8u4

Debian 7.0
all
python-django_1.4.5-1+deb7u16

130462 - Debian Linux 7.0, 8.0 DSA-3546-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2191, CVE-2016-3981, CVE-2016-3982

Description

The scan detected that the host is missing the following update:
DSA-3546-1

Observation

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

http://www.debian.org/security/2016/dsa-3546

Debian 8.0
all
optipng_0.7.5-1+deb8u1

Debian 7.0
all
optipng_0.6.4-1+deb7u2

130463 - Debian Linux 7.0 DSA-3547-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-3547-1

Observation

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

http://www.debian.org/security/2016/dsa-3547

Debian 7.0
all
imagemagick_8:6.7.7.10-5+deb7u4

144519 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:0994-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3119

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:0994-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-April/001993.html

SuSE SLED 12 SP1
x86_64
krb5-32bit-1.12.1-28.1
krb5-client-debuginfo-1.12.1-28.1
krb5-debuginfo-1.12.1-28.1
krb5-debugsource-1.12.1-28.1
krb5-client-1.12.1-28.1
krb5-1.12.1-28.1
krb5-debuginfo-32bit-1.12.1-28.1

SuSE SLED 12
x86_64
krb5-32bit-1.12.1-28.1
krb5-client-debuginfo-1.12.1-28.1
krb5-debuginfo-1.12.1-28.1
krb5-debugsource-1.12.1-28.1
krb5-client-1.12.1-28.1
krb5-1.12.1-28.1
krb5-debuginfo-32bit-1.12.1-28.1

SuSE SLES 12 SP1
x86_64
krb5-1.12.1-28.1
krb5-client-1.12.1-28.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.1-28.1
krb5-debugsource-1.12.1-28.1
krb5-debuginfo-32bit-1.12.1-28.1
krb5-client-debuginfo-1.12.1-28.1
krb5-server-1.12.1-28.1
krb5-plugin-kdb-ldap-debuginfo-1.12.1-28.1
krb5-plugin-kdb-ldap-1.12.1-28.1
krb5-plugin-preauth-otp-1.12.1-28.1
krb5-doc-1.12.1-28.1
krb5-debuginfo-1.12.1-28.1
krb5-server-debuginfo-1.12.1-28.1
krb5-32bit-1.12.1-28.1
krb5-plugin-preauth-otp-debuginfo-1.12.1-28.1
krb5-plugin-preauth-pkinit-1.12.1-28.1

SuSE SLES 12
x86_64
krb5-1.12.1-28.1
krb5-client-1.12.1-28.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.1-28.1
krb5-debugsource-1.12.1-28.1
krb5-debuginfo-32bit-1.12.1-28.1
krb5-client-debuginfo-1.12.1-28.1
krb5-server-1.12.1-28.1

krb5-plugin-kdb-ldap-debuginfo-1.12.1-28.1
krb5-plugin-kdb-ldap-1.12.1-28.1
krb5-plugin-preauth-otp-1.12.1-28.1
krb5-doc-1.12.1-28.1
krb5-debuginfo-1.12.1-28.1
krb5-server-debuginfo-1.12.1-28.1
krb5-32bit-1.12.1-28.1
krb5-plugin-preauth-otp-debuginfo-1.12.1-28.1
krb5-plugin-preauth-pkinit-1.12.1-28.1

181916 - FreeBSD samba Multiple Vulnerabilities (a636fc26-00d9-11e6-b704-000c292e4fd8)

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

Risk Level: Low

CVE: CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-2118

Description

The scan detected that the host is missing the following update:
samba -- multiple vulnerabilities (a636fc26-00d9-11e6-b704-000c292e4fd8)

Observation

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

http://www.vuxml.org/freebsd/a636fc26-00d9-11e6-b704-000c292e4fd8.html

Affected packages:
3.6.0 <= samba36 <= 3.6.25_3
4.0.0 <= samba4 <= 4.0.26
4.1.0 <= samba41 <= 4.1.23
4.2.0 <= samba42 < 4.2.11
4.3.0 <= samba43 < 4.3.8
4.4.0 <= samba44 < 4.4.2

190491 - Fedora Linux 22 FEDORA-2016-5f196e4e4a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3158, CVE-2016-3159

Description

The scan detected that the host is missing the following update:
FEDORA-2016-5f196e4e4a

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181699.html

Fedora Core 22

xen-4.5.3-1.fc22

190492 - Fedora Linux 23 FEDORA-2016-7e602c0e5e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2187, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3157

Description

The scan detected that the host is missing the following update:
FEDORA-2016-7e602c0e5e

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181584.html

Fedora Core 23

kernel-4.4.6-301.fc23

190493 - Fedora Linux 23 FEDORA-2016-b7f1f8e3bf Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3068, CVE-2016-3069, CVE-2016-3630

Description

The scan detected that the host is missing the following update:
FEDORA-2016-b7f1f8e3bf

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181542.html

Fedora Core 23

mercurial-3.5.2-1.fc23

190494 - Fedora Linux 22 FEDORA-2016-15fb7deba0 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-2016-15fb7deba0

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181527.html

Fedora Core 22

python-rsa-3.4.1-1.fc22

190495 - Fedora Linux 24 FEDORA-2016-6ab2d29fba 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-2016-6ab2d29fba

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181412.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181409.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181418.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181414.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181422.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181419.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181411.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181415.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181416.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181423.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181410.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181421.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181417.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181413.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181420.html

Fedora Core 24

nodejs-5.10.0-1.fc24
nodejs-fs-ext-0.5.0-9.fc24
nodejs-sqlite3-3.1.2-3.fc24
nodejs-node-stringprep-0.7.3-9.fc24
nodejs-request-2.67.0-6.fc24
nodejs-node-expat-2.3.11-8.fc24
nodejs-libxmljs-0.17.1-4.fc24
nodejs-srs-1.1.0-3.fc24
nodejs-buffertools-2.1.3-12.fc24
nodejs-zipfile-0.5.9-7.fc24
nodejs-i2c-0.2.1-6.fc24
nodejs-bl-1.1.2-1.fc24
nodejs-gdal-0.9.0-1.fc24
nodejs-mapnik-3.5.6-2.fc24
nodejs-iconv-2.1.11-8.fc24

190496 - Fedora Linux 22 FEDORA-2016-6ad4474058 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3076

Description

The scan detected that the host is missing the following update:
FEDORA-2016-6ad4474058

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181863.html

Fedora Core 22

python-pillow-2.8.2-5.fc22

190497 - Fedora Linux 23 FEDORA-2016-f8eee2e628 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2011-5326, CVE-2016-3994

Description

The scan detected that the host is missing the following update:
FEDORA-2016-f8eee2e628

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182141.html

Fedora Core 23

imlib2-1.4.8-1.fc23

190498 - Fedora Linux 22 FEDORA-2016-f61f02e9e2 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-2016-f61f02e9e2

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181675.html

Fedora Core 22

fuse-encfs-1.8.1-1.fc22

190499 - Fedora Linux 24 FEDORA-2016-c9a9231a9d 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-2016-c9a9231a9d

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182103.html

Fedora Core 24

postgresql-9.5.2-1.fc24

190500 - Fedora Linux 23 FEDORA-2016-df2529c86c 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-2016-df2529c86c

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181460.html

Fedora Core 23

python-rsa-3.4.1-1.fc23

190501 - Fedora Linux 23 FEDORA-2016-1cf1b49047 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-2016-1cf1b49047

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181724.html

Fedora Core 23

php-5.6.20-1.fc23

190502 - Fedora Linux 22 FEDORA-2016-9282d83bee 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-2016-9282d83bee

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181697.html

Fedora Core 22

php-5.6.20-1.fc22

190503 - Fedora Linux 23 FEDORA-2016-e5432ca977 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3158, CVE-2016-3159

Description

The scan detected that the host is missing the following update:
FEDORA-2016-e5432ca977

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181729.html

Fedora Core 23

xen-4.5.3-1.fc23

190504 - Fedora Linux 23 FEDORA-2016-680a5a8ead Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3071

Description

The scan detected that the host is missing the following update:
FEDORA-2016-680a5a8ead

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182130.html

Fedora Core 23

libreswan-3.17-1.fc23

190505 - Fedora Linux 22 FEDORA-2016-ed5110c4bb Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2187, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3157

Description

The scan detected that the host is missing the following update:
FEDORA-2016-ed5110c4bb

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181676.html

Fedora Core 22

kernel-4.4.6-201.fc22

190506 - Fedora Linux 24 FEDORA-2016-711a04c964 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3071

Description

The scan detected that the host is missing the following update:
FEDORA-2016-711a04c964

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182050.html

Fedora Core 24

libreswan-3.17-1.fc24

190507 - Fedora Linux 22 FEDORA-2016-c14cf5e34a 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-2016-c14cf5e34a

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181524.html

Fedora Core 22

libmaxminddb-1.2.0-1.fc22

190508 - Fedora Linux 24 FEDORA-2016-f75bd73891 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3095

Description

The scan detected that the host is missing the following update:
FEDORA-2016-f75bd73891

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182006.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182008.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-April/182007.html

Fedora Core 24

pulp-rpm-2.8.2-1.fc24
pulp-2.8.2-1.fc24
pulp-puppet-2.8.2-1.fc24

190509 - Fedora Linux 22 FEDORA-2016-79604dde9f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3068, CVE-2016-3069, CVE-2016-3630

Description

The scan detected that the host is missing the following update:
FEDORA-2016-79604dde9f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181505.html

Fedora Core 22

mercurial-3.5.2-1.fc22

190510 - Fedora Linux 23 FEDORA-2016-b9368247d4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8106

Description

The scan detected that the host is missing the following update:
FEDORA-2016-b9368247d4

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181725.html

Fedora Core 23

latex2rtf-2.3.10-1.fc23

190511 - Fedora Linux 22 FEDORA-2016-bfaf6a133b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2392, CVE-2016-2538, CVE-2016-2841, CVE-2016-2857

Description

The scan detected that the host is missing the following update:
FEDORA-2016-bfaf6a133b

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181689.html

Fedora Core 22

qemu-2.3.1-13.fc22

190512 - Fedora Linux 23 FEDORA-2016-b05672c54f 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-2016-b05672c54f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181573.html

Fedora Core 23

libmaxminddb-1.2.0-1.fc23

190513 - Fedora Linux 22 FEDORA-2016-246417376c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8106

Description

The scan detected that the host is missing the following update:
FEDORA-2016-246417376c

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181677.html

Fedora Core 22

latex2rtf-2.3.10-1.fc22

190514 - Fedora Linux 23 FEDORA-2016-35700c5956 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3076

Description

The scan detected that the host is missing the following update:
FEDORA-2016-35700c5956

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181943.html

Fedora Core 23

python-pillow-3.0.0-4.fc23

190516 - Fedora Linux 24 FEDORA-2016-2d33f969b7 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-2016-2d33f969b7

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181495.html

Fedora Core 24

libmaxminddb-1.2.0-1.fc24

190517 - Fedora Linux 23 FEDORA-2016-858277b967 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-2016-858277b967

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-April/181723.html

Fedora Core 23

fuse-encfs-1.8.1-1.fc23

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.