

MCAFFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

145532 - SuSE Linux 42.2 openSUSE-SU-2017:1401-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7494

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1401-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00081.html>

SuSE Linux 42.2

i586

libsamba-credentials0-debuginfo-4.4.2-11.9.1

libsamba-errors0-debuginfo-4.4.2-11.9.1

libsmbclient-devel-4.4.2-11.9.1

libtevent-util0-debuginfo-4.4.2-11.9.1

libndr-krb5pac-devel-4.4.2-11.9.1

libsamba-util0-debuginfo-4.4.2-11.9.1

libsamba-policy-devel-4.4.2-11.9.1

libtevent-util-devel-4.4.2-11.9.1

samba-python-debuginfo-4.4.2-11.9.1

libsmbldap-devel-4.4.2-11.9.1

libsamba-policy0-4.4.2-11.9.1

libwbclient-devel-4.4.2-11.9.1

libndr-standard-devel-4.4.2-11.9.1

libdcerpc0-debuginfo-4.4.2-11.9.1

samba-test-4.4.2-11.9.1

libsamdb0-4.4.2-11.9.1

samba-pidl-4.4.2-11.9.1

libsamba-hostconfig-devel-4.4.2-11.9.1

libwbclient0-debuginfo-4.4.2-11.9.1

libndr-standard0-debuginfo-4.4.2-11.9.1

libdcerpc-binding0-4.4.2-11.9.1

ctdb-tests-debuginfo-4.4.2-11.9.1

libndr-devel-4.4.2-11.9.1

libdcerpc-samr-devel-4.4.2-11.9.1

libwbclient0-4.4.2-11.9.1

libdcerpc0-4.4.2-11.9.1

libsamba-passdb0-4.4.2-11.9.1

libsamba-util-devel-4.4.2-11.9.1

libsamba-passdb-devel-4.4.2-11.9.1
ctdb-tests-4.4.2-11.9.1
libndr-nbt-devel-4.4.2-11.9.1
libsamba-credentials-devel-4.4.2-11.9.1
samba-winbind-4.4.2-11.9.1
libnetapi0-4.4.2-11.9.1
libndr0-debuginfo-4.4.2-11.9.1
libtevent-util0-4.4.2-11.9.1
libsmbclient0-debuginfo-4.4.2-11.9.1
samba-libs-4.4.2-11.9.1
samba-client-4.4.2-11.9.1
libsamba-passdb0-debuginfo-4.4.2-11.9.1
libsamba-policy0-debuginfo-4.4.2-11.9.1
libdcerpc-devel-4.4.2-11.9.1
samba-core-devel-4.4.2-11.9.1
libdcerpc-binding0-debuginfo-4.4.2-11.9.1
samba-winbind-debuginfo-4.4.2-11.9.1
ctdb-debuginfo-4.4.2-11.9.1
samba-4.4.2-11.9.1
libsamba-errors0-4.4.2-11.9.1
libsmbconf0-debuginfo-4.4.2-11.9.1
libsamdb-devel-4.4.2-11.9.1
libnetapi-devel-4.4.2-11.9.1
libsamba-hostconfig0-4.4.2-11.9.1
libsamba-util0-4.4.2-11.9.1
libndr-standard0-4.4.2-11.9.1
libdcerpc-samr0-4.4.2-11.9.1
libndr-nbt0-4.4.2-11.9.1
libndr-krb5pac0-debuginfo-4.4.2-11.9.1
libsmbclient0-4.4.2-11.9.1
samba-python-4.4.2-11.9.1
libsmbldap0-4.4.2-11.9.1
samba-test-debuginfo-4.4.2-11.9.1
libsmbconf-devel-4.4.2-11.9.1
samba-libs-debuginfo-4.4.2-11.9.1
libndr-nbt0-debuginfo-4.4.2-11.9.1
libsamba-credentials0-4.4.2-11.9.1
libsmbldap0-debuginfo-4.4.2-11.9.1
libsamba-errors-devel-4.4.2-11.9.1
samba-client-debuginfo-4.4.2-11.9.1
libndr0-4.4.2-11.9.1
samba-debugsource-4.4.2-11.9.1
libndr-krb5pac0-4.4.2-11.9.1
libnetapi0-debuginfo-4.4.2-11.9.1
ctdb-4.4.2-11.9.1
libdcerpc-samr0-debuginfo-4.4.2-11.9.1
libsamba-hostconfig0-debuginfo-4.4.2-11.9.1
libsmbconf0-4.4.2-11.9.1
libsamdb0-debuginfo-4.4.2-11.9.1
samba-debuginfo-4.4.2-11.9.1

noarch
samba-doc-4.4.2-11.9.1

x86_64
libdcerpc0-debuginfo-32bit-4.4.2-11.9.1
samba-winbind-32bit-4.4.2-11.9.1
libsmbconf0-32bit-4.4.2-11.9.1
libsamba-credentials0-debuginfo-4.4.2-11.9.1
libwbclient0-debuginfo-32bit-4.4.2-11.9.1

libsmbldap0-32bit-4.4.2-11.9.1
libdcerpc-samr0-32bit-4.4.2-11.9.1
libsamba-errors0-debuginfo-4.4.2-11.9.1
libsmbclient-devel-4.4.2-11.9.1
libtevent-util0-debuginfo-4.4.2-11.9.1
libndr-krb5pac-devel-4.4.2-11.9.1
libsamdb0-debuginfo-32bit-4.4.2-11.9.1
libsmbclient0-debuginfo-32bit-4.4.2-11.9.1
libsamba-util0-debuginfo-4.4.2-11.9.1
libsamba-credentials0-32bit-4.4.2-11.9.1
libsamba-policy0-debuginfo-32bit-4.4.2-11.9.1
libtevent-util0-debuginfo-32bit-4.4.2-11.9.1
libsamba-util0-debuginfo-32bit-4.4.2-11.9.1
libsamba-policy-devel-4.4.2-11.9.1
libtevent-util-devel-4.4.2-11.9.1
libndr-krb5pac0-32bit-4.4.2-11.9.1
samba-python-debuginfo-4.4.2-11.9.1
libsmbldap-devel-4.4.2-11.9.1
libsamba-policy0-4.4.2-11.9.1
libwbclient-devel-4.4.2-11.9.1
libndr-standard-devel-4.4.2-11.9.1
libdcerpc0-debuginfo-4.4.2-11.9.1
samba-test-4.4.2-11.9.1
libsamdb0-4.4.2-11.9.1
libsamba-hostconfig0-debuginfo-32bit-4.4.2-11.9.1
libndr-standard0-32bit-4.4.2-11.9.1
samba-pidl-4.4.2-11.9.1
libwbclient0-32bit-4.4.2-11.9.1
libsamba-hostconfig-devel-4.4.2-11.9.1
libwbclient0-debuginfo-4.4.2-11.9.1
libndr-standard0-debuginfo-4.4.2-11.9.1
libnetapi0-debuginfo-32bit-4.4.2-11.9.1
libsmbconf0-debuginfo-32bit-4.4.2-11.9.1
libndr0-32bit-4.4.2-11.9.1
libdcerpc-binding0-4.4.2-11.9.1
libdcerpc-samr0-debuginfo-32bit-4.4.2-11.9.1
ctdb-tests-debuginfo-4.4.2-11.9.1
libsamba-errors0-debuginfo-32bit-4.4.2-11.9.1
libdcerpc-binding0-32bit-4.4.2-11.9.1
libndr-devel-4.4.2-11.9.1
libdcerpc-samr-devel-4.4.2-11.9.1
libwbclient0-4.4.2-11.9.1
libdcerpc0-4.4.2-11.9.1
libsamba-passsdb0-4.4.2-11.9.1
libndr-nbt0-debuginfo-32bit-4.4.2-11.9.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-11.9.1
libsamba-util-devel-4.4.2-11.9.1
samba-client-debuginfo-32bit-4.4.2-11.9.1
libsamba-passsdb-devel-4.4.2-11.9.1
ctdb-tests-4.4.2-11.9.1
libndr-nbt-devel-4.4.2-11.9.1
libsamba-credentials-devel-4.4.2-11.9.1
libsamba-credentials0-debuginfo-32bit-4.4.2-11.9.1
samba-winbind-4.4.2-11.9.1
libnetapi0-4.4.2-11.9.1
libndr0-debuginfo-4.4.2-11.9.1
libtevent-util0-4.4.2-11.9.1
libsmbclient0-debuginfo-4.4.2-11.9.1
samba-libs-4.4.2-11.9.1
samba-client-4.4.2-11.9.1

libsamba-passdb0-debuginfo-4.4.2-11.9.1
libndr-krb5pac0-debuginfo-32bit-4.4.2-11.9.1
samba-libs-debuginfo-32bit-4.4.2-11.9.1
libsamba-policy0-debuginfo-4.4.2-11.9.1
libdcerpc-devel-4.4.2-11.9.1
samba-core-devel-4.4.2-11.9.1
libdcerpc-binding0-debuginfo-4.4.2-11.9.1
libsamba-policy0-32bit-4.4.2-11.9.1
samba-winbind-debuginfo-4.4.2-11.9.1
ctdb-debuginfo-4.4.2-11.9.1
libndr-standard0-debuginfo-32bit-4.4.2-11.9.1
samba-4.4.2-11.9.1
libsamba-errors0-4.4.2-11.9.1
libsmbconf0-debuginfo-4.4.2-11.9.1
libsamdb-devel-4.4.2-11.9.1
libnetapi-devel-4.4.2-11.9.1
libsamba-hostconfig0-4.4.2-11.9.1
libdcerpc0-32bit-4.4.2-11.9.1
libsamba-util0-4.4.2-11.9.1
libndr-standard0-4.4.2-11.9.1
libdcerpc-samr0-4.4.2-11.9.1
samba-libs-32bit-4.4.2-11.9.1
libndr-nbt0-4.4.2-11.9.1
libndr-krb5pac0-debuginfo-4.4.2-11.9.1
libsmbclient0-4.4.2-11.9.1
samba-python-4.4.2-11.9.1
libsamba-passdb0-debuginfo-32bit-4.4.2-11.9.1
libsmbldap0-4.4.2-11.9.1
samba-test-debuginfo-4.4.2-11.9.1
libtevent-util0-32bit-4.4.2-11.9.1
libsamba-passdb0-32bit-4.4.2-11.9.1
libsmbconf-devel-4.4.2-11.9.1
samba-libs-debuginfo-4.4.2-11.9.1
libndr-nbt0-debuginfo-4.4.2-11.9.1
libsmbclient0-32bit-4.4.2-11.9.1
libsamba-credentials0-4.4.2-11.9.1
libsmbldap0-debuginfo-4.4.2-11.9.1
libsamba-errors-devel-4.4.2-11.9.1
samba-client-debuginfo-4.4.2-11.9.1
libsamba-hostconfig0-32bit-4.4.2-11.9.1
libndr0-4.4.2-11.9.1
libnetapi0-32bit-4.4.2-11.9.1
libsamba-errors0-32bit-4.4.2-11.9.1
samba-debugsource-4.4.2-11.9.1
libndr-krb5pac0-4.4.2-11.9.1
samba-winbind-debuginfo-32bit-4.4.2-11.9.1
libnetapi0-debuginfo-4.4.2-11.9.1
libndr-nbt0-32bit-4.4.2-11.9.1
ctdb-4.4.2-11.9.1
libdcerpc-samr0-debuginfo-4.4.2-11.9.1
libsmbldap0-debuginfo-32bit-4.4.2-11.9.1
libsamba-util0-32bit-4.4.2-11.9.1
samba-client-32bit-4.4.2-11.9.1
libsamba-hostconfig0-debuginfo-4.4.2-11.9.1
libsmbconf0-4.4.2-11.9.1
libsamdb0-debuginfo-4.4.2-11.9.1
libndr0-debuginfo-32bit-4.4.2-11.9.1
libsamdb0-32bit-4.4.2-11.9.1
samba-debuginfo-4.4.2-11.9.1

145536 - SuSE Linux 42.2 openSUSE-SU-2017:0456-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8709, CVE-2016-7117, CVE-2016-8645, CVE-2016-9793, CVE-2016-9806, CVE-2016-9919, CVE-2017-2583, CVE-2017-2584, CVE-2017-5551, CVE-2017-5576, CVE-2017-5577

Description

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

openSUSE-SU-2017:0456-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00061.html>

SuSE Linux 42.2

x86_64

kernel-debug-base-debuginfo-4.4.46-11.1

kernel-vanilla-base-4.4.46-11.1

kernel-debug-base-4.4.46-11.1

kernel-obs-build-debugsource-4.4.46-11.1

kernel-debug-devel-debuginfo-4.4.46-11.1

kernel-vanilla-base-debuginfo-4.4.46-11.1

kernel-default-4.4.46-11.1

kernel-vanilla-4.4.46-11.1

kernel-vanilla-debugsource-4.4.46-11.1

kernel-default-devel-4.4.46-11.1

kernel-syms-4.4.46-11.1

kernel-vanilla-devel-4.4.46-11.1

kernel-obs-qa-4.4.46-11.1

kernel-default-debugsource-4.4.46-11.1

kernel-vanilla-debuginfo-4.4.46-11.1

kernel-debug-4.4.46-11.1

kernel-debug-debuginfo-4.4.46-11.1

kernel-debug-debugsource-4.4.46-11.1

kernel-default-base-debuginfo-4.4.46-11.1

kernel-default-base-4.4.46-11.1

kernel-obs-build-4.4.46-11.1

kernel-default-debuginfo-4.4.46-11.1

kernel-debug-devel-4.4.46-11.1

noarch

kernel-docs-pdf-4.4.46-11.3

kernel-docs-html-4.4.46-11.3

kernel-docs-4.4.46-11.3

kernel-macros-4.4.46-11.1

kernel-devel-4.4.46-11.1

kernel-source-vanilla-4.4.46-11.1

kernel-source-4.4.46-11.1

145548 - SuSE Linux 42.2 openSUSE-SU-2017:1826-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10912, CVE-2017-10913, CVE-2017-10914, CVE-2017-10915, CVE-2017-10917, CVE-2017-10918, CVE-2017-10920, CVE-2017-10921, CVE-2017-10922, CVE-2017-8309, CVE-2017-9330

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1826-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00047.html>

SuSE Linux 42.2

x86_64

xen-doc-html-4.7.2_06-11.9.1

xen-devel-4.7.2_06-11.9.1

xen-4.7.2_06-11.9.1

xen-tools-debuginfo-4.7.2_06-11.9.1

xen-libs-4.7.2_06-11.9.1

xen-tools-domU-4.7.2_06-11.9.1

xen-libs-debuginfo-32bit-4.7.2_06-11.9.1

xen-tools-4.7.2_06-11.9.1

xen-tools-domU-debuginfo-4.7.2_06-11.9.1

xen-libs-32bit-4.7.2_06-11.9.1

xen-libs-debuginfo-4.7.2_06-11.9.1

xen-debugsource-4.7.2_06-11.9.1

i586

xen-devel-4.7.2_06-11.9.1

xen-libs-4.7.2_06-11.9.1

xen-tools-domU-4.7.2_06-11.9.1

xen-tools-domU-debuginfo-4.7.2_06-11.9.1

xen-libs-debuginfo-4.7.2_06-11.9.1

xen-debugsource-4.7.2_06-11.9.1

145595 - SuSE Linux 42.1 openSUSE-SU-2017:0458-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-10147, CVE-2016-7117, CVE-2016-7917, CVE-2016-8645, CVE-2016-9793, CVE-2016-9806, CVE-2017-5551

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0458-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00062.html>

SuSE Linux 42.1

i586

kernel-default-debugsource-4.1.38-47.1

kernel-default-base-debuginfo-4.1.38-47.1

kernel-obs-build-4.1.38-47.3

kernel-default-base-4.1.38-47.1

kernel-obs-build-debugsource-4.1.38-47.3
kernel-obs-qa-4.1.38-47.1
kernel-default-debuginfo-4.1.38-47.1
kernel-syms-4.1.38-47.1
kernel-default-4.1.38-47.1
kernel-default-devel-4.1.38-47.1

i686

kernel-pv-devel-4.1.38-47.1
kernel-pv-base-debuginfo-4.1.38-47.1
kernel-ec2-debugsource-4.1.38-47.1
kernel-ec2-debuginfo-4.1.38-47.1
kernel-pae-4.1.38-47.1
kernel-debug-base-4.1.38-47.1
kernel-xen-base-debuginfo-4.1.38-47.1
kernel-pv-4.1.38-47.1
kernel-vanilla-debuginfo-4.1.38-47.1
kernel-pae-base-4.1.38-47.1
kernel-vanilla-4.1.38-47.1
kernel-xen-4.1.38-47.1
kernel-debug-debuginfo-4.1.38-47.1
kernel-xen-debugsource-4.1.38-47.1
kernel-vanilla-debugsource-4.1.38-47.1
kernel-pae-devel-4.1.38-47.1
kernel-debug-base-debuginfo-4.1.38-47.1
kernel-xen-devel-4.1.38-47.1
kernel-ec2-devel-4.1.38-47.1
kernel-pae-base-debuginfo-4.1.38-47.1
kernel-ec2-base-debuginfo-4.1.38-47.1
kernel-debug-devel-4.1.38-47.1
kernel-pae-debuginfo-4.1.38-47.1
kernel-xen-base-4.1.38-47.1
kernel-xen-debuginfo-4.1.38-47.1
kernel-ec2-base-4.1.38-47.1
kernel-pv-debuginfo-4.1.38-47.1
kernel-debug-4.1.38-47.1
kernel-pae-debugsource-4.1.38-47.1
kernel-ec2-4.1.38-47.1
kernel-pv-base-4.1.38-47.1
kernel-debug-devel-debuginfo-4.1.38-47.1
kernel-debug-debugsource-4.1.38-47.1
kernel-vanilla-devel-4.1.38-47.1
kernel-pv-debugsource-4.1.38-47.1

noarch

kernel-source-4.1.38-47.1
kernel-docs-html-4.1.38-47.2
kernel-macros-4.1.38-47.1
kernel-docs-4.1.38-47.2
kernel-source-vanilla-4.1.38-47.1
kernel-devel-4.1.38-47.1
kernel-docs-pdf-4.1.38-47.2

x86_64

kernel-pv-devel-4.1.38-47.1
kernel-pv-base-debuginfo-4.1.38-47.1
kernel-default-base-4.1.38-47.1
kernel-ec2-debugsource-4.1.38-47.1
kernel-ec2-debuginfo-4.1.38-47.1
kernel-debug-base-4.1.38-47.1

kernel-xen-base-debuginfo-4.1.38-47.1
kernel-default-4.1.38-47.1
kernel-pv-4.1.38-47.1
kernel-vanilla-debuginfo-4.1.38-47.1
kernel-obs-qa-4.1.38-47.1
kernel-obs-build-4.1.38-47.3
kernel-vanilla-4.1.38-47.1
kernel-xen-4.1.38-47.1
kernel-debug-debuginfo-4.1.38-47.1
kernel-xen-debugsource-4.1.38-47.1
kernel-default-base-debuginfo-4.1.38-47.1
kernel-vanilla-debugsource-4.1.38-47.1
kernel-debug-base-debuginfo-4.1.38-47.1
kernel-xen-devel-4.1.38-47.1
kernel-ec2-devel-4.1.38-47.1
kernel-ec2-base-debuginfo-4.1.38-47.1
kernel-debug-devel-4.1.38-47.1
kernel-syms-4.1.38-47.1
kernel-xen-base-4.1.38-47.1
kernel-default-debuginfo-4.1.38-47.1
kernel-xen-debuginfo-4.1.38-47.1
kernel-ec2-base-4.1.38-47.1
kernel-pv-debuginfo-4.1.38-47.1
kernel-debug-4.1.38-47.1
kernel-ec2-4.1.38-47.1
kernel-obs-build-debugsource-4.1.38-47.3
kernel-pv-base-4.1.38-47.1
kernel-debug-devel-debuginfo-4.1.38-47.1
kernel-default-devel-4.1.38-47.1
kernel-default-debugsource-4.1.38-47.1
kernel-debug-debugsource-4.1.38-47.1
kernel-vanilla-devel-4.1.38-47.1
kernel-pv-debugsource-4.1.38-47.1

145606 - SuSE Linux 42.2 openSUSE-SU-2017:0446-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4658, CVE-2016-9318, CVE-2016-9597

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0446-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00055.html>

SuSE Linux 42.2

i586

python-libxml2-2.9.4-3.1

libxml2-2-2.9.4-3.1

libxml2-tools-debuginfo-2.9.4-3.1

python-libxml2-debugsource-2.9.4-3.1

libxml2-tools-2.9.4-3.1

python-libxml2-debuginfo-2.9.4-3.1

libxml2-debugsource-2.9.4-3.1
libxml2-2-debuginfo-2.9.4-3.1
libxml2-devel-2.9.4-3.1

noarch
libxml2-doc-2.9.4-3.1

x86_64
python-libxml2-2.9.4-3.1
libxml2-2-2.9.4-3.1
libxml2-tools-debuginfo-2.9.4-3.1
python-libxml2-debugsource-2.9.4-3.1
libxml2-2-debuginfo-32bit-2.9.4-3.1
libxml2-tools-2.9.4-3.1
python-libxml2-debuginfo-2.9.4-3.1
libxml2-debugsource-2.9.4-3.1
libxml2-2-debuginfo-2.9.4-3.1
libxml2-devel-32bit-2.9.4-3.1
libxml2-devel-2.9.4-3.1
libxml2-2-32bit-2.9.4-3.1

145638 - SuSE Linux 42.2 openSUSE-SU-2017:1513-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7487, CVE-2017-7645, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9150

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1513-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00024.html>

SuSE Linux 42.2

x86_64
kernel-debug-devel-debuginfo-4.4.70-18.9.1
kernel-debug-base-4.4.70-18.9.1
kernel-obs-qa-4.4.70-18.9.1
kernel-default-base-debuginfo-4.4.70-18.9.1
kernel-vanilla-debugsource-4.4.70-18.9.1
kernel-debug-debuginfo-4.4.70-18.9.1
kernel-default-devel-4.4.70-18.9.1
kernel-debug-4.4.70-18.9.1
kernel-default-debugsource-4.4.70-18.9.1
kernel-debug-devel-4.4.70-18.9.1
kernel-debug-base-debuginfo-4.4.70-18.9.1
kernel-vanilla-debuginfo-4.4.70-18.9.1
kernel-vanilla-base-debuginfo-4.4.70-18.9.1
kernel-syms-4.4.70-18.9.1
kernel-obs-build-4.4.70-18.9.1
kernel-debug-debugsource-4.4.70-18.9.1
kernel-vanilla-base-4.4.70-18.9.1
kernel-default-4.4.70-18.9.1

kernel-default-debuginfo-4.4.70-18.9.1
kernel-vanilla-4.4.70-18.9.1
kernel-vanilla-devel-4.4.70-18.9.1
kernel-obs-build-debugsource-4.4.70-18.9.1
kernel-default-base-4.4.70-18.9.1

noarch
kernel-source-vanilla-4.4.70-18.9.1
kernel-docs-pdf-4.4.70-18.9.2
kernel-macros-4.4.70-18.9.1
kernel-docs-4.4.70-18.9.2
kernel-source-4.4.70-18.9.1
kernel-devel-4.4.70-18.9.1
kernel-docs-html-4.4.70-18.9.2

145728 - SuSE Linux 42.1 openSUSE-SU-2017:1415-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7494

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1415-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00087.html>

SuSE Linux 42.1

i586

libdcerpc-samr0-debuginfo-4.2.4-33.1
libndr-krb5pac0-4.2.4-33.1
libsamba-passdb0-4.2.4-33.1
libsamba-credentials0-4.2.4-33.1
libdcerpc-samr0-4.2.4-33.1
ctdb-4.2.4-33.1
libdcerpc-binding0-debuginfo-4.2.4-33.1
libregistry-devel-4.2.4-33.1
libsamba-util-devel-4.2.4-33.1
libsamba-passdb-devel-4.2.4-33.1
libtevent-util0-4.2.4-33.1
libwbclient-devel-4.2.4-33.1
libsmbldap0-debuginfo-4.2.4-33.1
libndr-standard0-debuginfo-4.2.4-33.1
libdcerpc0-debuginfo-4.2.4-33.1
libndr-standard-devel-4.2.4-33.1
samba-test-debuginfo-4.2.4-33.1
libtevent-util0-debuginfo-4.2.4-33.1
samba-python-debuginfo-4.2.4-33.1
samba-4.2.4-33.1
libgensec-devel-4.2.4-33.1
ctdb-debuginfo-4.2.4-33.1
libdcerpc0-4.2.4-33.1
libsamba-policy-devel-4.2.4-33.1
libsmbconf-devel-4.2.4-33.1

libsmbconf0-4.2.4-33.1
libsamba-policy0-4.2.4-33.1
ctdb-tests-4.2.4-33.1
libsmbconf0-debuginfo-4.2.4-33.1
libdcerpc-atSvc0-4.2.4-33.1
libsmbclient0-4.2.4-33.1
libndr-nbt-devel-4.2.4-33.1
libgensec0-4.2.4-33.1
libsamba-util0-debuginfo-4.2.4-33.1
samba-libs-4.2.4-33.1
libndr-krb5pac0-debuginfo-4.2.4-33.1
samba-pidl-4.2.4-33.1
samba-core-devel-4.2.4-33.1
samba-test-4.2.4-33.1
libsmbclient0-debuginfo-4.2.4-33.1
samba-libs-debuginfo-4.2.4-33.1
libsmbclient-raw0-debuginfo-4.2.4-33.1
libwbclient0-debuginfo-4.2.4-33.1
libdcerpc-devel-4.2.4-33.1
libsmbldap0-4.2.4-33.1
samba-debugsource-4.2.4-33.1
libsmbclient-raw0-4.2.4-33.1
libsamdb0-debuginfo-4.2.4-33.1
libsamdb0-4.2.4-33.1
ctdb-devel-4.2.4-33.1
libsmbclient-raw-devel-4.2.4-33.1
libsamba-credentials-devel-4.2.4-33.1
libndr-standard0-4.2.4-33.1
libdcerpc-atSvc-devel-4.2.4-33.1
samba-client-4.2.4-33.1
samba-python-4.2.4-33.1
libsamba-policy0-debuginfo-4.2.4-33.1
libsamdb-devel-4.2.4-33.1
libndr-devel-4.2.4-33.1
libtevent-util-devel-4.2.4-33.1
samba-client-debuginfo-4.2.4-33.1
libsamba-credentials0-debuginfo-4.2.4-33.1
libndr-nbt0-4.2.4-33.1
ctdb-tests-debuginfo-4.2.4-33.1
libsamba-util0-4.2.4-33.1
libdcerpc-atSvc0-debuginfo-4.2.4-33.1
samba-winbind-debuginfo-4.2.4-33.1
samba-debuginfo-4.2.4-33.1
libsmbclient-devel-4.2.4-33.1
libndr-krb5pac-devel-4.2.4-33.1
libnetapi0-4.2.4-33.1
libwbclient0-4.2.4-33.1
libsamba-hostconfig0-debuginfo-4.2.4-33.1
libregistry0-4.2.4-33.1
libnetapi0-debuginfo-4.2.4-33.1
libdcerpc-binding0-4.2.4-33.1
libsamba-hostconfig-devel-4.2.4-33.1
libndr0-4.2.4-33.1
libsamba-hostconfig0-4.2.4-33.1
libdcerpc-samr-devel-4.2.4-33.1
libsmbldap-devel-4.2.4-33.1
samba-test-devel-4.2.4-33.1
samba-winbind-4.2.4-33.1
libndr0-debuginfo-4.2.4-33.1
libgensec0-debuginfo-4.2.4-33.1

libregistry0-debuginfo-4.2.4-33.1
libnetapi-devel-4.2.4-33.1
libndr-nbt0-debuginfo-4.2.4-33.1
libsamba-passdb0-debuginfo-4.2.4-33.1

noarch
samba-doc-4.2.4-33.1

x86_64
samba-pidl-4.2.4-33.1
libndr0-debuginfo-32bit-4.2.4-33.1
libndr-krb5pac0-debuginfo-4.2.4-33.1
samba-test-debuginfo-4.2.4-33.1
samba-python-debuginfo-4.2.4-33.1
libsamba-credentials-devel-4.2.4-33.1
libregistry0-32bit-4.2.4-33.1
libsamba-credentials0-debuginfo-4.2.4-33.1
libtevent-util0-debuginfo-32bit-4.2.4-33.1
libtevent-util-devel-4.2.4-33.1
libndr-krb5pac0-4.2.4-33.1
libsamba-passdb0-debuginfo-4.2.4-33.1
libdcerpc-binding0-32bit-4.2.4-33.1
libsmbldap0-debuginfo-4.2.4-33.1
libdcerpc-atsvc-devel-4.2.4-33.1
libsamba-policy-devel-4.2.4-33.1
libwbclient0-32bit-4.2.4-33.1
libsmbclient0-debuginfo-32bit-4.2.4-33.1
libsamba-util0-debuginfo-4.2.4-33.1
libndr-devel-4.2.4-33.1
libdcerpc0-32bit-4.2.4-33.1
samba-core-devel-4.2.4-33.1
libsmbclient-raw0-32bit-4.2.4-33.1
libsamba-policy0-debuginfo-32bit-4.2.4-33.1
libtevent-util0-4.2.4-33.1
libndr0-4.2.4-33.1
libndr-nbt0-32bit-4.2.4-33.1
libndr-nbt-devel-4.2.4-33.1
samba-client-32bit-4.2.4-33.1
libsmbclient-raw-devel-4.2.4-33.1
libndr-krb5pac-devel-4.2.4-33.1
libwbclient0-debuginfo-32bit-4.2.4-33.1
libdcerpc-samr0-debuginfo-32bit-4.2.4-33.1
libndr-standard0-debuginfo-4.2.4-33.1
libgensec0-4.2.4-33.1
libsmbclient-devel-4.2.4-33.1
libsamdb0-debuginfo-4.2.4-33.1
libdcerpc-atsvc0-4.2.4-33.1
samba-debuginfo-4.2.4-33.1
libdcerpc-samr0-32bit-4.2.4-33.1
samba-winbind-debuginfo-32bit-4.2.4-33.1
libtevent-util0-32bit-4.2.4-33.1
libndr-standard0-debuginfo-32bit-4.2.4-33.1
libtevent-util0-debuginfo-4.2.4-33.1
libsamdb0-32bit-4.2.4-33.1
libndr-krb5pac0-32bit-4.2.4-33.1
libsmbclient0-4.2.4-33.1
libsamba-credentials0-32bit-4.2.4-33.1
samba-test-devel-4.2.4-33.1
libndr-standard0-32bit-4.2.4-33.1
libsamdb-devel-4.2.4-33.1

libdcerpc-at svc0-debuginfo-32bit-4.2.4-33.1
libdcerpc-samr-devel-4.2.4-33.1
samba-python-4.2.4-33.1
libsmbconf0-debuginfo-4.2.4-33.1
libndr0-debuginfo-4.2.4-33.1
libsamba-util0-32bit-4.2.4-33.1
libdcerpc0-debuginfo-32bit-4.2.4-33.1
libdcerpc-binding0-debuginfo-4.2.4-33.1
libsmbconf0-debuginfo-32bit-4.2.4-33.1
libgensec0-debuginfo-32bit-4.2.4-33.1
libnetapi0-4.2.4-33.1
libwbclient0-debuginfo-4.2.4-33.1
libdcerpc-samr0-debuginfo-4.2.4-33.1
libndr-krb5pac0-debuginfo-32bit-4.2.4-33.1
libnetapi-devel-4.2.4-33.1
samba-client-debuginfo-32bit-4.2.4-33.1
samba-libs-4.2.4-33.1
libndr-nbt0-debuginfo-4.2.4-33.1
libsamba-policy0-4.2.4-33.1
libgensec-devel-4.2.4-33.1
samba-client-debuginfo-4.2.4-33.1
libdcerpc0-debuginfo-4.2.4-33.1
samba-client-4.2.4-33.1
samba-winbind-4.2.4-33.1
libgensec0-32bit-4.2.4-33.1
libsamba-hostconfig0-4.2.4-33.1
libsamba-util0-4.2.4-33.1
libsamba-passdb-devel-4.2.4-33.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-33.1
ctdb-tests-4.2.4-33.1
libsamba-util0-debuginfo-32bit-4.2.4-33.1
libsmbclient0-debuginfo-4.2.4-33.1
samba-4.2.4-33.1
libsamba-credentials0-debuginfo-32bit-4.2.4-33.1
libsmbconf-devel-4.2.4-33.1
samba-debugsource-4.2.4-33.1
libsamba-passdb0-32bit-4.2.4-33.1
samba-libs-32bit-4.2.4-33.1
libdcerpc-at svc0-32bit-4.2.4-33.1
libdcerpc-binding0-4.2.4-33.1
libregistry0-debuginfo-32bit-4.2.4-33.1
samba-debuginfo-32bit-4.2.4-33.1
libsamba-hostconfig0-debuginfo-4.2.4-33.1
libsamba-hostconfig0-32bit-4.2.4-33.1
libdcerpc-samr0-4.2.4-33.1
libregistry0-4.2.4-33.1
libsamdb0-debuginfo-32bit-4.2.4-33.1
libsmbldap0-32bit-4.2.4-33.1
libndr-nbt0-4.2.4-33.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-33.1
samba-32bit-4.2.4-33.1
samba-libs-debuginfo-4.2.4-33.1
libsamba-util-devel-4.2.4-33.1
libsmbclient-raw0-debuginfo-4.2.4-33.1
ctdb-debuginfo-4.2.4-33.1
libnetapi0-debuginfo-4.2.4-33.1
libwbclient0-4.2.4-33.1
libsmbconf0-4.2.4-33.1
libregistry0-debuginfo-4.2.4-33.1
libndr-nbt0-debuginfo-32bit-4.2.4-33.1

libsmbldap0-debuginfo-32bit-4.2.4-33.1
libdcerpc0-4.2.4-33.1
ctdb-devel-4.2.4-33.1
libnetapi0-32bit-4.2.4-33.1
libgensec0-debuginfo-4.2.4-33.1
libsmbconf0-32bit-4.2.4-33.1
libsmbclient0-32bit-4.2.4-33.1
libsmbldap-devel-4.2.4-33.1
libregistry-devel-4.2.4-33.1
ctdb-4.2.4-33.1
libsmbldap0-4.2.4-33.1
libsamdb0-4.2.4-33.1
libndr-standard-devel-4.2.4-33.1
libsamba-policy0-debuginfo-4.2.4-33.1
ctdb-tests-debuginfo-4.2.4-33.1
libsmbclient-raw0-4.2.4-33.1
libsamba-hostconfig-devel-4.2.4-33.1

145767 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0022-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9957, CVE-2016-9958, CVE-2016-9959, CVE-2016-9960, CVE-2016-9961

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0022-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00011.html>

SuSE Linux 42.1

x86_64

libgme0-debuginfo-32bit-0.6.0-7.1
libgme0-0.6.0-7.1
libgme0-debuginfo-0.6.0-7.1
libgme-devel-0.6.0-7.1
libgme0-32bit-0.6.0-7.1
libgme-debugsource-0.6.0-7.1

i586

libgme-debugsource-0.6.0-7.1
libgme-devel-0.6.0-7.1
libgme0-debuginfo-0.6.0-7.1
libgme0-0.6.0-7.1

SuSE Linux 42.2

x86_64

libgme0-0.6.0-8.1
libgme0-32bit-0.6.0-8.1
libgme-devel-0.6.0-8.1
libgme-debugsource-0.6.0-8.1
libgme0-debuginfo-32bit-0.6.0-8.1
libgme0-debuginfo-0.6.0-8.1

i586
libgme0-0.6.0-8.1
libgme-devel-0.6.0-8.1
libgme-debugsource-0.6.0-8.1
libgme0-debuginfo-0.6.0-8.1

145837 - SuSE SLES 11 SP4 SUSE-SU-2017:2342-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9922, CVE-2015-3288, CVE-2015-8970, CVE-2016-10200, CVE-2016-2188, CVE-2016-4997, CVE-2016-4998, CVE-2016-5243, CVE-2016-7117, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-11176, CVE-2017-11473, CVE-2017-2636, CVE-2017-2647, CVE-2017-2671, CVE-2017-5669, CVE-2017-5970, CVE-2017-5986, CVE-2017-6074, CVE-2017-6214, CVE-2017-6348, CVE-2017-6353, CVE-2017-6951, CVE-2017-7184, CVE-2017-7187, CVE-2017-7261, CVE-2017-7294, CVE-2017-7308, CVE-2017-7482, CVE-2017-7487, CVE-2017-7533, CVE-2017-7542, CVE-2017-7616, CVE-2017-8890, CVE-2017-8924, CVE-2017-8925, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2342-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-September/003182.html>

SuSE SLES 11 SP4

x86_64
kernel-rt_trace-base-3.0.101.rt130-69.5.1
kernel-source-rt-3.0.101.rt130-69.5.1
kernel-rt-3.0.101.rt130-69.5.1
kernel-rt-base-3.0.101.rt130-69.5.1
kernel-syms-rt-3.0.101.rt130-69.5.1
kernel-rt-devel-3.0.101.rt130-69.5.1
kernel-rt_trace-3.0.101.rt130-69.5.1
kernel-rt_trace-devel-3.0.101.rt130-69.5.1

145874 - SuSE Linux 42.1 openSUSE-SU-2017:0487-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2108, CVE-2016-7056, CVE-2016-8610, CVE-2017-3731

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0487-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00075.html>

SuSE Linux 42.1

i586

openssl-debuginfo-1.0.1i-21.1
openssl-debugsource-1.0.1i-21.1
libopenssl1_0_0-hmac-1.0.1i-21.1
libopenssl-devel-1.0.1i-21.1
libopenssl1_0_0-debuginfo-1.0.1i-21.1
openssl-1.0.1i-21.1
libopenssl1_0_0-1.0.1i-21.1

noarch
openssl-doc-1.0.1i-21.1

x86_64
openssl-debuginfo-1.0.1i-21.1
libopenssl1_0_0-32bit-1.0.1i-21.1
openssl-debugsource-1.0.1i-21.1
libopenssl1_0_0-hmac-1.0.1i-21.1
libopenssl-devel-1.0.1i-21.1
libopenssl1_0_0-debuginfo-32bit-1.0.1i-21.1
libopenssl1_0_0-debuginfo-1.0.1i-21.1
libopenssl1_0_0-hmac-32bit-1.0.1i-21.1
libopenssl-devel-32bit-1.0.1i-21.1
openssl-1.0.1i-21.1
libopenssl1_0_0-1.0.1i-21.1

145875 - SuSE Linux 42.2 openSUSE-SU-2017:1797-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6706

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1797-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00027.html>

SuSE Linux 42.2
x86_64
clamav-debuginfo-0.99.2-16.3.1
clamav-debugsource-0.99.2-16.3.1
clamav-0.99.2-16.3.1

22335 - (K35520031) F5 BIG-IP Virtual Server With HTTP Explicit Proxy And/Or SOCKS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5700

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw occurs when HTTP Explicit Proxy functionality and/or SOCKS profiles are configured on virtual servers. Successful exploitation could allow an attacker to execute arbitrary code, retrieve sensitive data or make unauthorized modifications on the target system.

130872 - Debian Linux 8.0, 9.0 DSA-3963-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000115, CVE-2017-1000116, CVE-2017-9462

Description

The scan detected that the host is missing the following update:
DSA-3963-1

Observation

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

<http://www.debian.org/security/2017/dsa-3963>

Debian 8.0
all
mercurial_3.1.2-2+deb8u4

Debian 9.0
all
mercurial_4.0-1+deb9u1

145511 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0510-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0381

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0510-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00089.html>

SuSE Linux 42.1
x86_64
libopus0-1.1-5.1
libopus0-32bit-1.1-5.1
opus-debugsource-1.1-5.1
libopus-devel-1.1-5.1
libopus0-debuginfo-1.1-5.1
libopus-devel-static-1.1-5.1
libopus0-debuginfo-32bit-1.1-5.1

i586
libopus-devel-1.1-5.1
libopus0-1.1-5.1
libopus-devel-static-1.1-5.1
libopus0-debuginfo-1.1-5.1
opus-debugsource-1.1-5.1

SuSE Linux 42.2
x86_64
libopus0-debuginfo-1.1-6.1
opus-debugsource-1.1-6.1
libopus0-debuginfo-32bit-1.1-6.1
libopus-devel-1.1-6.1
libopus-devel-static-1.1-6.1
libopus0-1.1-6.1
libopus0-32bit-1.1-6.1

i586
libopus-devel-1.1-6.1
libopus0-1.1-6.1
libopus0-debuginfo-1.1-6.1
opus-debugsource-1.1-6.1
libopus-devel-static-1.1-6.1

145541 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1124-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7572

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1124-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00107.html>

SuSE Linux 42.1
noarch
backintime-lang-1.1.20-3.1
backintime-qt4-1.1.20-3.1
backintime-1.1.20-3.1

SuSE Linux 42.2
noarch
backintime-qt4-1.1.20-3.3.1
backintime-1.1.20-3.3.1
backintime-lang-1.1.20-3.3.1

145556 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0942-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8540, CVE-2016-10087

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0942-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00026.html>

SuSE Linux 42.1

x86_64

libpng12-devel-1.2.50-11.1
libpng12-debugsource-1.2.50-11.1
libpng12-compat-devel-1.2.50-11.1
libpng12-devel-32bit-1.2.50-11.1
libpng12-0-debuginfo-32bit-1.2.50-11.1
libpng12-compat-devel-32bit-1.2.50-11.1
libpng12-0-32bit-1.2.50-11.1
libpng12-0-1.2.50-11.1
libpng12-0-debuginfo-1.2.50-11.1

i586

libpng12-devel-1.2.50-11.1
libpng12-debugsource-1.2.50-11.1
libpng12-0-debuginfo-1.2.50-11.1
libpng12-compat-devel-1.2.50-11.1
libpng12-0-1.2.50-11.1

SuSE Linux 42.2

x86_64

libpng12-compat-devel-32bit-1.2.50-10.3.1
libpng12-0-debuginfo-1.2.50-10.3.1
libpng12-devel-32bit-1.2.50-10.3.1
libpng12-0-debuginfo-32bit-1.2.50-10.3.1
libpng12-debugsource-1.2.50-10.3.1
libpng12-devel-1.2.50-10.3.1
libpng12-0-1.2.50-10.3.1
libpng12-0-32bit-1.2.50-10.3.1
libpng12-compat-devel-1.2.50-10.3.1

i586

libpng12-0-1.2.50-10.3.1
libpng12-debugsource-1.2.50-10.3.1
libpng12-devel-1.2.50-10.3.1
libpng12-0-debuginfo-1.2.50-10.3.1
libpng12-compat-devel-1.2.50-10.3.1

145589 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1037-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8540, CVE-2016-10087

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1037-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00063.html>

SuSE Linux 42.1

x86_64

libpng15-15-debuginfo-32bit-1.5.22-7.1

libpng15-15-32bit-1.5.22-7.1

libpng15-15-1.5.22-7.1

libpng15-debugsource-1.5.22-7.1

libpng15-15-debuginfo-1.5.22-7.1

i586

libpng15-15-1.5.22-7.1

libpng15-debugsource-1.5.22-7.1

libpng15-15-debuginfo-1.5.22-7.1

SuSE Linux 42.2

x86_64

libpng15-debugsource-1.5.22-5.3.1

libpng15-15-debuginfo-1.5.22-5.3.1

libpng15-15-debuginfo-32bit-1.5.22-5.3.1

libpng15-15-32bit-1.5.22-5.3.1

libpng15-15-1.5.22-5.3.1

i586

libpng15-debugsource-1.5.22-5.3.1

libpng15-15-debuginfo-1.5.22-5.3.1

libpng15-15-1.5.22-5.3.1

145727 - SuSE Linux 42.2 openSUSE-SU-2017:1572-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9462

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1572-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00049.html>

SuSE Linux 42.2

i586

mercurial-debugsource-3.8.3-2.5.1

mercurial-3.8.3-2.5.1

mercurial-debuginfo-3.8.3-2.5.1

noarch

mercurial-lang-3.8.3-2.5.1

x86_64
mercurial-debugsource-3.8.3-2.5.1
mercurial-3.8.3-2.5.1
mercurial-debuginfo-3.8.3-2.5.1

145807 - SuSE Linux 42.2 openSUSE-SU-2017:1390-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7995, CVE-2015-9019, CVE-2016-4738, CVE-2017-5029

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1390-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00079.html>

SuSE Linux 42.2

x86_64
libxslt1-1.1.28-10.3.1
libxslt1-debuginfo-32bit-1.1.28-10.3.1
libxslt-devel-32bit-1.1.28-10.3.1
libxslt1-debuginfo-1.1.28-10.3.1
libxslt-debugsource-1.1.28-10.3.1
libxslt-python-debugsource-1.1.28-10.3.1
libxslt-python-debuginfo-1.1.28-10.3.1
libxslt1-32bit-1.1.28-10.3.1
libxslt-tools-1.1.28-10.3.1
libxslt-devel-1.1.28-10.3.1
libxslt-tools-debuginfo-1.1.28-10.3.1
libxslt-python-1.1.28-10.3.1

i586

libxslt1-1.1.28-10.3.1
libxslt1-debuginfo-1.1.28-10.3.1
libxslt-debugsource-1.1.28-10.3.1
libxslt-python-debugsource-1.1.28-10.3.1
libxslt-python-debuginfo-1.1.28-10.3.1
libxslt-tools-1.1.28-10.3.1
libxslt-devel-1.1.28-10.3.1
libxslt-tools-debuginfo-1.1.28-10.3.1
libxslt-python-1.1.28-10.3.1

145842 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2207-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10081

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2207-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00081.html>

SuSE Linux 42.2

noarch

shutter-0.93.1-2.3.1

shutter-lang-0.93.1-2.3.1

SuSE Linux 42.3

noarch

shutter-0.93.1-5.1

shutter-lang-0.93.1-5.1

22311 - (K34125394) F5 BIG-IP Apache HTTPD Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-3167

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in Apache HTTPD component. Successful exploitation could allow an attacker to bypass certain security restrictions.

22337 - IBM WebSphere Portal Apache Multiple Vulnerabilities (swg22006871)

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

Risk Level: High

CVE: CVE-2017-5661, CVE-2017-5662

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Portal.

Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

Multiple vulnerabilities are present in some versions of IBM WebSphere Portal. The flaws lie in the Apache FOP and Batik sub components. Successful exploitation could allow an attacker to cause a denial of service condition or retrieve sensitive data.

22391 - (S2-052) Apache Struts REST Plugin Deserialization Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-9805

Description

A remote code execution vulnerability is present in some versions of Apache Struts.

Observation

Apache Struts is a popular Java web application framework.

A remote code execution vulnerability is present in some versions of Apache Struts. The flaw is due to unsafe deserialization in REST plugin with XStream handler. Successful exploitation could allow an attacker to execute arbitrary code.

22323 - (K24613253) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-2516

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the NTP component. Successful exploitation could allow attacker to cause a denial of service condition on the target system.

22336 - (K95432245) F5 BIG-IP PHP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5768

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the PHP component. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial-of-service condition on target system.

22338 - Advantech WebAccess Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Advantech WebAccess.

Observation

Advantech WebAccess is a web-based HMI software application used in energy, manufacturing, and building automation systems.

Multiple vulnerabilities are present in some versions of Advantech WebAccess. The flaws exist in multiple components. Successful exploitation could allow a remote attacker to execute arbitrary code.

22341 - (K18829561) F5 BIG-IP BIND Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-2776

Description

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

Observation

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

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

22342 - (K16838) F5 BIG-IP Enterprise Manager Configuration Utilities XSS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-1470

Description

A cross-site scripting vulnerability is present in some versions of F5's BIG-IP products.

Observation

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

A cross-site scripting vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the Configuration utility, specifically in the login.jsp file. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22343 - (K38871451) F5 BIG-IP TIFF Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-7554

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the LibTIFF component. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or possibly have other unspecified impact on the target system.

22345 - (K15104541) F5 BIG-IP Expat XML Library Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-1283, CVE-2015-2716

Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP Products.

Observation

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

Multiple vulnerabilities are present in some versions of F5's BIG-IP Products. The flaws lie in the iControl SOAP component. Successful exploitation could allow an attacker to cause a denial-of-service condition or other unspecified impact on target system.

22352 - Wireshark Denial-of-Service Vulnerability Prior To 2.0.15

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

Risk Level: High

CVE: CVE-2017-13767

Description

A vulnerability is present in some versions of Wireshark.

Observation

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

A vulnerability is present in some versions of Wireshark. The flaw lies in MSDP dissector. Successful exploitation could allow an attacker to cause a denial of service condition.

132396 - Oracle VM OVMSA-2017-0148 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12135, CVE-2017-12137, CVE-2017-12855

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0148

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000774.html>

OVM3.3
x86_64
xen-tools-4.3.0-55.el6.186.45
xen-4.3.0-55.el6.186.45

132397 - Oracle VM OVMSA-2017-0149 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12135, CVE-2017-12137, CVE-2017-12855

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0149

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000775.html>

OVM3.2
x86_64
xen-tools-4.1.3-25.el5.223.82
xen-4.1.3-25.el5.223.82
xen-devel-4.1.3-25.el5.223.82

141699 - Red Hat Enterprise Linux RHSA-2017-2596 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3253, CVE-2016-6814

Description

The scan detected that the host is missing the following update:
RHSA-2017-2596

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-September/msg00009.html>

RHEL6_7S
noarch
rh-maven33-groovy-1.8.9-7.19.el6
rh-maven33-groovy-javadoc-1.8.9-7.19.el6

RHEL6S
noarch
rh-maven33-groovy-1.8.9-7.19.el6
rh-maven33-groovy-javadoc-1.8.9-7.19.el6

RHEL6WS
noarch
rh-maven33-groovy-1.8.9-7.19.el6
rh-maven33-groovy-javadoc-1.8.9-7.19.el6

RHEL7S
noarch
rh-maven33-groovy-javadoc-1.8.9-7.19.el7
rh-maven33-groovy-1.8.9-7.19.el7

RHEL7WS
noarch
rh-maven33-groovy-javadoc-1.8.9-7.19.el7
rh-maven33-groovy-1.8.9-7.19.el7

145506 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2209-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7782, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7798, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7804, CVE-2017-7807

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2209-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00083.html>

SuSE Linux 42.2

x86_64

MozillaThunderbird-devel-52.3.0-41.15.1
MozillaThunderbird-debugsource-52.3.0-41.15.1
MozillaThunderbird-translations-common-52.3.0-41.15.1
MozillaThunderbird-buildsymbols-52.3.0-41.15.1
MozillaThunderbird-debuginfo-52.3.0-41.15.1
MozillaThunderbird-52.3.0-41.15.1
MozillaThunderbird-translations-other-52.3.0-41.15.1

i586

MozillaThunderbird-devel-52.3.0-41.15.1
MozillaThunderbird-debugsource-52.3.0-41.15.1
MozillaThunderbird-translations-common-52.3.0-41.15.1
MozillaThunderbird-buildsymbols-52.3.0-41.15.1
MozillaThunderbird-debuginfo-52.3.0-41.15.1
MozillaThunderbird-52.3.0-41.15.1
MozillaThunderbird-translations-other-52.3.0-41.15.1

SuSE Linux 42.3

x86_64

MozillaThunderbird-debugsource-52.3.0-44.1
MozillaThunderbird-debuginfo-52.3.0-44.1
MozillaThunderbird-buildsymbols-52.3.0-44.1
MozillaThunderbird-devel-52.3.0-44.1
MozillaThunderbird-52.3.0-44.1
MozillaThunderbird-translations-common-52.3.0-44.1
MozillaThunderbird-translations-other-52.3.0-44.1

i586

MozillaThunderbird-debugsource-52.3.0-44.1
MozillaThunderbird-debuginfo-52.3.0-44.1
MozillaThunderbird-buildsymbols-52.3.0-44.1
MozillaThunderbird-devel-52.3.0-44.1
MozillaThunderbird-52.3.0-44.1
MozillaThunderbird-translations-common-52.3.0-44.1
MozillaThunderbird-translations-other-52.3.0-44.1

145510 - SuSE Linux 42.2 openSUSE-SU-2017:1825-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000365, CVE-2017-7518

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1825-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00046.html>

SuSE Linux 42.2

x86_64

kernel-obs-build-debugsource-4.4.74-18.20.1

kernel-vanilla-base-4.4.74-18.20.1

kernel-debug-devel-4.4.74-18.20.1

kernel-debug-base-debuginfo-4.4.74-18.20.1

kernel-default-debugsource-4.4.74-18.20.1

kernel-vanilla-base-debuginfo-4.4.74-18.20.1

kernel-default-debuginfo-4.4.74-18.20.1

kernel-debug-4.4.74-18.20.1

kernel-default-devel-4.4.74-18.20.1

kernel-debug-debuginfo-4.4.74-18.20.1

kernel-debug-debugsource-4.4.74-18.20.1

kernel-vanilla-4.4.74-18.20.1

kernel-debug-base-4.4.74-18.20.1

kernel-obs-qa-4.4.74-18.20.1

kernel-default-base-4.4.74-18.20.1

kernel-default-4.4.74-18.20.1

kernel-vanilla-devel-4.4.74-18.20.1

kernel-default-base-debuginfo-4.4.74-18.20.1

kernel-syms-4.4.74-18.20.1

kernel-debug-devel-debuginfo-4.4.74-18.20.1

kernel-vanilla-debuginfo-4.4.74-18.20.1

kernel-obs-build-4.4.74-18.20.1

kernel-vanilla-debugsource-4.4.74-18.20.1

noarch

kernel-source-4.4.74-18.20.1

kernel-docs-html-4.4.74-18.20.3

kernel-docs-pdf-4.4.74-18.20.3

kernel-docs-4.4.74-18.20.3

kernel-devel-4.4.74-18.20.1

kernel-source-vanilla-4.4.74-18.20.1

kernel-macros-4.4.74-18.20.1

145514 - SuSE Linux 42.2 openSUSE-SU-2017:1882-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10684, CVE-2017-10685

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1882-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00071.html>

SuSE Linux 42.2

x86_64

libncurses5-debuginfo-5.9-55.3.1

libncurses6-32bit-5.9-55.3.1

libncurses5-32bit-5.9-55.3.1

ncurses-devel-5.9-55.3.1

libncurses6-5.9-55.3.1

ncurses-devel-32bit-5.9-55.3.1

terminfo-5.9-55.3.1

tack-5.9-55.3.1

ncurses-debugsource-5.9-55.3.1

terminfo-base-5.9-55.3.1

libncurses6-debuginfo-32bit-5.9-55.3.1

libncurses5-debuginfo-32bit-5.9-55.3.1

ncurses-utils-debuginfo-5.9-55.3.1

tack-debuginfo-5.9-55.3.1

ncurses-utils-5.9-55.3.1

ncurses-devel-debuginfo-32bit-5.9-55.3.1

libncurses5-5.9-55.3.1

libncurses6-debuginfo-5.9-55.3.1

ncurses-devel-debuginfo-5.9-55.3.1

i586

libncurses5-debuginfo-5.9-55.3.1

ncurses-devel-5.9-55.3.1

libncurses6-5.9-55.3.1

terminfo-5.9-55.3.1

tack-5.9-55.3.1

ncurses-debugsource-5.9-55.3.1

terminfo-base-5.9-55.3.1

ncurses-utils-debuginfo-5.9-55.3.1

tack-debuginfo-5.9-55.3.1

ncurses-utils-5.9-55.3.1

libncurses5-5.9-55.3.1

libncurses6-debuginfo-5.9-55.3.1

ncurses-devel-debuginfo-5.9-55.3.1

145515 - SuSE Linux 42.2 openSUSE-SU-2017:1822-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7526

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1822-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00043.html>

SuSE Linux 42.2

x86_64

libgrypt-cavs-debuginfo-1.6.1-34.6.1

libgrypt-devel-1.6.1-34.6.1

libgrypt20-hmac-1.6.1-34.6.1

libgrypt-devel-debuginfo-1.6.1-34.6.1

libgrypt20-debuginfo-1.6.1-34.6.1

libgrypt20-debuginfo-32bit-1.6.1-34.6.1

libgrypt-debugsource-1.6.1-34.6.1

libgrypt-devel-debuginfo-32bit-1.6.1-34.6.1

libgrypt20-1.6.1-34.6.1

libgrypt-devel-32bit-1.6.1-34.6.1

libgrypt-cavs-1.6.1-34.6.1

libgrypt20-hmac-32bit-1.6.1-34.6.1

libgrypt20-32bit-1.6.1-34.6.1

i586

libgrypt20-1.6.1-34.6.1

libgrypt-cavs-debuginfo-1.6.1-34.6.1

libgrypt-devel-1.6.1-34.6.1

libgrypt-debugsource-1.6.1-34.6.1

libgrypt-cavs-1.6.1-34.6.1

libgrypt20-hmac-1.6.1-34.6.1

libgrypt20-debuginfo-1.6.1-34.6.1

libgrypt-devel-debuginfo-1.6.1-34.6.1

145517 - SuSE Linux 42.1 openSUSE-SU-2017:0043-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:0043-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00016.html>

SuSE Linux 42.1

i586

syncthing-0.14.16-11.1

noarch

syncthing-gtk-lang-0.9.2.3-6.1

syncthing-gtk-0.9.2.3-6.1

x86_64

syncthing-0.14.16-11.1

145519 - SuSE Linux 42.2 openSUSE-SU-2017:0828-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-4433

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0828-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00093.html>

SuSE Linux 42.2

i586

gegl-0_2-0.2.0-16.1

gegl-debugsource-0.2.0-16.1

gegl-0.2.0-16.1

gegl-debuginfo-0.2.0-16.1

libgegl-0_2-0-0.2.0-16.1

gegl-0_2-debuginfo-0.2.0-16.1

gegl-doc-0.2.0-16.1

gegl-devel-0.2.0-16.1

libgegl-0_2-0-debuginfo-0.2.0-16.1

noarch

gegl-0_2-lang-0.2.0-16.1

x86_64

gegl-0_2-0.2.0-16.1

gegl-debugsource-0.2.0-16.1

gegl-0.2.0-16.1

gegl-debuginfo-0.2.0-16.1

libgegl-0_2-0-0.2.0-16.1

gegl-0_2-debuginfo-0.2.0-16.1

gegl-doc-0.2.0-16.1

gegl-devel-0.2.0-16.1

libgegl-0_2-0-debuginfo-0.2.0-16.1

145523 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0512-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5225

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0512-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00091.html>

SuSE Linux 42.1

x86_64
libtiff5-debuginfo-32bit-4.0.7-15.1
libtiff5-32bit-4.0.7-15.1
libtiff5-4.0.7-15.1
tiff-debugsource-4.0.7-15.1
libtiff-devel-32bit-4.0.7-15.1
libtiff5-debuginfo-4.0.7-15.1
tiff-4.0.7-15.1
libtiff-devel-4.0.7-15.1
tiff-debuginfo-4.0.7-15.1

i586
libtiff5-4.0.7-15.1
tiff-debugsource-4.0.7-15.1
libtiff5-debuginfo-4.0.7-15.1
tiff-4.0.7-15.1
libtiff-devel-4.0.7-15.1
tiff-debuginfo-4.0.7-15.1

SuSE Linux 42.2

x86_64
libtiff5-debuginfo-32bit-4.0.7-15.1
libtiff5-32bit-4.0.7-15.1
libtiff5-4.0.7-15.1
tiff-debugsource-4.0.7-15.1
libtiff-devel-32bit-4.0.7-15.1
libtiff5-debuginfo-4.0.7-15.1
tiff-4.0.7-15.1
libtiff-devel-4.0.7-15.1
tiff-debuginfo-4.0.7-15.1

i586
libtiff5-4.0.7-15.1
tiff-debugsource-4.0.7-15.1
libtiff5-debuginfo-4.0.7-15.1
tiff-4.0.7-15.1
libtiff-devel-4.0.7-15.1
tiff-debuginfo-4.0.7-15.1

145524 - SuSE Linux 42.2 openSUSE-SU-2017:1810-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7375, CVE-2017-7376

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1810-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00040.html>

SuSE Linux 42.2

i586
python-libxml2-debugsource-2.9.4-5.10.1

libxml2-tools-2.9.4-5.10.1
libxml2-debugsource-2.9.4-5.10.1
python-libxml2-debuginfo-2.9.4-5.10.1
libxml2-tools-debuginfo-2.9.4-5.10.1
python-libxml2-2.9.4-5.10.1
libxml2-2-debuginfo-2.9.4-5.10.1
libxml2-2-2.9.4-5.10.1
libxml2-devel-2.9.4-5.10.1

noarch
libxml2-doc-2.9.4-5.10.1

x86_64
python-libxml2-debugsource-2.9.4-5.10.1
libxml2-tools-2.9.4-5.10.1
libxml2-debugsource-2.9.4-5.10.1
python-libxml2-debuginfo-2.9.4-5.10.1
libxml2-tools-debuginfo-2.9.4-5.10.1
libxml2-2-debuginfo-32bit-2.9.4-5.10.1
python-libxml2-2.9.4-5.10.1
libxml2-2-debuginfo-2.9.4-5.10.1
libxml2-2-2.9.4-5.10.1
libxml2-devel-2.9.4-5.10.1
libxml2-2-32bit-2.9.4-5.10.1
libxml2-devel-32bit-2.9.4-5.10.1

145525 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2186-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8871, CVE-2016-7163

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2186-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00079.html>

SuSE Linux 42.2

x86_64
libopenjp2-7-debuginfo-32bit-2.1.0-13.3.1
openjpeg2-debugsource-2.1.0-13.3.1
libopenjp2-7-32bit-2.1.0-13.3.1
openjpeg2-devel-2.1.0-13.3.1
libopenjp2-7-debuginfo-2.1.0-13.3.1
openjpeg2-2.1.0-13.3.1
libopenjp2-7-2.1.0-13.3.1
openjpeg2-debuginfo-2.1.0-13.3.1

i586

openjpeg2-debugsource-2.1.0-13.3.1
openjpeg2-devel-2.1.0-13.3.1
libopenjp2-7-debuginfo-2.1.0-13.3.1
openjpeg2-2.1.0-13.3.1

libopenjp2-7-2.1.0-13.3.1
openjpeg2-debuginfo-2.1.0-13.3.1

SuSE Linux 42.3

x86_64
openjpeg2-2.1.0-16.1
openjpeg2-debuginfo-2.1.0-16.1
libopenjp2-7-debuginfo-32bit-2.1.0-16.1
openjpeg2-devel-2.1.0-16.1
libopenjp2-7-2.1.0-16.1
libopenjp2-7-debuginfo-2.1.0-16.1
libopenjp2-7-32bit-2.1.0-16.1
openjpeg2-debugsource-2.1.0-16.1

i586

openjpeg2-2.1.0-16.1
openjpeg2-debuginfo-2.1.0-16.1
openjpeg2-devel-2.1.0-16.1
libopenjp2-7-2.1.0-16.1
libopenjp2-7-debuginfo-2.1.0-16.1
openjpeg2-debugsource-2.1.0-16.1

145526 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0620-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3135

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0620-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00012.html>

SuSE Linux 42.1

i586
bind-9.9.9P1-48.1
bind-chrootenv-9.9.9P1-48.1
bind-lwresd-9.9.9P1-48.1
bind-devel-9.9.9P1-48.1
bind-debugsource-9.9.9P1-48.1
bind-lwresd-debuginfo-9.9.9P1-48.1
bind-utils-9.9.9P1-48.1
bind-libs-9.9.9P1-48.1
bind-debuginfo-9.9.9P1-48.1
bind-utils-debuginfo-9.9.9P1-48.1
bind-libs-debuginfo-9.9.9P1-48.1

noarch

bind-doc-9.9.9P1-48.1

x86_64

bind-lwresd-9.9.9P1-48.1
bind-utils-9.9.9P1-48.1

bind-utils-debuginfo-9.9.9P1-48.1
bind-libs-debuginfo-32bit-9.9.9P1-48.1
bind-libs-9.9.9P1-48.1
bind-lwresd-debuginfo-9.9.9P1-48.1
bind-debugsource-9.9.9P1-48.1
bind-devel-9.9.9P1-48.1
bind-9.9.9P1-48.1
bind-libs-32bit-9.9.9P1-48.1
bind-debuginfo-9.9.9P1-48.1
bind-libs-debuginfo-9.9.9P1-48.1
bind-chrootenv-9.9.9P1-48.1

SuSE Linux 42.2

i586

bind-utils-debuginfo-9.9.9P1-46.1
bind-utils-9.9.9P1-46.1
bind-debugsource-9.9.9P1-46.1
bind-lwresd-debuginfo-9.9.9P1-46.1
bind-lwresd-9.9.9P1-46.1
bind-chrootenv-9.9.9P1-46.1
bind-libs-9.9.9P1-46.1
bind-debuginfo-9.9.9P1-46.1
bind-devel-9.9.9P1-46.1
bind-libs-debuginfo-9.9.9P1-46.1
bind-9.9.9P1-46.1

noarch

bind-doc-9.9.9P1-46.1

x86_64

bind-9.9.9P1-46.1
bind-libs-32bit-9.9.9P1-46.1
bind-utils-debuginfo-9.9.9P1-46.1
bind-debugsource-9.9.9P1-46.1
bind-devel-9.9.9P1-46.1
bind-chrootenv-9.9.9P1-46.1
bind-lwresd-9.9.9P1-46.1
bind-libs-debuginfo-9.9.9P1-46.1
bind-libs-debuginfo-32bit-9.9.9P1-46.1
bind-utils-9.9.9P1-46.1
bind-debuginfo-9.9.9P1-46.1
bind-libs-9.9.9P1-46.1
bind-lwresd-debuginfo-9.9.9P1-46.1

145534 - SuSE Linux 42.3 openSUSE-SU-2017:2272-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9263, CVE-2017-9265

Description

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

openSUSE-SU-2017:2272-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00103.html>

SuSE Linux 42.3

x86_64

openvswitch-ovn-central-2.7.0-4.1

openvswitch-ovn-vtep-2.7.0-4.1

openvswitch-2.7.0-4.1

openvswitch-test-debuginfo-2.7.0-4.1

openvswitch-ovn-docker-2.7.0-4.1

openvswitch-pki-2.7.0-4.1

openvswitch-ovn-common-debuginfo-2.7.0-4.1

openvswitch-devel-2.7.0-4.1

openvswitch-ovn-central-debuginfo-2.7.0-4.1

openvswitch-vtep-2.7.0-4.1

openvswitch-test-2.7.0-4.1

openvswitch-ovn-vtep-debuginfo-2.7.0-4.1

openvswitch-debuginfo-2.7.0-4.1

openvswitch-ovn-host-debuginfo-2.7.0-4.1

python-openvswitch-2.7.0-4.1

openvswitch-debugsource-2.7.0-4.1

python-openvswitch-test-2.7.0-4.1

openvswitch-ovn-host-2.7.0-4.1

openvswitch-ovn-common-2.7.0-4.1

openvswitch-vtep-debuginfo-2.7.0-4.1

145537 - SuSE Linux 42.2 openSUSE-SU-2017:0045-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:0045-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00018.html>

SuSE Linux 42.2

x86_64

syncthing-0.14.16-5.1

noarch

syncthing-gtk-0.9.2.3-3.1

syncthing-gtk-lang-0.9.2.3-3.1

145538 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1209-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5483, CVE-2017-3302, CVE-2017-3305, CVE-2017-3308, CVE-2017-3309, CVE-2017-3329, CVE-2017-3450, CVE-2017-3452, CVE-2017-3453, CVE-2017-3456, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3599, CVE-2017-3600

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1209-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00024.html>

SuSE Linux 42.1

x86_64

libmysql56client18-debuginfo-5.6.36-25.3
mysql-community-server-errormessages-5.6.36-25.3
mysql-community-server-test-debuginfo-5.6.36-25.3
mysql-community-server-tools-5.6.36-25.3
mysql-community-server-test-5.6.36-25.3
mysql-community-server-bench-debuginfo-5.6.36-25.3
libmysql56client_r18-32bit-5.6.36-25.3
mysql-community-server-tools-debuginfo-5.6.36-25.3
libmysql56client18-32bit-5.6.36-25.3
mysql-community-server-client-debuginfo-5.6.36-25.3
mysql-community-server-debuginfo-5.6.36-25.3
libmysql56client18-debuginfo-5.6.36-25.3
libmysql56client18-5.6.36-25.3
mysql-community-server-bench-5.6.36-25.3
libmysql56client_r18-5.6.36-25.3
mysql-community-server-5.6.36-25.3
mysql-community-server-client-5.6.36-25.3
mysql-community-server-debugsource-5.6.36-25.3

i586

mysql-community-server-errormessages-5.6.36-25.3
mysql-community-server-test-debuginfo-5.6.36-25.3
mysql-community-server-tools-5.6.36-25.3
mysql-community-server-test-5.6.36-25.3
mysql-community-server-bench-debuginfo-5.6.36-25.3
mysql-community-server-tools-debuginfo-5.6.36-25.3
mysql-community-server-client-debuginfo-5.6.36-25.3
mysql-community-server-debuginfo-5.6.36-25.3
libmysql56client18-debuginfo-5.6.36-25.3
libmysql56client18-5.6.36-25.3
mysql-community-server-bench-5.6.36-25.3
libmysql56client_r18-5.6.36-25.3
mysql-community-server-5.6.36-25.3
mysql-community-server-client-5.6.36-25.3
mysql-community-server-debugsource-5.6.36-25.3

SuSE Linux 42.2

x86_64

mysql-community-server-client-debuginfo-5.6.36-24.3.3
mysql-community-server-bench-debuginfo-5.6.36-24.3.3
libmysql56client18-5.6.36-24.3.3
libmysql56client_r18-32bit-5.6.36-24.3.3
libmysql56client_r18-5.6.36-24.3.3
mysql-community-server-errormessages-5.6.36-24.3.3
mysql-community-server-debugsource-5.6.36-24.3.3
mysql-community-server-test-debuginfo-5.6.36-24.3.3
mysql-community-server-tools-5.6.36-24.3.3

mysql-community-server-debuginfo-5.6.36-24.3.3
mysql-community-server-bench-5.6.36-24.3.3
libmysql56client18-debuginfo-5.6.36-24.3.3
mysql-community-server-client-5.6.36-24.3.3
libmysql56client18-32bit-5.6.36-24.3.3
mysql-community-server-test-5.6.36-24.3.3
mysql-community-server-tools-debuginfo-5.6.36-24.3.3
mysql-community-server-5.6.36-24.3.3
libmysql56client18-debuginfo-32bit-5.6.36-24.3.3

i586

mysql-community-server-client-debuginfo-5.6.36-24.3.3
mysql-community-server-bench-debuginfo-5.6.36-24.3.3
libmysql56client18-5.6.36-24.3.3
libmysql56client_r18-5.6.36-24.3.3
mysql-community-server-errormessages-5.6.36-24.3.3
mysql-community-server-debugsource-5.6.36-24.3.3
mysql-community-server-test-debuginfo-5.6.36-24.3.3
mysql-community-server-tools-5.6.36-24.3.3
mysql-community-server-debuginfo-5.6.36-24.3.3
mysql-community-server-bench-5.6.36-24.3.3
libmysql56client18-debuginfo-5.6.36-24.3.3
mysql-community-server-client-5.6.36-24.3.3
mysql-community-server-test-5.6.36-24.3.3
mysql-community-server-tools-debuginfo-5.6.36-24.3.3
mysql-community-server-5.6.36-24.3.3

145540 - SuSE Linux 42.2 openSUSE-SU-2017:1343-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8849

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1343-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00064.html>

SuSE Linux 42.2

i586

smb4k-doc-1.2.1-3.3.1
smb4k-debuginfo-1.2.1-3.3.1
smb4k-debugsource-1.2.1-3.3.1
smb4k-1.2.1-3.3.1

noarch

smb4k-lang-1.2.1-3.3.1

x86_64

smb4k-doc-1.2.1-3.3.1
smb4k-debuginfo-1.2.1-3.3.1
smb4k-debugsource-1.2.1-3.3.1
smb4k-1.2.1-3.3.1

145544 - SuSE Linux 42.3 openSUSE-SU-2017:2188-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2188-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00065.html>

SuSE Linux 42.3

x86_64

fossil-debugsource-2.3-3.1

fossil-2.3-3.1

fossil-debuginfo-2.3-3.1

i586

fossil-debugsource-2.3-3.1

fossil-2.3-3.1

fossil-debuginfo-2.3-3.1

145545 - SuSE Linux 42.2 openSUSE-SU-2017:1806-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9122, CVE-2017-9123, CVE-2017-9124, CVE-2017-9125, CVE-2017-9126, CVE-2017-9127, CVE-2017-9128

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1806-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00035.html>

SuSE Linux 42.2

x86_64

libquicktime0-1.2.4cvs20150223-8.3.1

libquicktime-devel-1.2.4cvs20150223-8.3.1

libquicktime0-32bit-1.2.4cvs20150223-8.3.1

libquicktime0-debuginfo-32bit-1.2.4cvs20150223-8.3.1

libquicktime-debugsource-1.2.4cvs20150223-8.3.1

libquicktime0-debuginfo-1.2.4cvs20150223-8.3.1

libquicktime-tools-debuginfo-1.2.4cvs20150223-8.3.1

libquicktime-tools-1.2.4cvs20150223-8.3.1

i586

libquicktime0-1.2.4cvs20150223-8.3.1
libquicktime-devel-1.2.4cvs20150223-8.3.1
libquicktime-debugsource-1.2.4cvs20150223-8.3.1
libquicktime0-debuginfo-1.2.4cvs20150223-8.3.1
libquicktime-tools-debuginfo-1.2.4cvs20150223-8.3.1
libquicktime-tools-1.2.4cvs20150223-8.3.1

145546 - SuSE Linux 42.1 openSUSE-SU-2017:0708-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8637

Description

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

openSUSE-SU-2017:0708-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00047.html>

SuSE Linux 42.1

x86_64

dracut-debugsource-037-80.1

dracut-debuginfo-037-80.1

dracut-037-80.1

dracut-fips-037-80.1

i586

dracut-debugsource-037-80.1

dracut-debuginfo-037-80.1

dracut-037-80.1

dracut-fips-037-80.1

145547 - SuSE Linux 42.3 openSUSE-SU-2017:2270-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10983, CVE-2017-10984, CVE-2017-10985, CVE-2017-10986, CVE-2017-10987, CVE-2017-10988

Description

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

openSUSE-SU-2017:2270-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00100.html>

SuSE Linux 42.3

x86_64

freeradius-server-mysql-3.0.15-3.1

freeradius-server-utils-3.0.15-3.1
freeradius-server-postgresql-3.0.15-3.1
freeradius-server-sqlite-3.0.15-3.1
freeradius-server-devel-3.0.15-3.1
freeradius-server-ldap-3.0.15-3.1
freeradius-server-utils-debuginfo-3.0.15-3.1
freeradius-server-libs-debuginfo-3.0.15-3.1
freeradius-server-debugsource-3.0.15-3.1
freeradius-server-python-debuginfo-3.0.15-3.1
freeradius-server-ldap-debuginfo-3.0.15-3.1
freeradius-server-sqlite-debuginfo-3.0.15-3.1
freeradius-server-perl-3.0.15-3.1
freeradius-server-libs-3.0.15-3.1
freeradius-server-krb5-3.0.15-3.1
freeradius-server-mysql-debuginfo-3.0.15-3.1
freeradius-server-perl-debuginfo-3.0.15-3.1
freeradius-server-debuginfo-3.0.15-3.1
freeradius-server-python-3.0.15-3.1
freeradius-server-krb5-debuginfo-3.0.15-3.1
freeradius-server-postgresql-debuginfo-3.0.15-3.1
freeradius-server-3.0.15-3.1
freeradius-server-doc-3.0.15-3.1

145550 - SuSE Linux 42.2 openSUSE-SU-2017:2111-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7435, CVE-2017-7436, CVE-2017-9269

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2111-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00022.html>

SuSE Linux 42.2

i586

libzypp-16.15.2-5.9.1
libzypp-devel-doc-16.15.2-5.9.1
libzypp-devel-16.15.2-5.9.1
zypper-1.13.30-5.9.1
zypper-debuginfo-1.13.30-5.9.1
libzypp-debugsource-16.15.2-5.9.1
zypper-debugsource-1.13.30-5.9.1
libzypp-debuginfo-16.15.2-5.9.1

noarch

zypper-aptitude-1.13.30-5.9.1
zypper-log-1.13.30-5.9.1

x86_64

libzypp-16.15.2-5.9.1
libzypp-devel-doc-16.15.2-5.9.1
libzypp-devel-16.15.2-5.9.1

zypper-1.13.30-5.9.1
zypper-debuginfo-1.13.30-5.9.1
libzypp-debugsource-16.15.2-5.9.1
zypper-debugsource-1.13.30-5.9.1
libzypp-debuginfo-16.15.2-5.9.1

145551 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2151-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7782, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7798, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7804, CVE-2017-7807

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2151-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00043.html>

SuSE Linux 42.2

x86_64
MozillaFirefox-translations-common-52.3.0-57.15.1
MozillaFirefox-debugsource-52.3.0-57.15.1
MozillaFirefox-translations-other-52.3.0-57.15.1
MozillaFirefox-debuginfo-52.3.0-57.15.1
MozillaFirefox-branding-upstream-52.3.0-57.15.1
MozillaFirefox-buildsymbols-52.3.0-57.15.1
MozillaFirefox-52.3.0-57.15.1
MozillaFirefox-devel-52.3.0-57.15.1

SuSE Linux 42.3

x86_64
MozillaFirefox-translations-common-52.3.0-60.1
MozillaFirefox-branding-upstream-52.3.0-60.1
MozillaFirefox-52.3.0-60.1
MozillaFirefox-devel-52.3.0-60.1
MozillaFirefox-translations-other-52.3.0-60.1
MozillaFirefox-buildsymbols-52.3.0-60.1
MozillaFirefox-debuginfo-52.3.0-60.1
MozillaFirefox-debugsource-52.3.0-60.1

145553 - SuSE Linux 42.1 openSUSE-SU-2017:0298-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808, CVE-2016-9810

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0298-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00150.html>

SuSE Linux 42.1

i586

gststreamer-0_10-plugin-esd-debuginfo-0.10.31-16.1
gststreamer-0_10-plugins-good-extra-0.10.31-16.1
gststreamer-0_10-plugins-good-0.10.31-16.1
gststreamer-0_10-plugins-good-debugsource-0.10.31-16.1
gststreamer-0_10-plugin-esd-0.10.31-16.1
gststreamer-0_10-plugins-good-debuginfo-0.10.31-16.1
gststreamer-0_10-plugins-good-doc-0.10.31-16.1
gststreamer-0_10-plugins-good-extra-debuginfo-0.10.31-16.1

noarch

gststreamer-0_10-plugins-good-lang-0.10.31-16.1

x86_64

gststreamer-0_10-plugins-good-extra-debuginfo-0.10.31-16.1
gststreamer-0_10-plugins-good-doc-0.10.31-16.1
gststreamer-0_10-plugin-esd-32bit-0.10.31-16.1
gststreamer-0_10-plugins-good-extra-0.10.31-16.1
gststreamer-0_10-plugins-good-debugsource-0.10.31-16.1
gststreamer-0_10-plugin-esd-debuginfo-32bit-0.10.31-16.1
gststreamer-0_10-plugin-esd-debuginfo-0.10.31-16.1
gststreamer-0_10-plugins-good-extra-32bit-0.10.31-16.1
gststreamer-0_10-plugins-good-debuginfo-0.10.31-16.1
gststreamer-0_10-plugins-good-32bit-0.10.31-16.1
gststreamer-0_10-plugins-good-0.10.31-16.1
gststreamer-0_10-plugins-good-debuginfo-32bit-0.10.31-16.1
gststreamer-0_10-plugin-esd-0.10.31-16.1
gststreamer-0_10-plugins-good-extra-debuginfo-32bit-0.10.31-16.1

145554 - SuSE Linux 42.2 openSUSE-SU-2017:2110-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10810, CVE-2017-11473, CVE-2017-7533, CVE-2017-7541, CVE-2017-7542

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2110-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00020.html>

SuSE Linux 42.2

x86_64

kernel-debug-devel-4.4.79-18.23.1
kernel-default-4.4.79-18.23.1
kernel-debug-debuginfo-4.4.79-18.23.1
kernel-debug-devel-debuginfo-4.4.79-18.23.1

kernel-default-debugsource-4.4.79-18.23.1
kernel-debug-base-debuginfo-4.4.79-18.23.1
kernel-vanilla-base-debuginfo-4.4.79-18.23.1
kernel-debug-4.4.79-18.23.1
kernel-vanilla-4.4.79-18.23.1
kernel-debug-base-4.4.79-18.23.1
kernel-syms-4.4.79-18.23.1
kernel-default-debuginfo-4.4.79-18.23.1
kernel-obs-build-4.4.79-18.23.1
kernel-default-base-debuginfo-4.4.79-18.23.1
kernel-vanilla-base-4.4.79-18.23.1
kernel-obs-qa-4.4.79-18.23.1
kernel-obs-build-debugsource-4.4.79-18.23.1
kernel-vanilla-debugsource-4.4.79-18.23.1
kernel-vanilla-devel-4.4.79-18.23.1
kernel-debug-debugsource-4.4.79-18.23.1
kernel-default-devel-4.4.79-18.23.1
kernel-default-base-4.4.79-18.23.1
kernel-vanilla-debuginfo-4.4.79-18.23.1

noarch

kernel-docs-html-4.4.79-18.23.2
kernel-devel-4.4.79-18.23.1
kernel-docs-pdf-4.4.79-18.23.2
kernel-macros-4.4.79-18.23.1
kernel-source-vanilla-4.4.79-18.23.1
kernel-source-4.4.79-18.23.1
kernel-docs-4.4.79-18.23.2

145555 - SuSE Linux 42.2 openSUSE-SU-2017:1381-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8779

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1381-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00078.html>

SuSE Linux 42.2

x86_64

libtirpc3-1.0.1-2.3.1
libtirpc3-debuginfo-1.0.1-2.3.1
libtirpc-devel-1.0.1-2.3.1
libtirpc-debugsource-1.0.1-2.3.1
libtirpc3-32bit-1.0.1-2.3.1
libtirpc3-debuginfo-32bit-1.0.1-2.3.1
libtirpc-netconfig-1.0.1-2.3.1

i586

libtirpc3-debuginfo-1.0.1-2.3.1
libtirpc-netconfig-1.0.1-2.3.1

libtirpc-devel-1.0.1-2.3.1
libtirpc3-1.0.1-2.3.1
libtirpc-debugsource-1.0.1-2.3.1

145559 - SuSE Linux 42.2 openSUSE-SU-2017:1087-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7700, CVE-2017-7701, CVE-2017-7702, CVE-2017-7703, CVE-2017-7704, CVE-2017-7705, CVE-2017-7745, CVE-2017-7746, CVE-2017-7747, CVE-2017-7748

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1087-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00088.html>

SuSE Linux 42.2
x86_64
wireshark-2.2.6-14.3.1
wireshark-devel-2.2.6-14.3.1
wireshark-debuginfo-2.2.6-14.3.1
wireshark-ui-qt-debuginfo-2.2.6-14.3.1
wireshark-ui-qt-2.2.6-14.3.1
wireshark-ui-gtk-2.2.6-14.3.1
wireshark-ui-gtk-debuginfo-2.2.6-14.3.1
wireshark-debugsource-2.2.6-14.3.1

145564 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2153-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2885

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2153-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00045.html>

SuSE Linux 42.2
i586
libsoup-2_4-1-debuginfo-2.54.1-2.3.1
libsoup-debugsource-2.54.1-2.3.1
typelib-1_0-Soup-2_4-2.54.1-2.3.1
libsoup-devel-2.54.1-2.3.1
libsoup-2_4-1-2.54.1-2.3.1

noarch
libsoup-lang-2.54.1-2.3.1

x86_64
libsoup-devel-2.54.1-2.3.1
typelib-1_0-Soup-2_4-2.54.1-2.3.1
libsoup-2_4-1-debuginfo-2.54.1-2.3.1
libsoup-devel-32bit-2.54.1-2.3.1
libsoup-debugsource-2.54.1-2.3.1
libsoup-2_4-1-2.54.1-2.3.1
libsoup-2_4-1-debuginfo-32bit-2.54.1-2.3.1
libsoup-2_4-1-32bit-2.54.1-2.3.1

SuSE Linux 42.3
i586
libsoup-2_4-1-2.54.1-5.1
libsoup-2_4-1-debuginfo-2.54.1-5.1
libsoup-debugsource-2.54.1-5.1
libsoup-devel-2.54.1-5.1
typelib-1_0-Soup-2_4-2.54.1-5.1

noarch
libsoup-lang-2.54.1-5.1

x86_64
libsoup-2_4-1-2.54.1-5.1
libsoup-debugsource-2.54.1-5.1
libsoup-devel-2.54.1-5.1
libsoup-2_4-1-debuginfo-32bit-2.54.1-5.1
libsoup-2_4-1-debuginfo-2.54.1-5.1
libsoup-2_4-1-32bit-2.54.1-5.1
typelib-1_0-Soup-2_4-2.54.1-5.1
libsoup-devel-32bit-2.54.1-5.1

145566 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2356-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2356-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-September/003188.html>

SuSE SLES 12 SP2
noarch
postgresql96-docs-9.6.4-3.6.1

x86_64
libpq5-32bit-9.6.4-3.6.1
postgresql96-server-9.6.4-3.6.1
postgresql96-contrib-9.6.4-3.6.1

libpq5-debuginfo-9.6.4-3.6.1
postgresql96-contrib-debuginfo-9.6.4-3.6.1
libpq5-9.6.4-3.6.1
libecpg6-debuginfo-9.6.4-3.6.1
postgresql96-server-debuginfo-9.6.4-3.6.1
libpq5-debuginfo-32bit-9.6.4-3.6.1
postgresql96-9.6.4-3.6.1
libecpg6-9.6.4-3.6.1
postgresql96-debugsource-9.6.4-3.6.1
postgresql96-libs-debugsource-9.6.4-3.6.1
postgresql96-debuginfo-9.6.4-3.6.1

SuSE SLED 12 SP3

x86_64
libecpg6-debuginfo-9.6.4-3.6.1
libpq5-9.6.4-3.6.1
postgresql96-libs-debugsource-9.6.4-3.6.1
postgresql96-debuginfo-9.6.4-3.6.1
libpq5-debuginfo-9.6.4-3.6.1
libecpg6-9.6.4-3.6.1
libpq5-32bit-9.6.4-3.6.1
libpq5-debuginfo-32bit-9.6.4-3.6.1
postgresql96-9.6.4-3.6.1
postgresql96-debugsource-9.6.4-3.6.1

SuSE SLED 12 SP2

x86_64
libecpg6-debuginfo-9.6.4-3.6.1
libpq5-9.6.4-3.6.1
postgresql96-libs-debugsource-9.6.4-3.6.1
postgresql96-debuginfo-9.6.4-3.6.1
libpq5-debuginfo-9.6.4-3.6.1
libecpg6-9.6.4-3.6.1
libpq5-32bit-9.6.4-3.6.1
libpq5-debuginfo-32bit-9.6.4-3.6.1
postgresql96-9.6.4-3.6.1
postgresql96-debugsource-9.6.4-3.6.1

SuSE SLES 12 SP3

noarch
postgresql96-docs-9.6.4-3.6.1

x86_64
libpq5-32bit-9.6.4-3.6.1
postgresql96-server-9.6.4-3.6.1
postgresql96-contrib-9.6.4-3.6.1
libpq5-debuginfo-9.6.4-3.6.1
postgresql96-contrib-debuginfo-9.6.4-3.6.1
libpq5-9.6.4-3.6.1
libecpg6-debuginfo-9.6.4-3.6.1
postgresql96-server-debuginfo-9.6.4-3.6.1
libpq5-debuginfo-32bit-9.6.4-3.6.1
postgresql96-9.6.4-3.6.1
libecpg6-9.6.4-3.6.1
postgresql96-debugsource-9.6.4-3.6.1
postgresql96-libs-debugsource-9.6.4-3.6.1
postgresql96-debuginfo-9.6.4-3.6.1

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

Risk Level: High

CVE: CVE-2014-4975, CVE-2015-1855, CVE-2015-3900, CVE-2015-7551, CVE-2016-2339

Description

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

openSUSE-SU-2017:1128-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00112.html>

SuSE Linux 42.1

i586

libruby2_1-2_1-debuginfo-2.1.9-10.2

ruby2.1-devel-extra-2.1.9-10.2

ruby2.1-debugsource-2.1.9-10.2

ruby2.1-devel-2.1.9-10.2

ruby2.1-doc-2.1.9-10.2

ruby2.1-stdlib-2.1.9-10.2

ruby2.1-2.1.9-10.2

ruby2.1-debuginfo-2.1.9-10.2

ruby2.1-stdlib-debuginfo-2.1.9-10.2

libruby2_1-2_1-2.1.9-10.2

noarch

ruby2.1-doc-ri-2.1.9-10.2

x86_64

libruby2_1-2_1-debuginfo-2.1.9-10.2

ruby2.1-devel-extra-2.1.9-10.2

ruby2.1-debugsource-2.1.9-10.2

ruby2.1-devel-2.1.9-10.2

ruby2.1-doc-2.1.9-10.2

ruby2.1-stdlib-2.1.9-10.2

ruby2.1-2.1.9-10.2

ruby2.1-debuginfo-2.1.9-10.2

ruby2.1-stdlib-debuginfo-2.1.9-10.2

libruby2_1-2_1-2.1.9-10.2

SuSE Linux 42.2

i586

libruby2_1-2_1-2.1.9-8.3.2

ruby2.1-devel-2.1.9-8.3.2

ruby2.1-doc-2.1.9-8.3.2

ruby2.1-debuginfo-2.1.9-8.3.2

ruby2.1-stdlib-2.1.9-8.3.2

ruby2.1-stdlib-debuginfo-2.1.9-8.3.2

ruby2.1-2.1.9-8.3.2

libruby2_1-2_1-debuginfo-2.1.9-8.3.2

ruby2.1-debugsource-2.1.9-8.3.2

ruby2.1-devel-extra-2.1.9-8.3.2

noarch

ruby2.1-doc-ri-2.1.9-8.3.2

x86_64

libruby2_1-2_1-2.1.9-8.3.2
ruby2.1-devel-2.1.9-8.3.2
ruby2.1-doc-2.1.9-8.3.2
ruby2.1-debuginfo-2.1.9-8.3.2
ruby2.1-stdlib-2.1.9-8.3.2
ruby2.1-stdlib-debuginfo-2.1.9-8.3.2
ruby2.1-2.1.9-8.3.2
libruby2_1-2_1-debuginfo-2.1.9-8.3.2
ruby2.1-debugsource-2.1.9-8.3.2
ruby2.1-devel-extra-2.1.9-8.3.2

145569 - SuSE Linux 42.2 openSUSE-SU-2017:1033-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8637

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1033-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00060.html>

SuSE Linux 42.2
x86_64
dracut-debugsource-044-16.3.1
dracut-fips-044-16.3.1
dracut-debuginfo-044-16.3.1
dracut-tools-044-16.3.1
dracut-044-16.3.1

i586
dracut-debugsource-044-16.3.1
dracut-fips-044-16.3.1
dracut-debuginfo-044-16.3.1
dracut-tools-044-16.3.1
dracut-044-16.3.1

145570 - SuSE Linux 42.2 openSUSE-SU-2017:0944-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0944-1

Observation

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

SuSE Linux 42.2

i586

libsmbconf-devel-4.4.2-11.3.1
libndr0-debuginfo-4.4.2-11.3.1
libtevent-util0-debuginfo-4.4.2-11.3.1
libdcerpc-devel-4.4.2-11.3.1
samba-client-4.4.2-11.3.1
libsamba-errors0-4.4.2-11.3.1
libtevent-util-devel-4.4.2-11.3.1
samba-core-devel-4.4.2-11.3.1
libsamba-credentials0-4.4.2-11.3.1
libnetapi-devel-4.4.2-11.3.1
libsmbclient-devel-4.4.2-11.3.1
libwbclient-devel-4.4.2-11.3.1
libsamba-policy0-4.4.2-11.3.1
samba-client-debuginfo-4.4.2-11.3.1
libdcerpc0-debuginfo-4.4.2-11.3.1
libsamdb-devel-4.4.2-11.3.1
libndr-standard-devel-4.4.2-11.3.1
libdcerpc-samr0-debuginfo-4.4.2-11.3.1
libsamba-passdb0-debuginfo-4.4.2-11.3.1
libndr-standard0-debuginfo-4.4.2-11.3.1
libdcerpc-binding0-4.4.2-11.3.1
libndr0-4.4.2-11.3.1
libsmbldap0-debuginfo-4.4.2-11.3.1
libsamba-errors-devel-4.4.2-11.3.1
libdcerpc-samr-devel-4.4.2-11.3.1
libwbclient0-4.4.2-11.3.1
libsamba-util-devel-4.4.2-11.3.1
libsamba-passdb0-4.4.2-11.3.1
samba-debugsource-4.4.2-11.3.1
libndr-krb5pac0-4.4.2-11.3.1
samba-python-debuginfo-4.4.2-11.3.1
libsamba-errors0-debuginfo-4.4.2-11.3.1
libndr-krb5pac-devel-4.4.2-11.3.1
ctdb-tests-4.4.2-11.3.1
libsamdb0-4.4.2-11.3.1
libsamba-policy-devel-4.4.2-11.3.1
samba-libs-debuginfo-4.4.2-11.3.1
libsamba-credentials-devel-4.4.2-11.3.1
libsamba-passdb-devel-4.4.2-11.3.1
libsmbclient0-debuginfo-4.4.2-11.3.1
samba-libs-4.4.2-11.3.1
libsmbconf0-4.4.2-11.3.1
libsamba-hostconfig0-4.4.2-11.3.1
libndr-krb5pac0-debuginfo-4.4.2-11.3.1
samba-debuginfo-4.4.2-11.3.1
libsamba-hostconfig-devel-4.4.2-11.3.1
libsmbldap0-4.4.2-11.3.1
samba-4.4.2-11.3.1
libdcerpc0-4.4.2-11.3.1
samba-pidl-4.4.2-11.3.1
ctdb-debuginfo-4.4.2-11.3.1
ctdb-4.4.2-11.3.1
samba-winbind-debuginfo-4.4.2-11.3.1
ctdb-tests-debuginfo-4.4.2-11.3.1
libdcerpc-samr0-4.4.2-11.3.1
libsmbclient0-4.4.2-11.3.1

libtevent-util0-4.4.2-11.3.1
samba-test-4.4.2-11.3.1
samba-python-4.4.2-11.3.1
samba-test-debuginfo-4.4.2-11.3.1
libndr-nbt0-4.4.2-11.3.1
libndr-nbt-devel-4.4.2-11.3.1
libsamba-hostconfig0-debuginfo-4.4.2-11.3.1
libwbclient0-debuginfo-4.4.2-11.3.1
libndr-nbt0-debuginfo-4.4.2-11.3.1
libsmbldap-devel-4.4.2-11.3.1
libsamba-policy0-debuginfo-4.4.2-11.3.1
libsamba-credentials0-debuginfo-4.4.2-11.3.1
libdcerpc-binding0-debuginfo-4.4.2-11.3.1
libnetapi0-debuginfo-4.4.2-11.3.1
libsmbconf0-debuginfo-4.4.2-11.3.1
samba-winbind-4.4.2-11.3.1
libsamdb0-debuginfo-4.4.2-11.3.1
libsamba-util0-debuginfo-4.4.2-11.3.1
libsamba-util0-4.4.2-11.3.1
libndr-standard0-4.4.2-11.3.1
libnetapi0-4.4.2-11.3.1
libndr-devel-4.4.2-11.3.1

noarch
samba-doc-4.4.2-11.3.1

x86_64
libndr-krb5pac0-debuginfo-32bit-4.4.2-11.3.1
libsamba-hostconfig0-32bit-4.4.2-11.3.1
libsmbconf-devel-4.4.2-11.3.1
libndr0-debuginfo-4.4.2-11.3.1
libtevent-util0-debuginfo-4.4.2-11.3.1
libdcerpc-devel-4.4.2-11.3.1
samba-client-4.4.2-11.3.1
libndr-nbt0-debuginfo-32bit-4.4.2-11.3.1
libndr-nbt0-32bit-4.4.2-11.3.1
samba-client-debuginfo-32bit-4.4.2-11.3.1
libsamba-errors0-4.4.2-11.3.1
libtevent-util-devel-4.4.2-11.3.1
libsamba-policy0-debuginfo-32bit-4.4.2-11.3.1
samba-core-devel-4.4.2-11.3.1
libsamba-credentials0-4.4.2-11.3.1
libnetapi-devel-4.4.2-11.3.1
libsmbclient-devel-4.4.2-11.3.1
libwbclient-devel-4.4.2-11.3.1
libsamba-errors0-debuginfo-32bit-4.4.2-11.3.1
libsmbclient0-debuginfo-32bit-4.4.2-11.3.1
libsamba-util0-32bit-4.4.2-11.3.1
libsamba-policy0-4.4.2-11.3.1
samba-client-debuginfo-4.4.2-11.3.1
libdcerpc0-debuginfo-4.4.2-11.3.1
libndr-krb5pac0-32bit-4.4.2-11.3.1
libsamdb-devel-4.4.2-11.3.1
libndr-standard-devel-4.4.2-11.3.1
libdcerpc-samr0-debuginfo-4.4.2-11.3.1
samba-winbind-debuginfo-32bit-4.4.2-11.3.1
libdcerpc-binding0-32bit-4.4.2-11.3.1
samba-client-32bit-4.4.2-11.3.1
libndr0-32bit-4.4.2-11.3.1
libsamba-passdb0-debuginfo-4.4.2-11.3.1

libdcerpc-samr0-debuginfo-32bit-4.4.2-11.3.1
libndr-standard0-debuginfo-4.4.2-11.3.1
libsamba-util0-debuginfo-32bit-4.4.2-11.3.1
libdcerpc-binding0-4.4.2-11.3.1
libndr0-4.4.2-11.3.1
libsmbldap0-debuginfo-4.4.2-11.3.1
libsamba-errors-devel-4.4.2-11.3.1
libdcerpc-samr-devel-4.4.2-11.3.1
libdcerpc0-debuginfo-32bit-4.4.2-11.3.1
libsamba-credentials0-32bit-4.4.2-11.3.1
libwbclient0-4.4.2-11.3.1
libsamba-util-devel-4.4.2-11.3.1
libsamba-passdb0-4.4.2-11.3.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-11.3.1
libsamba-errors0-32bit-4.4.2-11.3.1
samba-debugsource-4.4.2-11.3.1
libndr-krb5pac0-4.4.2-11.3.1
samba-python-debuginfo-4.4.2-11.3.1
libsamba-errors0-debuginfo-4.4.2-11.3.1
libndr-krb5pac-devel-4.4.2-11.3.1
ctdb-tests-4.4.2-11.3.1
libsamdb0-4.4.2-11.3.1
libsamba-policy-devel-4.4.2-11.3.1
libsamba-passdb0-32bit-4.4.2-11.3.1
samba-libs-debuginfo-4.4.2-11.3.1
libsamba-credentials-devel-4.4.2-11.3.1
libsamba-passdb-devel-4.4.2-11.3.1
libsmbclient0-debuginfo-4.4.2-11.3.1
libsamdb0-32bit-4.4.2-11.3.1
samba-libs-4.4.2-11.3.1
libsmbconf0-4.4.2-11.3.1
libsamba-hostconfig0-4.4.2-11.3.1
libndr0-debuginfo-32bit-4.4.2-11.3.1
libndr-standard0-32bit-4.4.2-11.3.1
libtevent-util0-32bit-4.4.2-11.3.1
libndr-krb5pac0-debuginfo-4.4.2-11.3.1
samba-debuginfo-4.4.2-11.3.1
samba-libs-debuginfo-32bit-4.4.2-11.3.1
libsamba-hostconfig-devel-4.4.2-11.3.1
libsmbldap0-4.4.2-11.3.1
libnetapi0-debuginfo-32bit-4.4.2-11.3.1
samba-4.4.2-11.3.1
libdcerpc-samr0-32bit-4.4.2-11.3.1
libdcerpc0-4.4.2-11.3.1
samba-pidl-4.4.2-11.3.1
libsamba-hostconfig0-debuginfo-32bit-4.4.2-11.3.1
ctdb-debuginfo-4.4.2-11.3.1
ctdb-4.4.2-11.3.1
libsamba-credentials0-debuginfo-32bit-4.4.2-11.3.1
samba-libs-32bit-4.4.2-11.3.1
libtevent-util0-debuginfo-32bit-4.4.2-11.3.1
samba-winbind-debuginfo-4.4.2-11.3.1
ctdb-tests-debuginfo-4.4.2-11.3.1
libdcerpc-samr0-4.4.2-11.3.1
libsmbclient0-4.4.2-11.3.1
libtevent-util0-4.4.2-11.3.1
samba-test-4.4.2-11.3.1
samba-python-4.4.2-11.3.1
libsamba-passdb0-debuginfo-32bit-4.4.2-11.3.1
samba-test-debuginfo-4.4.2-11.3.1

libndr-nbt0-4.4.2-11.3.1
libndr-nbt-devel-4.4.2-11.3.1
libsmbldap0-32bit-4.4.2-11.3.1
libwbclient0-32bit-4.4.2-11.3.1
libsamba-hostconfig0-debuginfo-4.4.2-11.3.1
libwbclient0-debuginfo-32bit-4.4.2-11.3.1
libwbclient0-debuginfo-4.4.2-11.3.1
libndr-nbt0-debuginfo-4.4.2-11.3.1
libdcerpc0-32bit-4.4.2-11.3.1
libsmbldap-devel-4.4.2-11.3.1
libsmbclient0-32bit-4.4.2-11.3.1
libsmbldap0-debuginfo-32bit-4.4.2-11.3.1
samba-winbind-32bit-4.4.2-11.3.1
libsamba-policy0-debuginfo-4.4.2-11.3.1
libsamba-credentials0-debuginfo-4.4.2-11.3.1
libdcerpc-binding0-debuginfo-4.4.2-11.3.1
libsamba-policy0-32bit-4.4.2-11.3.1
libnetapi0-debuginfo-4.4.2-11.3.1
libnetapi0-32bit-4.4.2-11.3.1
libndr-standard0-debuginfo-32bit-4.4.2-11.3.1
libsmbconf0-debuginfo-4.4.2-11.3.1
samba-winbind-4.4.2-11.3.1
libsamdb0-debuginfo-4.4.2-11.3.1
libsamdb0-debuginfo-32bit-4.4.2-11.3.1
libsmbconf0-debuginfo-32bit-4.4.2-11.3.1
libsamba-util0-debuginfo-4.4.2-11.3.1
libsamba-util0-4.4.2-11.3.1
libndr-standard0-4.4.2-11.3.1
libsmbconf0-32bit-4.4.2-11.3.1
libnetapi0-4.4.2-11.3.1
libndr-devel-4.4.2-11.3.1

145572 - SuSE Linux 42.3 openSUSE-SU-2017:2335-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7435, CVE-2017-7436, CVE-2017-9269

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2335-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00003.html>

SuSE Linux 42.3

i586

libzypp-devel-doc-16.15.3-9.1
yast2-pkg-bindings-debugsource-3.2.4-4.1
libzypp-debuginfo-16.15.3-9.1
yast2-pkg-bindings-3.2.4-4.1
libzypp-devel-16.15.3-9.1
libzypp-debugsource-16.15.3-9.1
libzypp-16.15.3-9.1
yast2-pkg-bindings-debuginfo-3.2.4-4.1

noarch
yast2-pkg-bindings-devel-doc-3.2.4-4.1

x86_64
libzypp-devel-doc-16.15.3-9.1
yast2-pkg-bindings-debugsource-3.2.4-4.1
libzypp-debuginfo-16.15.3-9.1
yast2-pkg-bindings-3.2.4-4.1
libzypp-devel-16.15.3-9.1
libzypp-debugsource-16.15.3-9.1
libzypp-16.15.3-9.1
yast2-pkg-bindings-debuginfo-3.2.4-4.1

145573 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2355-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Description

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

SUSE-SU-2017:2355-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-September/003187.html>

SuSE SLED 12 SP2

x86_64
postgresql94-debuginfo-9.4.13-21.5.1
postgresql94-9.4.13-21.5.1
postgresql94-debugsource-9.4.13-21.5.1

SuSE SLES 12 SP2

noarch
postgresql94-docs-9.4.13-21.5.1

x86_64
postgresql94-debuginfo-9.4.13-21.5.1
postgresql94-server-9.4.13-21.5.1
postgresql94-9.4.13-21.5.1
postgresql94-contrib-9.4.13-21.5.1
postgresql94-server-debuginfo-9.4.13-21.5.1
postgresql94-debugsource-9.4.13-21.5.1
postgresql94-contrib-debuginfo-9.4.13-21.5.1

145574 - SuSE Linux 42.2 openSUSE-SU-2017:0907-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10200, CVE-2016-2117, CVE-2016-9191, CVE-2017-2596, CVE-2017-2636, CVE-2017-6214, CVE-2017-6345, CVE-2017-6346, CVE-2017-6347, CVE-2017-6353, CVE-2017-7184

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0907-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00001.html>

SuSE Linux 42.2

x86_64

kernel-default-devel-4.4.57-18.3.1

kernel-debug-base-debuginfo-4.4.57-18.3.1

kernel-debug-devel-4.4.57-18.3.1

kernel-syms-4.4.57-18.3.1

kernel-default-debuginfo-4.4.57-18.3.1

kernel-vanilla-base-4.4.57-18.3.1

kernel-vanilla-debuginfo-4.4.57-18.3.1

kernel-obs-qa-4.4.57-18.3.1

kernel-debug-debugsource-4.4.57-18.3.1

kernel-default-base-debuginfo-4.4.57-18.3.1

kernel-default-debugsource-4.4.57-18.3.1

kernel-debug-debuginfo-4.4.57-18.3.1

kernel-vanilla-4.4.57-18.3.1

kernel-debug-4.4.57-18.3.1

kernel-obs-build-4.4.57-18.3.1

kernel-vanilla-devel-4.4.57-18.3.1

kernel-debug-devel-debuginfo-4.4.57-18.3.1

kernel-vanilla-base-debuginfo-4.4.57-18.3.1

kernel-vanilla-debugsource-4.4.57-18.3.1

kernel-obs-build-debugsource-4.4.57-18.3.1

kernel-default-base-4.4.57-18.3.1

kernel-debug-base-4.4.57-18.3.1

kernel-default-4.4.57-18.3.1

noarch

kernel-docs-html-4.4.57-18.3.2

kernel-docs-pdf-4.4.57-18.3.2

kernel-docs-4.4.57-18.3.2

kernel-source-vanilla-4.4.57-18.3.1

kernel-devel-4.4.57-18.3.1

kernel-macros-4.4.57-18.3.1

kernel-source-4.4.57-18.3.1

145575 - SuSE Linux 42.2 openSUSE-SU-2017:1809-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3142, CVE-2017-3143

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1809-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00038.html>

SuSE Linux 42.2

i586

bind-lwresd-9.9.9P1-48.6.1

bind-libs-9.9.9P1-48.6.1

bind-libs-debuginfo-9.9.9P1-48.6.1

bind-debuginfo-9.9.9P1-48.6.1

bind-lwresd-debuginfo-9.9.9P1-48.6.1

bind-utils-9.9.9P1-48.6.1

bind-debugsource-9.9.9P1-48.6.1

bind-devel-9.9.9P1-48.6.1

bind-utils-debuginfo-9.9.9P1-48.6.1

bind-9.9.9P1-48.6.1

bind-chrootenv-9.9.9P1-48.6.1

noarch

bind-doc-9.9.9P1-48.6.1

x86_64

bind-libs-debuginfo-32bit-9.9.9P1-48.6.1

bind-debugsource-9.9.9P1-48.6.1

bind-libs-9.9.9P1-48.6.1

bind-lwresd-9.9.9P1-48.6.1

bind-utils-9.9.9P1-48.6.1

bind-lwresd-debuginfo-9.9.9P1-48.6.1

bind-9.9.9P1-48.6.1

bind-libs-32bit-9.9.9P1-48.6.1

bind-chrootenv-9.9.9P1-48.6.1

bind-utils-debuginfo-9.9.9P1-48.6.1

bind-debuginfo-9.9.9P1-48.6.1

bind-libs-debuginfo-9.9.9P1-48.6.1

bind-devel-9.9.9P1-48.6.1

145576 - SuSE Linux 42.3 openSUSE-SU-2017:2155-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:2155-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00047.html>

SuSE Linux 42.3

x86_64

tcmu-runner-debuginfo-1.2.0-3.1

libtcmu-devel-1.2.0-3.1

tcmu-runner-devel-1.2.0-3.1

tcmu-runner-debugsource-1.2.0-3.1

libtcmu1-debuginfo-1.2.0-3.1

tcmu-runner-handler-rbd-debuginfo-1.2.0-3.1

tcmu-runner-handler-rbd-1.2.0-3.1
tcmu-runner-1.2.0-3.1
libtcmu1-1.2.0-3.1

i586

tcmu-runner-debuginfo-1.2.0-3.1
libtcmu-devel-1.2.0-3.1
tcmu-runner-devel-1.2.0-3.1
tcmu-runner-debugsource-1.2.0-3.1
libtcmu1-debuginfo-1.2.0-3.1
tcmu-runner-1.2.0-3.1
libtcmu1-1.2.0-3.1

145577 - SuSE Linux 42.3 openSUSE-SU-2017:2112-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11473, CVE-2017-7533, CVE-2017-7541, CVE-2017-7542

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2112-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00021.html>

SuSE Linux 42.3

x86_64

kernel-vanilla-debugsource-4.4.79-4.2
kernel-default-base-debuginfo-4.4.79-4.2
kernel-vanilla-debuginfo-4.4.79-4.2
kernel-debug-devel-debuginfo-4.4.79-4.2
kernel-default-debugsource-4.4.79-4.2
kernel-default-debuginfo-4.4.79-4.2
kernel-obs-build-4.4.79-4.2
kernel-vanilla-base-4.4.79-4.2
kernel-debug-debugsource-4.4.79-4.2
kernel-debug-4.4.79-4.2
kernel-debug-debuginfo-4.4.79-4.2
kernel-default-devel-4.4.79-4.2
kernel-syms-4.4.79-4.2
kernel-vanilla-4.4.79-4.2
kernel-debug-base-debuginfo-4.4.79-4.2
kernel-obs-build-debugsource-4.4.79-4.2
kernel-obs-qa-4.4.79-4.2
kernel-vanilla-devel-4.4.79-4.2
kernel-debug-devel-4.4.79-4.2
kernel-debug-base-4.4.79-4.2
kernel-vanilla-base-debuginfo-4.4.79-4.2
kernel-default-4.4.79-4.2
kernel-default-base-4.4.79-4.2

noarch

kernel-source-4.4.79-4.2
kernel-docs-pdf-4.4.79-4.2

kernel-docs-4.4.79-4.2
kernel-macros-4.4.79-4.2
kernel-docs-html-4.4.79-4.2
kernel-devel-4.4.79-4.2
kernel-source-vanilla-4.4.79-4.2

145578 - SuSE Linux 42.1 openSUSE-SU-2017:0906-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10200, CVE-2016-10208, CVE-2016-2117, CVE-2017-2583, CVE-2017-2584, CVE-2017-2596, CVE-2017-2636, CVE-2017-5669, CVE-2017-6214, CVE-2017-6345, CVE-2017-6346, CVE-2017-6347, CVE-2017-6348, CVE-2017-6353, CVE-2017-7184

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0906-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00000.html>

SuSE Linux 42.1

i586

kernel-default-base-debuginfo-4.1.39-53.1
kernel-default-4.1.39-53.1
kernel-obs-qa-4.1.39-53.1
kernel-default-debugsource-4.1.39-53.1
kernel-obs-build-debugsource-4.1.39-53.1
kernel-default-base-4.1.39-53.1
kernel-syms-4.1.39-53.1
kernel-default-devel-4.1.39-53.1
kernel-default-debuginfo-4.1.39-53.1
kernel-obs-build-4.1.39-53.1

i686

kernel-pae-base-debuginfo-4.1.39-53.1
kernel-xen-devel-4.1.39-53.1
kernel-ec2-debugsource-4.1.39-53.1
kernel-debug-base-debuginfo-4.1.39-53.1
kernel-ec2-debuginfo-4.1.39-53.1
kernel-pae-4.1.39-53.1
kernel-debug-4.1.39-53.1
kernel-pv-base-debuginfo-4.1.39-53.1
kernel-pv-base-4.1.39-53.1
kernel-vanilla-debuginfo-4.1.39-53.1
kernel-ec2-devel-4.1.39-53.1
kernel-debug-debugsource-4.1.39-53.1
kernel-pae-debuginfo-4.1.39-53.1
kernel-xen-4.1.39-53.1
kernel-debug-base-4.1.39-53.1
kernel-pv-4.1.39-53.1
kernel-ec2-base-debuginfo-4.1.39-53.1
kernel-vanilla-devel-4.1.39-53.1
kernel-xen-debugsource-4.1.39-53.1
kernel-pv-debuginfo-4.1.39-53.1

kernel-pv-devel-4.1.39-53.1
kernel-xen-debuginfo-4.1.39-53.1
kernel-debug-devel-4.1.39-53.1
kernel-xen-base-4.1.39-53.1
kernel-vanilla-debugsource-4.1.39-53.1
kernel-xen-base-debuginfo-4.1.39-53.1
kernel-pae-devel-4.1.39-53.1
kernel-ec2-base-4.1.39-53.1
kernel-pv-debugsource-4.1.39-53.1
kernel-pae-debugsource-4.1.39-53.1
kernel-ec2-4.1.39-53.1
kernel-pae-base-4.1.39-53.1
kernel-debug-devel-debuginfo-4.1.39-53.1
kernel-debug-debuginfo-4.1.39-53.1
kernel-vanilla-4.1.39-53.1

noarch

kernel-docs-pdf-4.1.39-53.2
kernel-docs-html-4.1.39-53.2
kernel-source-4.1.39-53.1
kernel-macros-4.1.39-53.1
kernel-devel-4.1.39-53.1
kernel-docs-4.1.39-53.2
kernel-source-vanilla-4.1.39-53.1

x86_64

kernel-default-base-4.1.39-53.1
kernel-xen-devel-4.1.39-53.1
kernel-ec2-debugsource-4.1.39-53.1
kernel-debug-base-debuginfo-4.1.39-53.1
kernel-ec2-debuginfo-4.1.39-53.1
kernel-xen-base-debuginfo-4.1.39-53.1
kernel-default-base-debuginfo-4.1.39-53.1
kernel-debug-4.1.39-53.1
kernel-pv-base-debuginfo-4.1.39-53.1
kernel-pv-base-4.1.39-53.1
kernel-xen-debuginfo-4.1.39-53.1
kernel-vanilla-debuginfo-4.1.39-53.1
kernel-ec2-devel-4.1.39-53.1
kernel-debug-debugsource-4.1.39-53.1
kernel-xen-4.1.39-53.1
kernel-debug-base-4.1.39-53.1
kernel-pv-4.1.39-53.1
kernel-ec2-base-debuginfo-4.1.39-53.1
kernel-vanilla-4.1.39-53.1
kernel-pv-debuginfo-4.1.39-53.1
kernel-xen-debugsource-4.1.39-53.1
kernel-default-debugsource-4.1.39-53.1
kernel-default-4.1.39-53.1
kernel-default-debuginfo-4.1.39-53.1
kernel-pv-devel-4.1.39-53.1
kernel-obs-qa-4.1.39-53.1
kernel-debug-devel-4.1.39-53.1
kernel-xen-base-4.1.39-53.1
kernel-vanilla-debugsource-4.1.39-53.1
kernel-default-devel-4.1.39-53.1
kernel-obs-build-4.1.39-53.1
kernel-ec2-base-4.1.39-53.1
kernel-syms-4.1.39-53.1
kernel-vanilla-devel-4.1.39-53.1

kernel-ec2-4.1.39-53.1
kernel-debug-devel-debuginfo-4.1.39-53.1
kernel-debug-debuginfo-4.1.39-53.1
kernel-obs-build-debugsource-4.1.39-53.1
kernel-pv-debugsource-4.1.39-53.1

145579 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2349-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2349-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00008.html>

SuSE Linux 42.2

x86_64
wireshark-devel-2.2.9-14.13.1
wireshark-ui-qt-debuginfo-2.2.9-14.13.1
wireshark-debuginfo-2.2.9-14.13.1
wireshark-ui-qt-2.2.9-14.13.1
wireshark-ui-gtk-2.2.9-14.13.1
wireshark-ui-gtk-debuginfo-2.2.9-14.13.1
wireshark-2.2.9-14.13.1
wireshark-debugsource-2.2.9-14.13.1

SuSE Linux 42.3

x86_64
wireshark-ui-qt-debuginfo-2.2.9-21.1
wireshark-ui-qt-2.2.9-21.1
wireshark-devel-2.2.9-21.1
wireshark-ui-gtk-2.2.9-21.1
wireshark-debuginfo-2.2.9-21.1
wireshark-ui-gtk-debuginfo-2.2.9-21.1
wireshark-2.2.9-21.1
wireshark-debugsource-2.2.9-21.1

145585 - SuSE Linux 42.1 openSUSE-SU-2017:0007-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10013, CVE-2016-10024, CVE-2016-7777, CVE-2016-7908, CVE-2016-7909, CVE-2016-7995, CVE-2016-8576, CVE-2016-8667, CVE-2016-8669, CVE-2016-8909, CVE-2016-8910, CVE-2016-9101, CVE-2016-9377, CVE-2016-9378, CVE-2016-9379, CVE-2016-9380, CVE-2016-9381, CVE-2016-9382, CVE-2016-9383, CVE-2016-9385, CVE-2016-9386, CVE-2016-9637, CVE-2016-9776, CVE-2016-9932

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0007-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00003.html>

SuSE Linux 42.1

x86_64

xen-libs-debuginfo-4.5.5_06-18.1

xen-debugsource-4.5.5_06-18.1

xen-doc-html-4.5.5_06-18.1

xen-tools-domU-debuginfo-4.5.5_06-18.1

xen-devel-4.5.5_06-18.1

xen-kmp-default-debuginfo-4.5.5_06_k4.1.36_41-18.1

xen-libs-32bit-4.5.5_06-18.1

xen-kmp-default-4.5.5_06_k4.1.36_41-18.1

xen-tools-domU-4.5.5_06-18.1

xen-libs-debuginfo-32bit-4.5.5_06-18.1

xen-tools-4.5.5_06-18.1

xen-libs-4.5.5_06-18.1

xen-4.5.5_06-18.1

xen-tools-debuginfo-4.5.5_06-18.1

i586

xen-tools-domU-debuginfo-4.5.5_06-18.1

xen-libs-debuginfo-4.5.5_06-18.1

xen-tools-domU-4.5.5_06-18.1

xen-libs-4.5.5_06-18.1

xen-debugsource-4.5.5_06-18.1

xen-devel-4.5.5_06-18.1

145588 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0447-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0447-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00056.html>

SuSE Linux 42.1

x86_64

irssi-debuginfo-1.0.1-12.1

irssi-1.0.1-12.1

irssi-debugsource-1.0.1-12.1

irssi-devel-1.0.1-12.1

i586

irssi-debuginfo-1.0.1-12.1

irssi-1.0.1-12.1

irssi-debugsource-1.0.1-12.1
irssi-devel-1.0.1-12.1

SuSE Linux 42.2
x86_64
irssi-debuginfo-1.0.1-12.1
irssi-1.0.1-12.1
irssi-debugsource-1.0.1-12.1
irssi-devel-1.0.1-12.1

i586
irssi-debuginfo-1.0.1-12.1
irssi-1.0.1-12.1
irssi-debugsource-1.0.1-12.1
irssi-devel-1.0.1-12.1

145590 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:1993-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5091, CVE-2017-5092, CVE-2017-5093, CVE-2017-5094, CVE-2017-5095, CVE-2017-5096, CVE-2017-5097, CVE-2017-5098, CVE-2017-5099, CVE-2017-5100, CVE-2017-5101, CVE-2017-5102, CVE-2017-5103, CVE-2017-5104, CVE-2017-5105, CVE-2017-5106, CVE-2017-5107, CVE-2017-5108, CVE-2017-5109, CVE-2017-5110, CVE-2017-7000

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1993-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00104.html>

SuSE Linux 42.2
x86_64
chromium-60.0.3112.78-104.21.1
chromium-debuginfo-60.0.3112.78-104.21.1
chromedriver-60.0.3112.78-104.21.1
chromium-debugsource-60.0.3112.78-104.21.1
chromedriver-debuginfo-60.0.3112.78-104.21.1

SuSE Linux 42.3
x86_64
chromium-60.0.3112.78-107.1
chromedriver-60.0.3112.78-107.1
chromium-debugsource-60.0.3112.78-107.1
chromedriver-debuginfo-60.0.3112.78-107.1
chromium-debuginfo-60.0.3112.78-107.1

145592 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0737-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0737-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00051.html>

SuSE Linux 42.1
x86_64
irssi-devel-1.0.2-15.1
irssi-debugsource-1.0.2-15.1
irssi-1.0.2-15.1
irssi-debuginfo-1.0.2-15.1

i586
irssi-devel-1.0.2-15.1
irssi-debugsource-1.0.2-15.1
irssi-1.0.2-15.1
irssi-debuginfo-1.0.2-15.1

SuSE Linux 42.2
x86_64
irssi-devel-1.0.2-15.1
irssi-debugsource-1.0.2-15.1
irssi-1.0.2-15.1
irssi-debuginfo-1.0.2-15.1

i586
irssi-devel-1.0.2-15.1
irssi-debugsource-1.0.2-15.1
irssi-1.0.2-15.1
irssi-debuginfo-1.0.2-15.1

145597 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0690-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0690-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00044.html>

SuSE Linux 42.1
i586
MozillaFirefox-devel-52.0-55.1

MozillaFirefox-branding-upstream-52.0-55.1
mozilla-nss-certs-debuginfo-3.28.3-38.1
mozilla-nss-debugsource-3.28.3-38.1
mozilla-nss-sysinit-3.28.3-38.1
MozillaFirefox-debugsource-52.0-55.1
java-1_8_0-openjdk-src-1.8.0.121-23.1
java-1_8_0-openjdk-1.8.0.121-23.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-23.1
java-1_8_0-openjdk-debuginfo-1.8.0.121-23.1
libfreebl3-debuginfo-3.28.3-38.1
java-1_8_0-openjdk-headless-1.8.0.121-23.1
mozilla-nss-3.28.3-38.1
libsoftokn3-debuginfo-3.28.3-38.1
mozilla-nss-devel-3.28.3-38.1
libsoftokn3-3.28.3-38.1
MozillaFirefox-translations-other-52.0-55.1
mozilla-nss-sysinit-debuginfo-3.28.3-38.1
mozilla-nss-tools-debuginfo-3.28.3-38.1
java-1_8_0-openjdk-debugsource-1.8.0.121-23.1
MozillaFirefox-buildsymbols-52.0-55.1
java-1_8_0-openjdk-devel-1.8.0.121-23.1
MozillaFirefox-debuginfo-52.0-55.1
libfreebl3-3.28.3-38.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-23.1
mozilla-nss-certs-3.28.3-38.1
MozillaFirefox-52.0-55.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-23.1
mozilla-nss-tools-3.28.3-38.1
mozilla-nss-debuginfo-3.28.3-38.1
java-1_8_0-openjdk-accessibility-1.8.0.121-23.1
java-1_8_0-openjdk-demo-1.8.0.121-23.1
MozillaFirefox-translations-common-52.0-55.1

noarch

java-1_8_0-openjdk-javadoc-1.8.0.121-23.1

x86_64

libsoftokn3-32bit-3.28.3-38.1
MozillaFirefox-debugsource-52.0-55.2
mozilla-nss-certs-debuginfo-3.28.3-38.1
mozilla-nss-debugsource-3.28.3-38.1
mozilla-nss-sysinit-3.28.3-38.1
MozillaFirefox-translations-other-52.0-55.2
mozilla-nss-sysinit-debuginfo-32bit-3.28.3-38.1
libfreebl3-32bit-3.28.3-38.1
java-1_8_0-openjdk-src-1.8.0.121-23.1
java-1_8_0-openjdk-1.8.0.121-23.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-23.1
java-1_8_0-openjdk-debuginfo-1.8.0.121-23.1
libfreebl3-debuginfo-3.28.3-38.1
java-1_8_0-openjdk-headless-1.8.0.121-23.1
mozilla-nss-3.28.3-38.1
libsoftokn3-debuginfo-32bit-3.28.3-38.1
libsoftokn3-debuginfo-3.28.3-38.1
mozilla-nss-devel-3.28.3-38.1
libsoftokn3-3.28.3-38.1
mozilla-nss-sysinit-debuginfo-3.28.3-38.1
mozilla-nss-tools-debuginfo-3.28.3-38.1
java-1_8_0-openjdk-debugsource-1.8.0.121-23.1
MozillaFirefox-translations-common-52.0-55.2

java-1_8_0-openjdk-devel-1.8.0.121-23.1
MozillaFirefox-52.0-55.2
libfreebl3-3.28.3-38.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-23.1
mozilla-nss-certs-3.28.3-38.1
mozilla-nss-sysinit-32bit-3.28.3-38.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-23.1
MozillaFirefox-branding-upstream-52.0-55.2
libfreebl3-debuginfo-32bit-3.28.3-38.1
mozilla-nss-debuginfo-32bit-3.28.3-38.1
mozilla-nss-tools-3.28.3-38.1
mozilla-nss-32bit-3.28.3-38.1
MozillaFirefox-devel-52.0-55.2
mozilla-nss-debuginfo-3.28.3-38.1
java-1_8_0-openjdk-accessibility-1.8.0.121-23.1
MozillaFirefox-debuginfo-52.0-55.2
java-1_8_0-openjdk-demo-1.8.0.121-23.1
mozilla-nss-certs-32bit-3.28.3-38.1
mozilla-nss-certs-debuginfo-32bit-3.28.3-38.1
MozillaFirefox-buildsymbols-52.0-55.2

SuSE Linux 42.2

i586

MozillaFirefox-debugsource-52.0-55.2
java-1_8_0-openjdk-accessibility-1.8.0.121-8.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-8.1
mozilla-nss-certs-debuginfo-3.28.3-38.1
mozilla-nss-debugsource-3.28.3-38.1
mozilla-nss-sysinit-3.28.3-38.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-8.1
java-1_8_0-openjdk-headless-1.8.0.121-8.1
libfreebl3-debuginfo-3.28.3-38.1
MozillaFirefox-devel-52.0-55.2
MozillaFirefox-translations-common-52.0-55.2
java-1_8_0-openjdk-debugsource-1.8.0.121-8.1
libsoftokn3-debuginfo-3.28.3-38.1
mozilla-nss-devel-3.28.3-38.1
libsoftokn3-3.28.3-38.1
java-1_8_0-openjdk-demo-1.8.0.121-8.1
mozilla-nss-sysinit-debuginfo-3.28.3-38.1
MozillaFirefox-buildsymbols-52.0-55.2
java-1_8_0-openjdk-debuginfo-1.8.0.121-8.1
MozillaFirefox-52.0-55.2
java-1_8_0-openjdk-src-1.8.0.121-8.1
libfreebl3-3.28.3-38.1
java-1_8_0-openjdk-1.8.0.121-8.1
java-1_8_0-openjdk-devel-1.8.0.121-8.1
MozillaFirefox-translations-other-52.0-55.2
mozilla-nss-debuginfo-3.28.3-38.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-8.1
mozilla-nss-3.28.3-38.1
mozilla-nss-tools-3.28.3-38.1
mozilla-nss-tools-debuginfo-3.28.3-38.1
mozilla-nss-certs-3.28.3-38.1
MozillaFirefox-branding-upstream-52.0-55.2
MozillaFirefox-debuginfo-52.0-55.2

noarch

java-1_8_0-openjdk-javadoc-1.8.0.121-8.1

x86_64
libsoftokn3-32bit-3.28.3-38.1
MozillaFirefox-debugsource-52.0-55.2
java-1_8_0-openjdk-accessibility-1.8.0.121-8.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-8.1
mozilla-nss-certs-debuginfo-3.28.3-38.1
mozilla-nss-debugsource-3.28.3-38.1
mozilla-nss-sysinit-3.28.3-38.1
mozilla-nss-sysinit-debuginfo-32bit-3.28.3-38.1
libfreebl3-32bit-3.28.3-38.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-8.1
java-1_8_0-openjdk-headless-1.8.0.121-8.1
libsoftokn3-debuginfo-32bit-3.28.3-38.1
libfreebl3-debuginfo-3.28.3-38.1
MozillaFirefox-devel-52.0-55.2
MozillaFirefox-translations-common-52.0-55.2
java-1_8_0-openjdk-debugsource-1.8.0.121-8.1
libsoftokn3-debuginfo-3.28.3-38.1
mozilla-nss-devel-3.28.3-38.1
libsoftokn3-3.28.3-38.1
java-1_8_0-openjdk-demo-1.8.0.121-8.1
mozilla-nss-sysinit-debuginfo-3.28.3-38.1
MozillaFirefox-buildsymbols-52.0-55.2
mozilla-nss-debuginfo-32bit-3.28.3-38.1
java-1_8_0-openjdk-debuginfo-1.8.0.121-8.1
MozillaFirefox-52.0-55.2
java-1_8_0-openjdk-src-1.8.0.121-8.1
libfreebl3-3.28.3-38.1
java-1_8_0-openjdk-1.8.0.121-8.1
mozilla-nss-sysinit-32bit-3.28.3-38.1
java-1_8_0-openjdk-devel-1.8.0.121-8.1
MozillaFirefox-translations-other-52.0-55.2
mozilla-nss-debuginfo-3.28.3-38.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-8.1
libfreebl3-debuginfo-32bit-3.28.3-38.1
mozilla-nss-3.28.3-38.1
mozilla-nss-tools-3.28.3-38.1
mozilla-nss-tools-debuginfo-3.28.3-38.1
mozilla-nss-32bit-3.28.3-38.1
mozilla-nss-certs-3.28.3-38.1
MozillaFirefox-branding-upstream-52.0-55.2
MozillaFirefox-debuginfo-52.0-55.2
mozilla-nss-certs-32bit-3.28.3-38.1
mozilla-nss-certs-debuginfo-32bit-3.28.3-38.1

145600 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1099-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5429, CVE-2017-5443, CVE-2017-5444, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5460, CVE-2017-5461, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467

Description

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

openSUSE-SU-2017:1099-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00091.html>

SuSE Linux 42.1

x86_64

MozillaFirefox-devel-52.1.0-61.1

MozillaFirefox-branding-upstream-52.1.0-61.1

MozillaFirefox-debuginfo-52.1.0-61.1

MozillaFirefox-translations-other-52.1.0-61.1

MozillaFirefox-debugsource-52.1.0-61.1

MozillaFirefox-52.1.0-61.1

MozillaFirefox-translations-common-52.1.0-61.1

MozillaFirefox-buildsymbols-52.1.0-61.1

SuSE Linux 42.2

x86_64

MozillaFirefox-debuginfo-52.1.0-57.6.1

MozillaFirefox-translations-other-52.1.0-57.6.1

MozillaFirefox-branding-upstream-52.1.0-57.6.1

MozillaFirefox-debugsource-52.1.0-57.6.1

MozillaFirefox-translations-common-52.1.0-57.6.1

MozillaFirefox-buildsymbols-52.1.0-57.6.1

MozillaFirefox-52.1.0-57.6.1

MozillaFirefox-devel-52.1.0-57.6.1

i586

MozillaFirefox-debuginfo-52.1.0-57.6.1

MozillaFirefox-translations-other-52.1.0-57.6.1

MozillaFirefox-branding-upstream-52.1.0-57.6.1

MozillaFirefox-debugsource-52.1.0-57.6.1

MozillaFirefox-translations-common-52.1.0-57.6.1

MozillaFirefox-buildsymbols-52.1.0-57.6.1

MozillaFirefox-52.1.0-57.6.1

MozillaFirefox-devel-52.1.0-57.6.1

145602 - SuSE Linux 42.2 openSUSE-SU-2017:1679-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:1679-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00092.html>

SuSE Linux 42.2

i586

libqt5-qtdeclarative-tools-5.6.1-7.3.1

libQt5DBus5-debuginfo-5.6.1-3.3.1

libQt5Sql-devel-5.6.1-3.3.1

libQt5Xml-devel-5.6.1-3.3.1

libQt5Sql5-sqlite-debuginfo-5.6.1-3.3.1
libQt5Gui5-debuginfo-5.6.1-3.3.1
libQt5Network5-debuginfo-5.6.1-3.3.1
libqt5-qtdeclarative-debugsource-5.6.1-7.3.1
libqt5-qtbase-examples-5.6.1-3.3.1
libQtQuick5-debuginfo-5.6.1-7.3.1
libQt5Sql5-unixODBC-debuginfo-5.6.1-3.3.1
libqt5-qtbase-common-devel-debuginfo-5.6.1-3.3.1
libQt5PrintSupport5-debuginfo-5.6.1-3.3.1
libQt5Concurrent-devel-5.6.1-3.3.1
libQt5Widgets5-5.6.1-3.3.1
libQt5DBus-devel-5.6.1-3.3.1
libqt5-qtdeclarative-examples-debuginfo-5.6.1-7.3.1
libQt5Gui5-5.6.1-3.3.1
libQt5OpenGL5-debuginfo-5.6.1-3.3.1
libQt5OpenGL5-5.6.1-3.3.1
libQt5Test5-debuginfo-5.6.1-3.3.1
libqt5-qtbase-devel-5.6.1-3.3.1
libqt5-qtdeclarative-tools-debuginfo-5.6.1-7.3.1
libqt5-qtdeclarative-devel-5.6.1-7.3.1
libQt5Test5-5.6.1-3.3.1
libQt5Gui-devel-5.6.1-3.3.1
libqt5-qtbase-common-devel-5.6.1-3.3.1
libQt5Bootstrap-devel-static-5.6.1-3.3.1
libQt5OpenGL-devel-5.6.1-3.3.1
libQt5Xml5-5.6.1-3.3.1
libQt5Sql5-sqlite-5.6.1-3.3.1
libQt5Core-devel-5.6.1-3.3.1
libQt5Xml5-debuginfo-5.6.1-3.3.1
libQt5Sql5-unixODBC-5.6.1-3.3.1
libQt5Network5-5.6.1-3.3.1
libQtQuick5-5.6.1-7.3.1
libQt5Sql5-mysql-debuginfo-5.6.1-3.3.1
libQt5Widgets5-debuginfo-5.6.1-3.3.1
libQt5Sql5-debuginfo-5.6.1-3.3.1
libQt5Network-devel-5.6.1-3.3.1
libQt5DBus5-5.6.1-3.3.1
libQt5PlatformHeaders-devel-5.6.1-3.3.1
libQt5Core5-5.6.1-3.3.1
libQt5Sql5-5.6.1-3.3.1
libQt5Core5-debuginfo-5.6.1-3.3.1
libQt5PlatformSupport-devel-static-5.6.1-3.3.1
libqt5-qtdeclarative-devel-debuginfo-5.6.1-7.3.1
libQt5Sql5-mysql-5.6.1-3.3.1
libqt5-qtbase-examples-debuginfo-5.6.1-3.3.1
libQt5Widgets-devel-5.6.1-3.3.1
libQt5DBus-devel-debuginfo-5.6.1-3.3.1
libQt5Sql5-postgresql-debuginfo-5.6.1-3.3.1
libQt5Concurrent5-5.6.1-3.3.1
libQt5OpenGLExtensions-devel-static-5.6.1-3.3.1
libqt5-qtbase-debugsource-5.6.1-3.3.1
libQt5PrintSupport5-5.6.1-3.3.1
libQt5Concurrent5-debuginfo-5.6.1-3.3.1
libqt5-qtdeclarative-examples-5.6.1-7.3.1
libQt5PrintSupport-devel-5.6.1-3.3.1
libQt5Sql5-postgresql-5.6.1-3.3.1
libQt5Test-devel-5.6.1-3.3.1

noarch

libqt5-qtbase-private-headers-devel-5.6.1-3.3.1

libQt5Widgets-private-headers-devel-5.6.1-3.3.1
libqt5-qtdeclarative-private-headers-devel-5.6.1-7.3.1
libQt5PlatformSupport-private-headers-devel-5.6.1-3.3.1
libQt5Core-private-headers-devel-5.6.1-3.3.1
libQt5Test-private-headers-devel-5.6.1-3.3.1
libQt5Gui-private-headers-devel-5.6.1-3.3.1
libQt5PrintSupport-private-headers-devel-5.6.1-3.3.1
libQt5OpenGL-private-headers-devel-5.6.1-3.3.1
libQt5Sql-private-headers-devel-5.6.1-3.3.1
libQt5Network-private-headers-devel-5.6.1-3.3.1
libQt5DBus-private-headers-devel-5.6.1-3.3.1

x86_64

libQt5Network5-32bit-5.6.1-3.3.1
libQt5Bootstrap-devel-static-5.6.1-3.3.1
libQt5PrintSupport5-5.6.1-3.3.1
libQt5Core5-debuginfo-5.6.1-3.3.1
libQt5Core5-32bit-5.6.1-3.3.1
libQt5OpenGL5-debuginfo-32bit-5.6.1-3.3.1
libqt5-qtbase-examples-debuginfo-32bit-5.6.1-3.3.1
libQt5Core-devel-32bit-5.6.1-3.3.1
libQt5PrintSupport-devel-32bit-5.6.1-3.3.1
libqt5-qtbase-debugsource-5.6.1-3.3.1
libQt5Widgets-devel-32bit-5.6.1-3.3.1
libQt5Network-devel-5.6.1-3.3.1
libQt5Sql5-mysql-5.6.1-3.3.1
libQt5Xml5-5.6.1-3.3.1
libQt5Gui-devel-32bit-5.6.1-3.3.1
libQt5Sql5-5.6.1-3.3.1
libQt5Sql5-unixODBC-32bit-5.6.1-3.3.1
libQt5Concurrent-devel-32bit-5.6.1-3.3.1
libqt5-qtbase-devel-5.6.1-3.3.1
libQt5DBus5-5.6.1-3.3.1
libQt5Xml5-32bit-5.6.1-3.3.1
libQt5OpenGL-devel-5.6.1-3.3.1
libQt5Network5-debuginfo-5.6.1-3.3.1
libQt5Network5-debuginfo-32bit-5.6.1-3.3.1
libQt5Sql5-unixODBC-debuginfo-32bit-5.6.1-3.3.1
libQt5PrintSupport5-debuginfo-32bit-5.6.1-3.3.1
libQt5Sql5-mysql-debuginfo-32bit-5.6.1-3.3.1
libQt5Sql5-debuginfo-5.6.1-3.3.1
libQt5Test5-debuginfo-5.6.1-3.3.1
libQt5OpenGL-devel-32bit-5.6.1-3.3.1
libQt5Core5-debuginfo-32bit-5.6.1-3.3.1
libQtQuick5-5.6.1-7.3.1
libQt5PrintSupport-devel-5.6.1-3.3.1
libQt5Sql-devel-5.6.1-3.3.1
libQt5Sql5-postgresql-debuginfo-5.6.1-3.3.1
libQt5DBus-devel-debuginfo-32bit-5.6.1-3.3.1
libqt5-qtdeclarative-devel-5.6.1-7.3.1
libQt5Core5-5.6.1-3.3.1
libQt5Gui5-debuginfo-5.6.1-3.3.1
libQt5Gui5-32bit-5.6.1-3.3.1
libqt5-qtbase-common-devel-5.6.1-3.3.1
libqt5-qtdeclarative-devel-32bit-5.6.1-7.3.1
libqt5-qtdeclarative-debugsource-5.6.1-7.3.1
libQt5Concurrent5-32bit-5.6.1-3.3.1
libQt5PrintSupport5-debuginfo-5.6.1-3.3.1
libQt5Sql5-32bit-5.6.1-3.3.1
libQt5Test-devel-32bit-5.6.1-3.3.1

libQt5Test5-32bit-5.6.1-3.3.1
libqt5-qtdeclarative-tools-5.6.1-7.3.1
libqt5-qtbase-examples-5.6.1-3.3.1
libQt5Xml-devel-32bit-5.6.1-3.3.1
libQt5Sql5-unixODBC-5.6.1-3.3.1
libQt5Sql5-sqlite-5.6.1-3.3.1
libQt5Sql5-unixODBC-debuginfo-5.6.1-3.3.1
libQt5Sql5-mysql-debuginfo-5.6.1-3.3.1
libQt5Xml-devel-5.6.1-3.3.1
libQt5Sql5-mysql-32bit-5.6.1-3.3.1
libQt5Network5-5.6.1-3.3.1
libQt5Core-devel-5.6.1-3.3.1
libQt5DBus5-32bit-5.6.1-3.3.1
libQt5DBus5-debuginfo-32bit-5.6.1-3.3.1
libQt5Sql5-postgresql-32bit-5.6.1-3.3.1
libqt5-qtbase-examples-32bit-5.6.1-3.3.1
libQt5Sql5-debuginfo-32bit-5.6.1-3.3.1
libQt5Sql5-postgresql-debuginfo-32bit-5.6.1-3.3.1
libQtQuick5-debuginfo-32bit-5.6.1-7.3.1
libQt5Test-devel-5.6.1-3.3.1
libQt5PrintSupport5-32bit-5.6.1-3.3.1
libQt5DBus-devel-32bit-5.6.1-3.3.1
libQt5Concurrent-devel-5.6.1-3.3.1
libQt5PlatformSupport-devel-static-5.6.1-3.3.1
libQt5Concurrent5-debuginfo-32bit-5.6.1-3.3.1
libQt5DBus5-debuginfo-5.6.1-3.3.1
libQt5Widgets5-debuginfo-5.6.1-3.3.1
libQt5Sql5-postgresql-5.6.1-3.3.1
libQt5Concurrent5-debuginfo-5.6.1-3.3.1
libQtQuick5-debuginfo-5.6.1-7.3.1
libQt5Widgets5-debuginfo-32bit-5.6.1-3.3.1
libQt5DBus-devel-5.6.1-3.3.1
libQt5Sql-devel-32bit-5.6.1-3.3.1
libqt5-qtdeclarative-devel-debuginfo-32bit-5.6.1-7.3.1
libQt5OpenGL5-debuginfo-5.6.1-3.3.1
libQt5Widgets5-32bit-5.6.1-3.3.1
libQt5Sql5-sqlite-debuginfo-32bit-5.6.1-3.3.1
libQt5Sql5-sqlite-debuginfo-5.6.1-3.3.1
libqt5-qtdeclarative-examples-debuginfo-5.6.1-7.3.1
libQtQuick5-32bit-5.6.1-7.3.1
libqt5-qtdeclarative-examples-5.6.1-7.3.1
libqt5-qtdeclarative-devel-debuginfo-5.6.1-7.3.1
libQt5Test5-debuginfo-32bit-5.6.1-3.3.1
libQt5OpenGL5-5.6.1-3.3.1
libQt5Widgets-devel-5.6.1-3.3.1
libQt5Xml5-debuginfo-5.6.1-3.3.1
libQt5Gui5-debuginfo-32bit-5.6.1-3.3.1
libQt5PlatformSupport-devel-static-32bit-5.6.1-3.3.1
libQt5DBus-devel-debuginfo-5.6.1-3.3.1
libqt5-qtdeclarative-tools-debuginfo-5.6.1-7.3.1
libQt5Concurrent5-5.6.1-3.3.1
libQt5OpenGL5-32bit-5.6.1-3.3.1
libQt5OpenGLExtensions-devel-static-32bit-5.6.1-3.3.1
libQt5Xml5-debuginfo-32bit-5.6.1-3.3.1
libqt5-qtbase-examples-debuginfo-5.6.1-3.3.1
libQt5Gui-devel-5.6.1-3.3.1
libQt5Bootstrap-devel-static-32bit-5.6.1-3.3.1
libQt5OpenGLExtensions-devel-static-5.6.1-3.3.1
libQt5Widgets5-5.6.1-3.3.1
libQt5Gui5-5.6.1-3.3.1

libQt5Network-devel-32bit-5.6.1-3.3.1
libQt5PlatformHeaders-devel-5.6.1-3.3.1
libqt5-qtbase-common-devel-debuginfo-5.6.1-3.3.1

145604 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2158-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10684, CVE-2017-10685, CVE-2017-11112, CVE-2017-11113

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2158-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00048.html>

SuSE Linux 42.2

x86_64
terminfo-base-5.9-55.6.1
libncurses6-debuginfo-5.9-55.6.1
ncurses-devel-32bit-5.9-55.6.1
ncurses-devel-5.9-55.6.1
libncurses5-debuginfo-5.9-55.6.1
ncurses-devel-debuginfo-32bit-5.9-55.6.1
terminfo-5.9-55.6.1
libncurses6-32bit-5.9-55.6.1
libncurses5-5.9-55.6.1
tack-debuginfo-5.9-55.6.1
ncurses-utils-debuginfo-5.9-55.6.1
libncurses5-32bit-5.9-55.6.1
ncurses-devel-debuginfo-5.9-55.6.1
tack-5.9-55.6.1
ncurses-debugsource-5.9-55.6.1
libncurses5-debuginfo-32bit-5.9-55.6.1
libncurses6-debuginfo-32bit-5.9-55.6.1
libncurses6-5.9-55.6.1
ncurses-utils-5.9-55.6.1

i586

terminfo-base-5.9-55.6.1
libncurses6-debuginfo-5.9-55.6.1
ncurses-devel-5.9-55.6.1
libncurses5-debuginfo-5.9-55.6.1
terminfo-5.9-55.6.1
libncurses5-5.9-55.6.1
tack-debuginfo-5.9-55.6.1
ncurses-utils-debuginfo-5.9-55.6.1
ncurses-devel-debuginfo-5.9-55.6.1
tack-5.9-55.6.1
ncurses-debugsource-5.9-55.6.1
libncurses6-5.9-55.6.1
ncurses-utils-5.9-55.6.1

SuSE Linux 42.3

x86_64
libncurses5-32bit-5.9-59.1
tack-5.9-59.1
tack-debuginfo-5.9-59.1
libncurses6-32bit-5.9-59.1
libncurses5-5.9-59.1
ncurses-devel-debuginfo-32bit-5.9-59.1
libncurses6-debuginfo-5.9-59.1
libncurses6-debuginfo-32bit-5.9-59.1
libncurses5-debuginfo-5.9-59.1
ncurses-devel-5.9-59.1
ncurses-debugsource-5.9-59.1
ncurses-devel-debuginfo-5.9-59.1
libncurses6-5.9-59.1
ncurses-utils-5.9-59.1
ncurses-utils-debuginfo-5.9-59.1
terminfo-5.9-59.1
terminfo-base-5.9-59.1
libncurses5-debuginfo-32bit-5.9-59.1
ncurses-devel-32bit-5.9-59.1

i586
tack-5.9-59.1
tack-debuginfo-5.9-59.1
libncurses5-5.9-59.1
libncurses6-debuginfo-5.9-59.1
libncurses5-debuginfo-5.9-59.1
ncurses-devel-5.9-59.1
ncurses-debugsource-5.9-59.1
ncurses-devel-debuginfo-5.9-59.1
libncurses6-5.9-59.1
ncurses-utils-5.9-59.1
ncurses-utils-debuginfo-5.9-59.1
terminfo-5.9-59.1
terminfo-base-5.9-59.1

145605 - SuSE Linux 42.2 openSUSE-SU-2017:1520-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1520-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00027.html>

SuSE Linux 42.2

x86_64
catdoc-debuginfo-0.95-7.3.1
catdoc-debugsource-0.95-7.3.1
catdoc-0.95-7.3.1

i586
catdoc-debuginfo-0.95-7.3.1
catdoc-debugsource-0.95-7.3.1
catdoc-0.95-7.3.1

145607 - SuSE Linux 42.2 openSUSE-SU-2017:0910-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9579

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0910-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00004.html>

SuSE Linux 42.2

x86_64

ceph-radosgw-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
python-cephfs-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-test-10.2.6+git.1489493035.3ad7a68-6.4.1
libcephfs1-10.2.6+git.1489493035.3ad7a68-6.4.1
librados-devel-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
rbd-nbd-10.2.6+git.1489493035.3ad7a68-6.4.1
librados2-10.2.6+git.1489493035.3ad7a68-6.4.1
librgw-devel-10.2.6+git.1489493035.3ad7a68-6.4.1
python-rbd-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-osd-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
python-rbd-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
librados-devel-10.2.6+git.1489493035.3ad7a68-6.4.1
libradosstriper1-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-common-10.2.6+git.1489493035.3ad7a68-6.4.1
librados2-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-base-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-base-10.2.6+git.1489493035.3ad7a68-6.4.1
librbd1-10.2.6+git.1489493035.3ad7a68-6.4.1
librgw2-10.2.6+git.1489493035.3ad7a68-6.4.1
librbd1-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-common-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
python-cephfs-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-mds-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
python-rados-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
librbd-devel-10.2.6+git.1489493035.3ad7a68-6.4.1
libcephfs-devel-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-osd-10.2.6+git.1489493035.3ad7a68-6.4.1
rbd-mirror-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
libradosstriper-devel-10.2.6+git.1489493035.3ad7a68-6.4.1
librgw2-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-fuse-10.2.6+git.1489493035.3ad7a68-6.4.1
python-rados-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-test-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
libcephfs1-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-fuse-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1

ceph-mds-10.2.6+git.1489493035.3ad7a68-6.4.1
rbd-fuse-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-mon-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-resource-agents-10.2.6+git.1489493035.3ad7a68-6.4.1
rbd-fuse-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-radosgw-10.2.6+git.1489493035.3ad7a68-6.4.1
rbd-nbd-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-10.2.6+git.1489493035.3ad7a68-6.4.1
python-ceph-compat-10.2.6+git.1489493035.3ad7a68-6.4.1
rbd-mirror-10.2.6+git.1489493035.3ad7a68-6.4.1
ceph-mon-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1
libradosstriper1-debuginfo-10.2.6+git.1489493035.3ad7a68-6.4.1

145608 - SuSE Linux 42.3 openSUSE-SU-2017:1934-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:1934-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00084.html>

SuSE Linux 42.3

x86_64

xorg-x11-server-extra-debuginfo-7.6_1.18.3-22.1

xorg-x11-server-debugsource-7.6_1.18.3-22.1

xorg-x11-server-sdk-7.6_1.18.3-22.1

xorg-x11-server-extra-7.6_1.18.3-22.1

xorg-x11-server-source-7.6_1.18.3-22.1

xorg-x11-server-debuginfo-7.6_1.18.3-22.1

xorg-x11-server-7.6_1.18.3-22.1

i586

xorg-x11-server-extra-debuginfo-7.6_1.18.3-22.1

xorg-x11-server-debugsource-7.6_1.18.3-22.1

xorg-x11-server-sdk-7.6_1.18.3-22.1

xorg-x11-server-extra-7.6_1.18.3-22.1

xorg-x11-server-source-7.6_1.18.3-22.1

xorg-x11-server-debuginfo-7.6_1.18.3-22.1

xorg-x11-server-7.6_1.18.3-22.1

145615 - SuSE Linux 42.2 openSUSE-SU-2017:1516-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10375

Description

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

openSUSE-SU-2017:1516-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00026.html>

SuSE Linux 42.2
x86_64
yodl-3.05.01-3.3.1
yodl-debuginfo-3.05.01-3.3.1
yodl-debugsource-3.05.01-3.3.1

145620 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2120-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5946

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2120-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00025.html>

SuSE Linux 42.2
x86_64
ruby2.1-rubygem-rubyzip-doc-1.1.7-5.3.1
ruby2.1-rubygem-rubyzip-testsuite-1.1.7-5.3.1
ruby2.1-rubygem-rubyzip-1.1.7-5.3.1

i586
ruby2.1-rubygem-rubyzip-doc-1.1.7-5.3.1
ruby2.1-rubygem-rubyzip-testsuite-1.1.7-5.3.1
ruby2.1-rubygem-rubyzip-1.1.7-5.3.1

SuSE Linux 42.3
x86_64
ruby2.2-rubygem-rubyzip-1.1.7-8.1
ruby2.2-rubygem-rubyzip-doc-1.1.7-8.1
ruby2.1-rubygem-rubyzip-doc-1.1.7-8.1
ruby2.4-rubygem-rubyzip-doc-1.1.7-8.1
ruby2.4-rubygem-rubyzip-testsuite-1.1.7-8.1
ruby2.1-rubygem-rubyzip-1.1.7-8.1
ruby2.3-rubygem-rubyzip-doc-1.1.7-8.1
ruby2.2-rubygem-rubyzip-testsuite-1.1.7-8.1
ruby2.1-rubygem-rubyzip-testsuite-1.1.7-8.1
ruby2.3-rubygem-rubyzip-1.1.7-8.1
ruby2.4-rubygem-rubyzip-1.1.7-8.1
ruby2.3-rubygem-rubyzip-testsuite-1.1.7-8.1

i586

ruby2.2-rubygem-rubyzip-1.1.7-8.1
ruby2.2-rubygem-rubyzip-doc-1.1.7-8.1
ruby2.1-rubygem-rubyzip-doc-1.1.7-8.1
ruby2.4-rubygem-rubyzip-doc-1.1.7-8.1
ruby2.4-rubygem-rubyzip-testsuite-1.1.7-8.1
ruby2.1-rubygem-rubyzip-1.1.7-8.1
ruby2.3-rubygem-rubyzip-doc-1.1.7-8.1
ruby2.2-rubygem-rubyzip-testsuite-1.1.7-8.1
ruby2.1-rubygem-rubyzip-testsuite-1.1.7-8.1
ruby2.3-rubygem-rubyzip-1.1.7-8.1
ruby2.4-rubygem-rubyzip-1.1.7-8.1
ruby2.3-rubygem-rubyzip-testsuite-1.1.7-8.1

145621 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1098-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1098-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00090.html>

SuSE Linux 42.1

x86_64

chromium-debuginfo-58.0.3029.81-111.1

chromium-58.0.3029.81-111.1

chromium-debugsource-58.0.3029.81-111.1

chromedriver-58.0.3029.81-111.1

chromedriver-debuginfo-58.0.3029.81-111.1

SuSE Linux 42.2

x86_64

chromium-debugsource-58.0.3029.81-104.9.1

chromedriver-debuginfo-58.0.3029.81-104.9.1

chromedriver-58.0.3029.81-104.9.1

chromium-58.0.3029.81-104.9.1

chromium-debuginfo-58.0.3029.81-104.9.1

145628 - SuSE Linux 42.2 openSUSE-SU-2017:1801-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2626

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1801-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00030.html>

SuSE Linux 42.2

x86_64

libICE-devel-32bit-1.0.9-5.3.1
libICE6-debuginfo-32bit-1.0.9-5.3.1
libICE6-debuginfo-1.0.9-5.3.1
libICE6-1.0.9-5.3.1
libICE-debugsource-1.0.9-5.3.1
libICE6-32bit-1.0.9-5.3.1
libICE-devel-1.0.9-5.3.1

i586

libICE-debugsource-1.0.9-5.3.1
libICE-devel-1.0.9-5.3.1
libICE6-debuginfo-1.0.9-5.3.1
libICE6-1.0.9-5.3.1

145631 - SuSE Linux 42.2 openSUSE-SU-2017:1609-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9148

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1609-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00069.html>

SuSE Linux 42.2

x86_64

freeradius-server-debuginfo-3.0.12-2.3.1
freeradius-server-ldap-debuginfo-3.0.12-2.3.1
freeradius-server-mysql-3.0.12-2.3.1
freeradius-server-devel-3.0.12-2.3.1
freeradius-server-utils-3.0.12-2.3.1
freeradius-server-3.0.12-2.3.1
freeradius-server-perl-debuginfo-3.0.12-2.3.1
freeradius-server-krb5-debuginfo-3.0.12-2.3.1
freeradius-server-debugsource-3.0.12-2.3.1
freeradius-server-postgresql-debuginfo-3.0.12-2.3.1
freeradius-server-sqlite-debuginfo-3.0.12-2.3.1
freeradius-server-krb5-3.0.12-2.3.1
freeradius-server-doc-3.0.12-2.3.1
freeradius-server-python-debuginfo-3.0.12-2.3.1
freeradius-server-mysql-debuginfo-3.0.12-2.3.1
freeradius-server-libs-3.0.12-2.3.1
freeradius-server-utils-debuginfo-3.0.12-2.3.1
freeradius-server-perl-3.0.12-2.3.1

freeradius-server-python-3.0.12-2.3.1
freeradius-server-ldap-3.0.12-2.3.1
freeradius-server-libs-debuginfo-3.0.12-2.3.1
freeradius-server-postgresql-3.0.12-2.3.1
freeradius-server-sqlite-3.0.12-2.3.1

145636 - SuSE Linux 42.2 openSUSE-SU-2017:1497-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7178, CVE-2017-9031

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1497-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00014.html>

SuSE Linux 42.2
noarch
deluge-1.3.15-3.3.1
deluge-lang-1.3.15-3.3.1

145639 - SuSE Linux 42.2 openSUSE-SU-2017:1803-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3167, CVE-2017-3169, CVE-2017-7679

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1803-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00032.html>

SuSE Linux 42.2
i586
apache2-2.4.23-8.6.1
apache2-utils-debuginfo-2.4.23-8.6.1
apache2-prefork-debuginfo-2.4.23-8.6.1
apache2-worker-2.4.23-8.6.1
apache2-example-pages-2.4.23-8.6.1
apache2-debugsource-2.4.23-8.6.1
apache2-utils-2.4.23-8.6.1
apache2-debuginfo-2.4.23-8.6.1
apache2-worker-debuginfo-2.4.23-8.6.1
apache2-prefork-2.4.23-8.6.1
apache2-devel-2.4.23-8.6.1

apache2-event-2.4.23-8.6.1
apache2-event-debuginfo-2.4.23-8.6.1

noarch
apache2-doc-2.4.23-8.6.1

x86_64
apache2-2.4.23-8.6.1
apache2-utils-debuginfo-2.4.23-8.6.1
apache2-prefork-debuginfo-2.4.23-8.6.1
apache2-worker-2.4.23-8.6.1
apache2-example-pages-2.4.23-8.6.1
apache2-debugsource-2.4.23-8.6.1
apache2-utils-2.4.23-8.6.1
apache2-debuginfo-2.4.23-8.6.1
apache2-worker-debuginfo-2.4.23-8.6.1
apache2-prefork-2.4.23-8.6.1
apache2-devel-2.4.23-8.6.1
apache2-event-2.4.23-8.6.1
apache2-event-debuginfo-2.4.23-8.6.1

145640 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2125-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10686, CVE-2017-11111

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2125-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00030.html>

SuSE Linux 42.2
x86_64
nasm-doc-2.10.09-7.3.1
nasm-debuginfo-2.10.09-7.3.1
nasm-2.10.09-7.3.1
nasm-debugsource-2.10.09-7.3.1

i586
nasm-doc-2.10.09-7.3.1
nasm-debuginfo-2.10.09-7.3.1
nasm-2.10.09-7.3.1
nasm-debugsource-2.10.09-7.3.1

SuSE Linux 42.3
x86_64
nasm-debuginfo-2.10.09-10.1
nasm-2.10.09-10.1
nasm-debugsource-2.10.09-10.1
nasm-doc-2.10.09-10.1

i586

nasm-debuginfo-2.10.09-10.1
nasm-2.10.09-10.1
nasm-debugsource-2.10.09-10.1
nasm-doc-2.10.09-10.1

145641 - SuSE Linux 42.2 openSUSE-SU-2017:1460-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6886, CVE-2017-6887, CVE-2017-6889, CVE-2017-6890

Description

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

openSUSE-SU-2017:1460-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00111.html>

SuSE Linux 42.2

x86_64

libraw15-0.17.1-2.3.1

libraw-tools-debuginfo-0.17.1-2.3.1

libraw15-debuginfo-0.17.1-2.3.1

libraw-devel-0.17.1-2.3.1

libraw-devel-static-0.17.1-2.3.1

libraw-tools-0.17.1-2.3.1

libraw-debugsource-0.17.1-2.3.1

i586

libraw15-0.17.1-2.3.1

libraw-tools-debuginfo-0.17.1-2.3.1

libraw15-debuginfo-0.17.1-2.3.1

libraw-devel-0.17.1-2.3.1

libraw-devel-static-0.17.1-2.3.1

libraw-tools-0.17.1-2.3.1

libraw-debugsource-0.17.1-2.3.1

145642 - SuSE Linux 42.2 openSUSE-SU-2017:1757-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6294, CVE-2017-9224, CVE-2017-9226, CVE-2017-9227

Description

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

openSUSE-SU-2017:1757-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00011.html>

SuSE Linux 42.2

i586

php5-shmop-5.5.14-77.6.1
php5-xmlwriter-debuginfo-5.5.14-77.6.1
php5-fileinfo-5.5.14-77.6.1
php5-xmlrpc-debuginfo-5.5.14-77.6.1
php5-readline-5.5.14-77.6.1
php5-mssql-5.5.14-77.6.1
php5-fastcgi-debuginfo-5.5.14-77.6.1
php5-mcrypt-debuginfo-5.5.14-77.6.1
php5-bcmath-debuginfo-5.5.14-77.6.1
php5-bz2-5.5.14-77.6.1
php5-json-debuginfo-5.5.14-77.6.1
php5-tokenizer-5.5.14-77.6.1
php5-calendar-5.5.14-77.6.1
apache2-mod_php5-debuginfo-5.5.14-77.6.1
php5-fpm-5.5.14-77.6.1
php5-sqlite-5.5.14-77.6.1
php5-snmp-debuginfo-5.5.14-77.6.1
php5-gettext-5.5.14-77.6.1
php5-gettext-debuginfo-5.5.14-77.6.1
php5-opcode-5.5.14-77.6.1
php5-pgsql-debuginfo-5.5.14-77.6.1
php5-snmp-5.5.14-77.6.1
php5-pcntl-5.5.14-77.6.1
php5-ldap-5.5.14-77.6.1
apache2-mod_php5-5.5.14-77.6.1
php5-xmlrpc-5.5.14-77.6.1
php5-exif-debuginfo-5.5.14-77.6.1
php5-sysvshm-5.5.14-77.6.1
php5-zip-5.5.14-77.6.1
php5-suhosin-debuginfo-5.5.14-77.6.1
php5-mbstring-5.5.14-77.6.1
php5-pdo-5.5.14-77.6.1
php5-sockets-debuginfo-5.5.14-77.6.1
php5-sysvsem-debuginfo-5.5.14-77.6.1
php5-gd-debuginfo-5.5.14-77.6.1
php5-debuginfo-5.5.14-77.6.1
php5-ctype-debuginfo-5.5.14-77.6.1
php5-intl-debuginfo-5.5.14-77.6.1
php5-zip-debuginfo-5.5.14-77.6.1
php5-tokenizer-debuginfo-5.5.14-77.6.1
php5-zlib-debuginfo-5.5.14-77.6.1
php5-calendar-debuginfo-5.5.14-77.6.1
php5-phar-debuginfo-5.5.14-77.6.1
php5-mcrypt-5.5.14-77.6.1
php5-mssql-debuginfo-5.5.14-77.6.1
php5-sysvmsg-debuginfo-5.5.14-77.6.1
php5-json-5.5.14-77.6.1
php5-bcmath-5.5.14-77.6.1
php5-ldap-5.5.14-77.6.1
php5-mysql-5.5.14-77.6.1
php5-ldap-5.5.14-77.6.1
php5-gd-5.5.14-77.6.1
php5-mbstring-debuginfo-5.5.14-77.6.1
php5-pgsql-5.5.14-77.6.1
php5-bz2-debuginfo-5.5.14-77.6.1
php5-dba-debuginfo-5.5.14-77.6.1
php5-intl-5.5.14-77.6.1
php5-devel-5.5.14-77.6.1

php5-xmlwriter-5.5.14-77.6.1
php5-tidy-debuginfo-5.5.14-77.6.1
php5-phar-5.5.14-77.6.1
php5-odbc-debuginfo-5.5.14-77.6.1
php5-curl-5.5.14-77.6.1
php5-ctype-5.5.14-77.6.1
php5-openssl-5.5.14-77.6.1
php5-wddx-5.5.14-77.6.1
php5-sysvsem-5.5.14-77.6.1
php5-ftp-debuginfo-5.5.14-77.6.1
php5-fastcgi-5.5.14-77.6.1
php5-sqlite-debuginfo-5.5.14-77.6.1
php5-gmp-debuginfo-5.5.14-77.6.1
php5-firebird-debuginfo-5.5.14-77.6.1
php5-gmp-5.5.14-77.6.1
php5-dba-5.5.14-77.6.1
php5-xsl-5.5.14-77.6.1
php5-firebird-5.5.14-77.6.1
php5-fpm-debuginfo-5.5.14-77.6.1
php5-sockets-5.5.14-77.6.1
php5-readline-debuginfo-5.5.14-77.6.1
php5-sysvmsg-5.5.14-77.6.1
php5-soap-debuginfo-5.5.14-77.6.1
php5-pcntl-debuginfo-5.5.14-77.6.1
php5-fileinfo-debuginfo-5.5.14-77.6.1
php5-5.5.14-77.6.1
php5-ldap-5.5.14-77.6.1
php5-exif-5.5.14-77.6.1
php5-xmlreader-5.5.14-77.6.1
php5-mysql-debuginfo-5.5.14-77.6.1
php5-pdo-debuginfo-5.5.14-77.6.1
php5-ldap-debuginfo-5.5.14-77.6.1
php5-dom-debuginfo-5.5.14-77.6.1
php5-posix-5.5.14-77.6.1
php5-shmop-debuginfo-5.5.14-77.6.1
php5-opcache-debuginfo-5.5.14-77.6.1
php5-dom-5.5.14-77.6.1
php5-tidy-5.5.14-77.6.1
php5-iconv-5.5.14-77.6.1
php5-zlib-5.5.14-77.6.1
php5-openssl-debuginfo-5.5.14-77.6.1
php5-soap-5.5.14-77.6.1
php5-posix-debuginfo-5.5.14-77.6.1
php5-odbc-5.5.14-77.6.1
php5-enchanted-5.5.14-77.6.1
php5-ispell-5.5.14-77.6.1
php5-sysvshm-debuginfo-5.5.14-77.6.1
php5-debugsource-5.5.14-77.6.1
php5-xsl-debuginfo-5.5.14-77.6.1
php5-iconv-debuginfo-5.5.14-77.6.1
php5-xmlreader-debuginfo-5.5.14-77.6.1
php5-curl-debuginfo-5.5.14-77.6.1
php5-ftp-5.5.14-77.6.1
php5-imap-debuginfo-5.5.14-77.6.1
php5-suhosin-5.5.14-77.6.1
php5-wddx-debuginfo-5.5.14-77.6.1

noarch

php5-pear-5.5.14-77.6.1

x86_64
php5-shmop-5.5.14-77.6.1
php5-xmlwriter-debuginfo-5.5.14-77.6.1
php5-fileinfo-5.5.14-77.6.1
php5-xmlrpc-debuginfo-5.5.14-77.6.1
php5-readline-5.5.14-77.6.1
php5-mssql-5.5.14-77.6.1
php5-fastcgi-debuginfo-5.5.14-77.6.1
php5-mcrypt-debuginfo-5.5.14-77.6.1
php5-bcmath-debuginfo-5.5.14-77.6.1
php5-bz2-5.5.14-77.6.1
php5-json-debuginfo-5.5.14-77.6.1
php5-tokenizer-5.5.14-77.6.1
php5-calendar-5.5.14-77.6.1
apache2-mod_php5-debuginfo-5.5.14-77.6.1
php5-fpm-5.5.14-77.6.1
php5-sqlite-5.5.14-77.6.1
php5-snmp-debuginfo-5.5.14-77.6.1
php5-gettext-5.5.14-77.6.1
php5-gettext-debuginfo-5.5.14-77.6.1
php5-opcode-5.5.14-77.6.1
php5-pgsql-debuginfo-5.5.14-77.6.1
php5-snmp-5.5.14-77.6.1
php5-pcntl-5.5.14-77.6.1
php5-ldap-5.5.14-77.6.1
apache2-mod_php5-5.5.14-77.6.1
php5-xmlrpc-5.5.14-77.6.1
php5-exif-debuginfo-5.5.14-77.6.1
php5-sysvshm-5.5.14-77.6.1
php5-zip-5.5.14-77.6.1
php5-suhosin-debuginfo-5.5.14-77.6.1
php5-mbstring-5.5.14-77.6.1
php5-pdo-5.5.14-77.6.1
php5-sockets-debuginfo-5.5.14-77.6.1
php5-sysvsem-debuginfo-5.5.14-77.6.1
php5-gd-debuginfo-5.5.14-77.6.1
php5-debuginfo-5.5.14-77.6.1
php5-ctype-debuginfo-5.5.14-77.6.1
php5-intl-debuginfo-5.5.14-77.6.1
php5-zip-debuginfo-5.5.14-77.6.1
php5-tokenizer-debuginfo-5.5.14-77.6.1
php5-zlib-debuginfo-5.5.14-77.6.1
php5-calendar-debuginfo-5.5.14-77.6.1
php5-phar-debuginfo-5.5.14-77.6.1
php5-mcrypt-5.5.14-77.6.1
php5-mssql-debuginfo-5.5.14-77.6.1
php5-sysvmsg-debuginfo-5.5.14-77.6.1
php5-json-5.5.14-77.6.1
php5-bcmath-5.5.14-77.6.1
php5-ldap-5.5.14-77.6.1
php5-mysql-5.5.14-77.6.1
php5-ldap-5.5.14-77.6.1
php5-gd-5.5.14-77.6.1
php5-mbstring-debuginfo-5.5.14-77.6.1
php5-pgsql-5.5.14-77.6.1
php5-bz2-debuginfo-5.5.14-77.6.1
php5-dba-debuginfo-5.5.14-77.6.1
php5-intl-5.5.14-77.6.1
php5-devel-5.5.14-77.6.1
php5-xmlwriter-5.5.14-77.6.1

php5-tidy-debuginfo-5.5.14-77.6.1
php5-phar-5.5.14-77.6.1
php5-odbc-debuginfo-5.5.14-77.6.1
php5-curl-5.5.14-77.6.1
php5-ctype-5.5.14-77.6.1
php5-openssl-5.5.14-77.6.1
php5-wddx-5.5.14-77.6.1
php5-sysvsem-5.5.14-77.6.1
php5-ftp-debuginfo-5.5.14-77.6.1
php5-fastcgi-5.5.14-77.6.1
php5-sqlite-debuginfo-5.5.14-77.6.1
php5-gmp-debuginfo-5.5.14-77.6.1
php5-firebird-debuginfo-5.5.14-77.6.1
php5-gmp-5.5.14-77.6.1
php5-dba-5.5.14-77.6.1
php5-xsl-5.5.14-77.6.1
php5-firebird-5.5.14-77.6.1
php5-fpm-debuginfo-5.5.14-77.6.1
php5-sockets-5.5.14-77.6.1
php5-readline-debuginfo-5.5.14-77.6.1
php5-sysvmsg-5.5.14-77.6.1
php5-soap-debuginfo-5.5.14-77.6.1
php5-pcntl-debuginfo-5.5.14-77.6.1
php5-fileinfo-debuginfo-5.5.14-77.6.1
php5-5.5.14-77.6.1
php5-ldap-5.5.14-77.6.1
php5-exif-5.5.14-77.6.1
php5-xmlreader-5.5.14-77.6.1
php5-mysql-debuginfo-5.5.14-77.6.1
php5-pdo-debuginfo-5.5.14-77.6.1
php5-ldap-debuginfo-5.5.14-77.6.1
php5-dom-debuginfo-5.5.14-77.6.1
php5-posix-5.5.14-77.6.1
php5-shmop-debuginfo-5.5.14-77.6.1
php5-opcache-debuginfo-5.5.14-77.6.1
php5-dom-5.5.14-77.6.1
php5-tidy-5.5.14-77.6.1
php5-iconv-5.5.14-77.6.1
php5-zlib-5.5.14-77.6.1
php5-openssl-debuginfo-5.5.14-77.6.1
php5-soap-5.5.14-77.6.1
php5-posix-debuginfo-5.5.14-77.6.1
php5-odbc-5.5.14-77.6.1
php5-enchanted-5.5.14-77.6.1
php5-ispell-5.5.14-77.6.1
php5-sysvshm-debuginfo-5.5.14-77.6.1
php5-debugsource-5.5.14-77.6.1
php5-xsl-debuginfo-5.5.14-77.6.1
php5-iconv-debuginfo-5.5.14-77.6.1

145644 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0386-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7444, CVE-2016-8610, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

Description

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

openSUSE-SU-2017:0386-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00023.html>

SuSE Linux 42.1

x86_64

libgnutlsxx28-3.2.15-8.1
libgnutls28-32bit-3.2.15-8.1
libgnutlsxx-devel-3.2.15-8.1
libgnutls28-debuginfo-32bit-3.2.15-8.1
libgnutls-devel-3.2.15-8.1
libgnutls-openssl-devel-3.2.15-8.1
libgnutls28-3.2.15-8.1
libgnutls-openssl27-3.2.15-8.1
libgnutlsxx28-debuginfo-3.2.15-8.1
gnutls-debugsource-3.2.15-8.1
libgnutls-openssl27-debuginfo-3.2.15-8.1
libgnutls-devel-32bit-3.2.15-8.1
gnutls-3.2.15-8.1
libgnutls28-debuginfo-3.2.15-8.1
gnutls-debuginfo-3.2.15-8.1

i586

libgnutlsxx28-debuginfo-3.2.15-8.1
libgnutls28-debuginfo-3.2.15-8.1
libgnutls28-3.2.15-8.1
gnutls-debugsource-3.2.15-8.1
gnutls-debuginfo-3.2.15-8.1
libgnutlsxx28-3.2.15-8.1
libgnutls-openssl27-3.2.15-8.1
libgnutls-openssl-devel-3.2.15-8.1
libgnutls-devel-3.2.15-8.1
libgnutls-openssl27-debuginfo-3.2.15-8.1
gnutls-3.2.15-8.1
libgnutlsxx-devel-3.2.15-8.1

SuSE Linux 42.2

x86_64

gnutls-debugsource-3.2.15-9.1
libgnutls28-32bit-3.2.15-9.1
libgnutls28-debuginfo-32bit-3.2.15-9.1
libgnutls-openssl27-3.2.15-9.1
libgnutlsxx-devel-3.2.15-9.1
libgnutls28-3.2.15-9.1
libgnutls28-debuginfo-3.2.15-9.1
libgnutls-openssl-devel-3.2.15-9.1
libgnutls-devel-32bit-3.2.15-9.1
libgnutls-openssl27-debuginfo-3.2.15-9.1
libgnutls-devel-3.2.15-9.1
libgnutlsxx28-3.2.15-9.1
gnutls-3.2.15-9.1
libgnutlsxx28-debuginfo-3.2.15-9.1
gnutls-debuginfo-3.2.15-9.1

i586

libgnutls-openssl27-3.2.15-9.1
libgnutls-openssl-devel-3.2.15-9.1

libgnutls-devel-3.2.15-9.1
libgnutlsxx-devel-3.2.15-9.1
gnutls-debuginfo-3.2.15-9.1
libgnutls28-3.2.15-9.1
gnutls-3.2.15-9.1
libgnutls-openssl27-debuginfo-3.2.15-9.1
libgnutlsxx28-debuginfo-3.2.15-9.1
libgnutls28-debuginfo-3.2.15-9.1
gnutls-debugsource-3.2.15-9.1
libgnutlsxx28-3.2.15-9.1

145645 - SuSE Linux 42.2 openSUSE-SU-2017:1800-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6294, CVE-2017-6441, CVE-2017-9224, CVE-2017-9226, CVE-2017-9227

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1800-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00029.html>

SuSE Linux 42.2

i586

php7-ftp-7.0.7-14.6.1
php7-sysvmsg-7.0.7-14.6.1
php7-openssl-debuginfo-7.0.7-14.6.1
php7-tokenizer-debuginfo-7.0.7-14.6.1
php7-imap-debuginfo-7.0.7-14.6.1
php7-gd-debuginfo-7.0.7-14.6.1
php7-7.0.7-14.6.1
php7-pspell-debuginfo-7.0.7-14.6.1
php7-snmp-debuginfo-7.0.7-14.6.1
php7-shmop-7.0.7-14.6.1
php7-bcmath-7.0.7-14.6.1
php7-posix-7.0.7-14.6.1
php7-ctype-7.0.7-14.6.1
php7-gettext-7.0.7-14.6.1
php7-ctype-debuginfo-7.0.7-14.6.1
php7-tidy-debuginfo-7.0.7-14.6.1
php7-mysql-7.0.7-14.6.1
php7-sysvshm-7.0.7-14.6.1
php7-xmlrpc-7.0.7-14.6.1
php7-phar-7.0.7-14.6.1
php7-sockets-7.0.7-14.6.1
php7-exif-debuginfo-7.0.7-14.6.1
php7-zip-debuginfo-7.0.7-14.6.1
php7-bcmath-debuginfo-7.0.7-14.6.1
php7-fileinfo-7.0.7-14.6.1
php7-ldap-debuginfo-7.0.7-14.6.1
php7-ldap-7.0.7-14.6.1
php7-json-debuginfo-7.0.7-14.6.1
php7-firebird-7.0.7-14.6.1

php7-devel-7.0.7-14.6.1
php7-sockets-debuginfo-7.0.7-14.6.1
php7-odbc-debuginfo-7.0.7-14.6.1
php7-dom-7.0.7-14.6.1
php7-debugsource-7.0.7-14.6.1
php7-calendar-debuginfo-7.0.7-14.6.1
php7-fpm-7.0.7-14.6.1
php7-sysvsem-7.0.7-14.6.1
php7-xsl-7.0.7-14.6.1
php7-readline-7.0.7-14.6.1
php7-mcrypt-debuginfo-7.0.7-14.6.1
php7-mcrypt-7.0.7-14.6.1
php7-bz2-debuginfo-7.0.7-14.6.1
php7-odbc-7.0.7-14.6.1
php7-opcache-debuginfo-7.0.7-14.6.1
php7-wddx-7.0.7-14.6.1
php7-firebird-debuginfo-7.0.7-14.6.1
php7-json-7.0.7-14.6.1
php7-xmlwriter-debuginfo-7.0.7-14.6.1
php7-tidy-7.0.7-14.6.1
php7-pgsql-debuginfo-7.0.7-14.6.1
php7-enchanted-7.0.7-14.6.1
php7-mbstring-7.0.7-14.6.1
php7-calendar-7.0.7-14.6.1
php7-dom-debuginfo-7.0.7-14.6.1
php7-sqlite-7.0.7-14.6.1
php7-opcache-7.0.7-14.6.1
php7-xmlrpc-debuginfo-7.0.7-14.6.1
php7-sysvmsg-debuginfo-7.0.7-14.6.1
php7-sysvsem-debuginfo-7.0.7-14.6.1
php7-phar-debuginfo-7.0.7-14.6.1
php7-dba-debuginfo-7.0.7-14.6.1
php7-posix-debuginfo-7.0.7-14.6.1
php7-fastcgi-debuginfo-7.0.7-14.6.1
apache2-mod_php7-debuginfo-7.0.7-14.6.1
php7-pdo-debuginfo-7.0.7-14.6.1
php7-snmp-7.0.7-14.6.1
php7-bz2-7.0.7-14.6.1
php7-pcntl-debuginfo-7.0.7-14.6.1
php7-enchanted-debuginfo-7.0.7-14.6.1
php7-fpm-debuginfo-7.0.7-14.6.1
php7-zlib-7.0.7-14.6.1
php7-intl-debuginfo-7.0.7-14.6.1
apache2-mod_php7-7.0.7-14.6.1
php7-zip-7.0.7-14.6.1
php7-soap-debuginfo-7.0.7-14.6.1
php7-openssl-7.0.7-14.6.1
php7-pdo-7.0.7-14.6.1
php7-fileinfo-debuginfo-7.0.7-14.6.1
php7-soap-7.0.7-14.6.1
php7-gd-7.0.7-14.6.1
php7-gettext-debuginfo-7.0.7-14.6.1
php7-xsl-debuginfo-7.0.7-14.6.1
php7-readline-debuginfo-7.0.7-14.6.1
php7-xmlreader-7.0.7-14.6.1
php7-gmp-7.0.7-14.6.1
php7-dba-7.0.7-14.6.1
php7-sysvshm-debuginfo-7.0.7-14.6.1
php7-curl-7.0.7-14.6.1
php7-iconv-7.0.7-14.6.1

php7-fastcgi-7.0.7-14.6.1
php7-tokenizer-7.0.7-14.6.1
php7-debuginfo-7.0.7-14.6.1
php7-wddx-debuginfo-7.0.7-14.6.1
php7-zlib-debuginfo-7.0.7-14.6.1
php7-mysql-debuginfo-7.0.7-14.6.1
php7-mbstring-debuginfo-7.0.7-14.6.1
php7-pspell-7.0.7-14.6.1
php7-imap-7.0.7-14.6.1
php7-pcntl-7.0.7-14.6.1
php7-shmop-debuginfo-7.0.7-14.6.1
php7-iconv-debuginfo-7.0.7-14.6.1
php7-ftp-debuginfo-7.0.7-14.6.1
php7-sqlite-debuginfo-7.0.7-14.6.1
php7-gmp-debuginfo-7.0.7-14.6.1
php7-xmlwriter-7.0.7-14.6.1
php7-intl-7.0.7-14.6.1
php7-curl-debuginfo-7.0.7-14.6.1
php7-pgsql-7.0.7-14.6.1
php7-exif-7.0.7-14.6.1
php7-xmlreader-debuginfo-7.0.7-14.6.1

noarch

php7-pear-7.0.7-14.6.1
php7-pear-Archive_Tar-7.0.7-14.6.1

x86_64

php7-ftp-7.0.7-14.6.1
php7-sysvmsg-7.0.7-14.6.1
php7-openssl-debuginfo-7.0.7-14.6.1
php7-tokenizer-debuginfo-7.0.7-14.6.1
php7-imap-debuginfo-7.0.7-14.6.1
php7-gd-debuginfo-7.0.7-14.6.1
php7-7.0.7-14.6.1
php7-pspell-debuginfo-7.0.7-14.6.1
php7-snmp-debuginfo-7.0.7-14.6.1
php7-shmop-7.0.7-14.6.1
php7-bcmath-7.0.7-14.6.1
php7-posix-7.0.7-14.6.1
php7-ctype-7.0.7-14.6.1
php7-gettext-7.0.7-14.6.1
php7-ctype-debuginfo-7.0.7-14.6.1
php7-tidy-debuginfo-7.0.7-14.6.1
php7-mysql-7.0.7-14.6.1
php7-sysvshm-7.0.7-14.6.1
php7-xmlrpc-7.0.7-14.6.1
php7-phar-7.0.7-14.6.1
php7-sockets-7.0.7-14.6.1
php7-exif-debuginfo-7.0.7-14.6.1
php7-zip-debuginfo-7.0.7-14.6.1
php7-bcmath-debuginfo-7.0.7-14.6.1
php7-fileinfo-7.0.7-14.6.1
php7-ldap-debuginfo-7.0.7-14.6.1
php7-ldap-7.0.7-14.6.1
php7-json-debuginfo-7.0.7-14.6.1
php7-firebird-7.0.7-14.6.1
php7-devel-7.0.7-14.6.1
php7-sockets-debuginfo-7.0.7-14.6.1
php7-odbc-debuginfo-7.0.7-14.6.1
php7-dom-7.0.7-14.6.1

php7-debugsource-7.0.7-14.6.1
php7-calendar-debuginfo-7.0.7-14.6.1
php7-fpm-7.0.7-14.6.1
php7-sysvsem-7.0.7-14.6.1
php7-xsl-7.0.7-14.6.1
php7-readline-7.0.7-14.6.1
php7-mcrypt-debuginfo-7.0.7-14.6.1
php7-mcrypt-7.0.7-14.6.1
php7-bz2-debuginfo-7.0.7-14.6.1
php7-odbc-7.0.7-14.6.1
php7-opcache-debuginfo-7.0.7-14.6.1
php7-wddx-7.0.7-14.6.1
php7-firebird-debuginfo-7.0.7-14.6.1
php7-json-7.0.7-14.6.1
php7-xmlwriter-debuginfo-7.0.7-14.6.1
php7-tidy-7.0.7-14.6.1
php7-pgsql-debuginfo-7.0.7-14.6.1
php7-enchanted-7.0.7-14.6.1
php7-mbstring-7.0.7-14.6.1
php7-calendar-7.0.7-14.6.1
php7-dom-debuginfo-7.0.7-14.6.1
php7-sqlite-7.0.7-14.6.1
php7-opcache-7.0.7-14.6.1
php7-xmlrpc-debuginfo-7.0.7-14.6.1
php7-sysvmsg-debuginfo-7.0.7-14.6.1
php7-sysvsem-debuginfo-7.0.7-14.6.1
php7-phar-debuginfo-7.0.7-14.6.1
php7-dba-debuginfo-7.0.7-14.6.1
php7-posix-debuginfo-7.0.7-14.6.1
php7-fastcgi-debuginfo-7.0.7-14.6.1
apache2-mod_php7-debuginfo-7.0.7-14.6.1
php7-pdo-debuginfo-7.0.7-14.6.1
php7-snmp-7.0.7-14.6.1
php7-bz2-7.0.7-14.6.1
php7-pcntl-debuginfo-7.0.7-14.6.1
php7-enchanted-7.0.7-14.6.1
php7-fpm-debuginfo-7.0.7-14.6.1
php7-zlib-7.0.7-14.6.1
php7-intl-debuginfo-7.0.7-14.6.1
apache2-mod_php7-7.0.7-14.6.1
php7-zip-7.0.7-14.6.1
php7-soap-debuginfo-7.0.7-14.6.1
php7-openssl-7.0.7-14.6.1
php7-pdo-7.0.7-14.6.1
php7-fileinfo-debuginfo-7.0.7-14.6.1
php7-soap-7.0.7-14.6.1
php7-gd-7.0.7-14.6.1
php7-gettext-debuginfo-7.0.7-14.6.1
php7-xsl-debuginfo-7.0.7-14.6.1
php7-readline-debuginfo-7.0.7-14.6.1
php7-xmlreader-7.0.7-14.6.1
php7-gmp-7.0.7-14.6.1
php7-dba-7.0.7-14.6.1
php7-sysvshm-debuginfo-7.0.7-14.6.1
php7-curl-7.0.7-14.6.1
php7-iconv-7.0.7-14.6.1
php7-fastcgi-7.0.7-14.6.1
php7-tokenizer-7.0.7-14.6.1
php7-debuginfo-7.0.7-14.6.1
php7-wddx-debuginfo-7.0.7-14.6.1

php7-zlib-debuginfo-7.0.7-14.6.1
php7-mysql-debuginfo-7.0.7-14.6.1
php7-mbstring-debuginfo-7.0.7-14.6.1
php7-pspell-7.0.7-14.6.1
php7-imap-7.0.7-14.6.1
php7-pcntl-7.0.7-14.6.1
php7-shmop-debuginfo-7.0.7-14.6.1
php7-iconv-debuginfo-7.0.7-14.6.1
php7-ftp-debuginfo-7.0.7-14.6.1
php7-sqlite-debuginfo-7.0.7-14.6.1
php7-gmp-debuginfo-7.0.7-14.6.1
php7-xmlwriter-7.0.7-14.6.1
php7-intl-7.0.7-14.6.1
php7-curl-debuginfo-7.0.7-14.6.1
php7-pgsql-7.0.7-14.6.1
php7-exif-7.0.7-14.6.1
php7-xmlreader-debuginfo-7.0.7-14.6.1

145646 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0221-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7068

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0221-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00122.html>

SuSE Linux 42.1

x86_64

pdns-recursor-debugsource-3.7.3-6.1

pdns-recursor-3.7.3-6.1

pdns-recursor-debuginfo-3.7.3-6.1

i586

pdns-recursor-debugsource-3.7.3-6.1

pdns-recursor-3.7.3-6.1

pdns-recursor-debuginfo-3.7.3-6.1

SuSE Linux 42.2

x86_64

pdns-recursor-debugsource-3.7.3-7.1

pdns-recursor-debuginfo-3.7.3-7.1

pdns-recursor-3.7.3-7.1

i586

pdns-recursor-debugsource-3.7.3-7.1

pdns-recursor-debuginfo-3.7.3-7.1

pdns-recursor-3.7.3-7.1

145647 - SuSE Linux 42.2 openSUSE-SU-2017:0830-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0830-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00094.html>

SuSE Linux 42.2

x86_64

xtrabackup-test-2.3.7-5.3.1

xtrabackup-2.3.7-5.3.1

xtrabackup-debuginfo-2.3.7-5.3.1

xtrabackup-debugsource-2.3.7-5.3.1

145650 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0409-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7056

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0409-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00038.html>

SuSE Linux 42.1

i586

libressl-2.3.0-10.1

libressl-devel-2.3.0-10.1

libssl37-debuginfo-2.3.0-10.1

libressl-debugsource-2.3.0-10.1

libcrypto36-2.3.0-10.1

libtls9-2.3.0-10.1

libtls9-debuginfo-2.3.0-10.1

libcrypto36-debuginfo-2.3.0-10.1

libressl-debuginfo-2.3.0-10.1

libssl37-2.3.0-10.1

noarch

libressl-devel-doc-2.3.0-10.1

x86_64

libssl37-debuginfo-32bit-2.3.0-10.1

libssl37-2.3.0-10.1

libcrypto36-debuginfo-32bit-2.3.0-10.1
libressl-devel-2.3.0-10.1
libressl-devel-32bit-2.3.0-10.1
libtls9-32bit-2.3.0-10.1
libtls9-2.3.0-10.1
libressl-2.3.0-10.1
libcrypto36-debuginfo-2.3.0-10.1
libssl37-debuginfo-2.3.0-10.1
libressl-debugsource-2.3.0-10.1
libtls9-debuginfo-32bit-2.3.0-10.1
libtls9-debuginfo-2.3.0-10.1
libcrypto36-2.3.0-10.1
libcrypto36-32bit-2.3.0-10.1
libressl-debuginfo-2.3.0-10.1
libssl37-32bit-2.3.0-10.1

SuSE Linux 42.2

i586

libressl-devel-2.3.4-3.1
libcrypto37-2.3.4-3.1
libressl-debugsource-2.3.4-3.1
libtls10-2.3.4-3.1
libtls10-debuginfo-2.3.4-3.1
libssl38-2.3.4-3.1
libressl-2.3.4-3.1
libressl-debuginfo-2.3.4-3.1
libssl38-debuginfo-2.3.4-3.1
libcrypto37-debuginfo-2.3.4-3.1

noarch

libressl-devel-doc-2.3.4-3.1

x86_64

libtls10-32bit-2.3.4-3.1
libressl-devel-2.3.4-3.1
libressl-2.3.4-3.1
libtls10-debuginfo-32bit-2.3.4-3.1
libcrypto37-2.3.4-3.1
libcrypto37-debuginfo-32bit-2.3.4-3.1
libcrypto37-debuginfo-2.3.4-3.1
libssl38-debuginfo-2.3.4-3.1
libressl-debugsource-2.3.4-3.1
libcrypto37-32bit-2.3.4-3.1
libssl38-2.3.4-3.1
libtls10-debuginfo-2.3.4-3.1
libressl-debuginfo-2.3.4-3.1
libressl-devel-32bit-2.3.4-3.1
libtls10-2.3.4-3.1
libssl38-debuginfo-32bit-2.3.4-3.1
libssl38-32bit-2.3.4-3.1

145651 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0678-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:0678-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00036.html>

SuSE Linux 42.1
x86_64
pax-utils-1.2.2-5.1
pax-utils-debuginfo-1.2.2-5.1
pax-utils-debugsource-1.2.2-5.1

i586
pax-utils-1.2.2-5.1
pax-utils-debuginfo-1.2.2-5.1
pax-utils-debugsource-1.2.2-5.1

SuSE Linux 42.2
x86_64
pax-utils-1.2.2-6.1
pax-utils-debugsource-1.2.2-6.1
pax-utils-debuginfo-1.2.2-6.1

i586
pax-utils-1.2.2-6.1
pax-utils-debugsource-1.2.2-6.1
pax-utils-debuginfo-1.2.2-6.1

145653 - SuSE Linux 42.2 openSUSE-SU-2017:1697-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000368

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1697-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00103.html>

SuSE Linux 42.2
x86_64
sudo-devel-1.8.10p3-9.6.1
sudo-debugsource-1.8.10p3-9.6.1
sudo-1.8.10p3-9.6.1
sudo-test-1.8.10p3-9.6.1
sudo-debuginfo-1.8.10p3-9.6.1

i586
sudo-devel-1.8.10p3-9.6.1
sudo-debugsource-1.8.10p3-9.6.1

sudo-1.8.10p3-9.6.1
sudo-test-1.8.10p3-9.6.1
sudo-debuginfo-1.8.10p3-9.6.1

145654 - SuSE Linux 42.2 openSUSE-SU-2017:1802-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2625

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1802-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00031.html>

SuSE Linux 42.2

x86_64

libXdmpc-devel-1.1.2-3.3.1
libXdmpc6-debuginfo-1.1.2-3.3.1
libXdmpc-debugsource-1.1.2-3.3.1
libXdmpc6-32bit-1.1.2-3.3.1
libXdmpc-devel-32bit-1.1.2-3.3.1
libXdmpc6-debuginfo-32bit-1.1.2-3.3.1
libXdmpc6-1.1.2-3.3.1

i586

libXdmpc-debugsource-1.1.2-3.3.1
libXdmpc6-debuginfo-1.1.2-3.3.1
libXdmpc6-1.1.2-3.3.1
libXdmpc-devel-1.1.2-3.3.1

145655 - SuSE Linux 42.2 openSUSE-SU-2017:0892-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2640

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0892-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00115.html>

SuSE Linux 42.2

x86_64

libpurple-debuginfo-2.10.11-8.3.1
finch-2.10.11-8.3.1

libpurple-meanwhile-debuginfo-2.10.11-8.3.1
finch-devel-2.10.11-8.3.1
pidgin-debugsource-2.10.11-8.3.1
libpurple-tcl-debuginfo-2.10.11-8.3.1
finch-debuginfo-2.10.11-8.3.1
pidgin-devel-2.10.11-8.3.1
pidgin-debuginfo-2.10.11-8.3.1
pidgin-2.10.11-8.3.1
libpurple-devel-2.10.11-8.3.1
libpurple-meanwhile-2.10.11-8.3.1
libpurple-2.10.11-8.3.1
libpurple-tcl-2.10.11-8.3.1

noarch
libpurple-branding-upstream-2.10.11-8.3.1
libpurple-lang-2.10.11-8.3.1

145656 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0357-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0357-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00003.html>

SuSE Linux 42.1

x86_64

MozillaThunderbird-devel-45.7.0-34.1
MozillaThunderbird-debuginfo-45.7.0-34.1
MozillaThunderbird-translations-other-45.7.0-34.1
MozillaThunderbird-translations-common-45.7.0-34.1
MozillaThunderbird-debugsource-45.7.0-34.1
MozillaThunderbird-45.7.0-34.1
MozillaThunderbird-buildsymbols-45.7.0-34.1

i586

MozillaThunderbird-devel-45.7.0-34.1
MozillaThunderbird-debuginfo-45.7.0-34.1
MozillaThunderbird-translations-other-45.7.0-34.1
MozillaThunderbird-translations-common-45.7.0-34.1
MozillaThunderbird-debugsource-45.7.0-34.1
MozillaThunderbird-45.7.0-34.1
MozillaThunderbird-buildsymbols-45.7.0-34.1

SuSE Linux 42.2

x86_64

MozillaThunderbird-devel-45.7.0-34.1
MozillaThunderbird-debuginfo-45.7.0-34.1
MozillaThunderbird-translations-other-45.7.0-34.1

MozillaThunderbird-translations-common-45.7.0-34.1
MozillaThunderbird-debugsource-45.7.0-34.1
MozillaThunderbird-45.7.0-34.1
MozillaThunderbird-buildsymbols-45.7.0-34.1

145659 - SuSE Linux 42.2 openSUSE-SU-2017:0399-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10048, CVE-2016-10050, CVE-2016-10051, CVE-2016-10052, CVE-2016-10068, CVE-2016-10070, CVE-2016-10146, CVE-2017-5511

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0399-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00031.html>

SuSE Linux 42.2

x86_64

GraphicsMagick-debugsource-1.3.25-9.1
libGraphicsMagick++-Q16-12-1.3.25-9.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-9.1
GraphicsMagick-devel-1.3.25-9.1
libGraphicsMagick++-devel-1.3.25-9.1
GraphicsMagick-debuginfo-1.3.25-9.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-9.1
libGraphicsMagickWand-Q16-2-1.3.25-9.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-9.1
GraphicsMagick-1.3.25-9.1
perl-GraphicsMagick-debuginfo-1.3.25-9.1
perl-GraphicsMagick-1.3.25-9.1
libGraphicsMagick3-config-1.3.25-9.1
libGraphicsMagick-Q16-3-1.3.25-9.1

i586

GraphicsMagick-debugsource-1.3.25-9.1
libGraphicsMagick++-Q16-12-1.3.25-9.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-9.1
GraphicsMagick-devel-1.3.25-9.1
libGraphicsMagick++-devel-1.3.25-9.1
GraphicsMagick-debuginfo-1.3.25-9.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-9.1
libGraphicsMagickWand-Q16-2-1.3.25-9.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-9.1
GraphicsMagick-1.3.25-9.1
perl-GraphicsMagick-debuginfo-1.3.25-9.1
perl-GraphicsMagick-1.3.25-9.1
libGraphicsMagick3-config-1.3.25-9.1
libGraphicsMagick-Q16-3-1.3.25-9.1

145661 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0587-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10046, CVE-2016-10048, CVE-2016-10049, CVE-2016-10050, CVE-2016-10051, CVE-2016-10052, CVE-2016-10059, CVE-2016-10060, CVE-2016-10061, CVE-2016-10062, CVE-2016-10063, CVE-2016-10064, CVE-2016-10065, CVE-2016-10068, CVE-2016-10069, CVE-2016-10070, CVE-2016-10071, CVE-2016-10144, CVE-2016-10145, CVE-2016-10146, CVE-2017-5506, CVE-2017-5507, CVE-2017-5508, CVE-2017-5510, CVE-2017-5511

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0587-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00000.html>

SuSE Linux 42.1

i586

perl-PerlMagick-6.8.8.1-30.1
perl-PerlMagick-debuginfo-6.8.8.1-30.1
ImageMagick-debugsource-6.8.8.1-30.1
ImageMagick-debuginfo-6.8.8.1-30.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.1
libMagick++-devel-6.8.8.1-30.1
ImageMagick-devel-6.8.8.1-30.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.1
ImageMagick-extra-debuginfo-6.8.8.1-30.1
libMagickCore-6_Q16-1-6.8.8.1-30.1
ImageMagick-6.8.8.1-30.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.1
ImageMagick-extra-6.8.8.1-30.1
libMagickWand-6_Q16-1-6.8.8.1-30.1
libMagick++-6_Q16-3-6.8.8.1-30.1

noarch

ImageMagick-doc-6.8.8.1-30.1

x86_64

perl-PerlMagick-6.8.8.1-30.1
perl-PerlMagick-debuginfo-6.8.8.1-30.1
ImageMagick-debugsource-6.8.8.1-30.1
ImageMagick-debuginfo-6.8.8.1-30.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-30.1
libMagick++-devel-6.8.8.1-30.1
ImageMagick-devel-6.8.8.1-30.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-30.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.1
ImageMagick-extra-debuginfo-6.8.8.1-30.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-30.1
ImageMagick-devel-32bit-6.8.8.1-30.1
libMagick++-6_Q16-3-32bit-6.8.8.1-30.1
libMagickCore-6_Q16-1-6.8.8.1-30.1
ImageMagick-6.8.8.1-30.1
libMagick++-devel-32bit-6.8.8.1-30.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.1
ImageMagick-extra-6.8.8.1-30.1
libMagickWand-6_Q16-1-6.8.8.1-30.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-30.1

libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-30.1
libMagick++-6_Q16-3-6.8.8.1-30.1

SuSE Linux 42.2

i586

ImageMagick-devel-6.8.8.1-28.1
ImageMagick-debuginfo-6.8.8.1-28.1
libMagick++-devel-6.8.8.1-28.1
ImageMagick-6.8.8.1-28.1
ImageMagick-extra-6.8.8.1-28.1
libMagickCore-6_Q16-1-6.8.8.1-28.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-28.1
perl-PerlMagick-debuginfo-6.8.8.1-28.1
ImageMagick-debugsource-6.8.8.1-28.1
perl-PerlMagick-6.8.8.1-28.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-28.1
ImageMagick-extra-debuginfo-6.8.8.1-28.1
libMagickWand-6_Q16-1-6.8.8.1-28.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-28.1
libMagick++-6_Q16-3-6.8.8.1-28.1

noarch

ImageMagick-doc-6.8.8.1-28.1

x86_64

ImageMagick-devel-6.8.8.1-28.1
ImageMagick-debuginfo-6.8.8.1-28.1
libMagick++-devel-6.8.8.1-28.1
ImageMagick-devel-32bit-6.8.8.1-28.1
ImageMagick-6.8.8.1-28.1
libMagick++-6_Q16-3-32bit-6.8.8.1-28.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-28.1
ImageMagick-extra-6.8.8.1-28.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-28.1
libMagickCore-6_Q16-1-6.8.8.1-28.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-28.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-28.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-28.1
perl-PerlMagick-debuginfo-6.8.8.1-28.1
ImageMagick-debugsource-6.8.8.1-28.1
perl-PerlMagick-6.8.8.1-28.1
libMagick++-devel-32bit-6.8.8.1-28.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-28.1
ImageMagick-extra-debuginfo-6.8.8.1-28.1
libMagickWand-6_Q16-1-6.8.8.1-28.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-28.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-28.1
libMagick++-6_Q16-3-6.8.8.1-28.1

145662 - SuSE Linux 42.2 openSUSE-SU-2017:1807-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2669

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1807-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00036.html>

SuSE Linux 42.2

x86_64

dovecot22-fts-squat-debuginfo-2.2.30.2-5.4.1
dovecot22-backend-mysql-2.2.30.2-5.4.1
dovecot22-fts-squat-2.2.30.2-5.4.1
dovecot22-fts-lucene-debuginfo-2.2.30.2-5.4.1
dovecot22-fts-2.2.30.2-5.4.1
dovecot22-fts-solr-2.2.30.2-5.4.1
dovecot22-fts-solr-debuginfo-2.2.30.2-5.4.1
dovecot22-2.2.30.2-5.4.1
dovecot22-backend-mysql-debuginfo-2.2.30.2-5.4.1
dovecot22-backend-pgsql-debuginfo-2.2.30.2-5.4.1
dovecot22-backend-pgsql-2.2.30.2-5.4.1
dovecot22-devel-2.2.30.2-5.4.1
dovecot22-debugsource-2.2.30.2-5.4.1
dovecot22-backend-sqlite-debuginfo-2.2.30.2-5.4.1
dovecot22-fts-debuginfo-2.2.30.2-5.4.1
dovecot22-fts-lucene-2.2.30.2-5.4.1
dovecot22-backend-sqlite-2.2.30.2-5.4.1
dovecot22-debuginfo-2.2.30.2-5.4.1

i586

dovecot22-fts-squat-debuginfo-2.2.30.2-5.4.1
dovecot22-backend-mysql-2.2.30.2-5.4.1
dovecot22-fts-squat-2.2.30.2-5.4.1
dovecot22-fts-lucene-debuginfo-2.2.30.2-5.4.1
dovecot22-fts-2.2.30.2-5.4.1
dovecot22-fts-solr-2.2.30.2-5.4.1
dovecot22-fts-solr-debuginfo-2.2.30.2-5.4.1
dovecot22-2.2.30.2-5.4.1
dovecot22-backend-mysql-debuginfo-2.2.30.2-5.4.1
dovecot22-backend-pgsql-debuginfo-2.2.30.2-5.4.1
dovecot22-backend-pgsql-2.2.30.2-5.4.1
dovecot22-devel-2.2.30.2-5.4.1
dovecot22-debugsource-2.2.30.2-5.4.1
dovecot22-backend-sqlite-debuginfo-2.2.30.2-5.4.1
dovecot22-fts-debuginfo-2.2.30.2-5.4.1
dovecot22-fts-lucene-2.2.30.2-5.4.1
dovecot22-backend-sqlite-2.2.30.2-5.4.1
dovecot22-debuginfo-2.2.30.2-5.4.1

145665 - SuSE Linux 42.2 openSUSE-SU-2017:2169-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112, CVE-2017-8831

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2169-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00058.html>

SuSE Linux 42.2

x86_64

kernel-vanilla-debugsource-4.4.79-18.26.2

kernel-obs-build-4.4.79-18.26.2

kernel-obs-build-debugsource-4.4.79-18.26.2

kernel-default-debugsource-4.4.79-18.26.2

kernel-vanilla-debuginfo-4.4.79-18.26.2

kernel-debug-base-debuginfo-4.4.79-18.26.2

kernel-debug-4.4.79-18.26.2

kernel-vanilla-base-debuginfo-4.4.79-18.26.2

kernel-syms-4.4.79-18.26.1

kernel-default-4.4.79-18.26.2

kernel-debug-debugsource-4.4.79-18.26.2

kernel-debug-base-4.4.79-18.26.2

kernel-vanilla-base-4.4.79-18.26.2

kernel-debug-devel-4.4.79-18.26.2

kernel-obs-qa-4.4.79-18.26.1

kernel-debug-debuginfo-4.4.79-18.26.2

kernel-vanilla-4.4.79-18.26.2

kernel-default-base-debuginfo-4.4.79-18.26.2

kernel-default-devel-4.4.79-18.26.2

kernel-debug-devel-debuginfo-4.4.79-18.26.2

kernel-default-base-4.4.79-18.26.2

kernel-default-debuginfo-4.4.79-18.26.2

kernel-vanilla-devel-4.4.79-18.26.2

noarch

kernel-source-4.4.79-18.26.1

kernel-docs-pdf-4.4.79-18.26.3

kernel-docs-html-4.4.79-18.26.3

kernel-source-vanilla-4.4.79-18.26.1

kernel-macros-4.4.79-18.26.1

kernel-devel-4.4.79-18.26.1

kernel-docs-4.4.79-18.26.3

145668 - SuSE Linux 42.2 openSUSE-SU-2017:2360-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:2360-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00010.html>

SuSE Linux 42.2

noarch

145674 - SuSE Linux 42.2 openSUSE-SU-2017:0369-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10132, CVE-2016-10133, CVE-2016-10141

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0369-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00012.html>

SuSE Linux 42.2
x86_64
mupdf-devel-static-1.10a-6.3
mupdf-1.10a-6.3

i586
mupdf-devel-static-1.10a-6.3
mupdf-1.10a-6.3

145679 - SuSE SLED 12 SP3 SUSE-SU-2017:2327-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2327-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-September/003180.html>

SuSE SLED 12 SP3
x86_64
xen-libs-32bit-4.9.0_11-3.9.1
xen-libs-4.9.0_11-3.9.1
xen-4.9.0_11-3.9.1
xen-libs-debuginfo-4.9.0_11-3.9.1
xen-libs-debuginfo-32bit-4.9.0_11-3.9.1
xen-debugsource-4.9.0_11-3.9.1

145680 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0368-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0368-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00011.html>

SuSE Linux 42.1

noarch

clamav-database-201701300007-213.1

SuSE Linux 42.2

noarch

clamav-database-201701300007-34.1

145681 - SuSE Linux 42.1 openSUSE-SU-2017:0373-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10132, CVE-2016-10133, CVE-2016-10141

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0373-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00016.html>

SuSE Linux 42.1

x86_64

mupdf-1.10a-10.1

mupdf-devel-static-1.10a-10.1

i586

mupdf-1.10a-10.1

mupdf-devel-static-1.10a-10.1

145682 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:2320-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2320-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003178.html>

SuSE SLES 12 SP3
x86_64
git-core-debuginfo-2.12.3-27.5.1
git-debugsource-2.12.3-27.5.1
git-core-2.12.3-27.5.1

SuSE SLES 12 SP2
noarch
git-doc-2.12.3-27.5.1

x86_64
git-core-debuginfo-2.12.3-27.5.1
git-debugsource-2.12.3-27.5.1
git-core-2.12.3-27.5.1

145683 - SuSE Linux 42.3 openSUSE-SU-2017:2171-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112, CVE-2017-8831

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2171-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00059.html>

SuSE Linux 42.3
x86_64
kernel-default-debugsource-4.4.79-19.1
kernel-syms-4.4.79-19.1
kernel-default-devel-4.4.79-19.1
kernel-debug-base-4.4.79-19.1
kernel-debug-4.4.79-19.1
kernel-debug-devel-4.4.79-19.1
kernel-debug-devel-debuginfo-4.4.79-19.1
kernel-vanilla-4.4.79-19.1
kernel-vanilla-base-debuginfo-4.4.79-19.1
kernel-obs-build-debugsource-4.4.79-19.1
kernel-debug-debugsource-4.4.79-19.1
kernel-vanilla-base-4.4.79-19.1
kernel-vanilla-devel-4.4.79-19.1
kernel-vanilla-debugsource-4.4.79-19.1
kernel-vanilla-debuginfo-4.4.79-19.1
kernel-obs-qa-4.4.79-19.1
kernel-debug-base-debuginfo-4.4.79-19.1
kernel-default-base-4.4.79-19.1

kernel-obs-build-4.4.79-19.1
kernel-default-base-debuginfo-4.4.79-19.1
kernel-default-4.4.79-19.1
kernel-debug-debuginfo-4.4.79-19.1
kernel-default-debuginfo-4.4.79-19.1

noarch
kernel-source-4.4.79-19.1
kernel-docs-4.4.79-19.2
kernel-source-vanilla-4.4.79-19.1
kernel-docs-html-4.4.79-19.2
kernel-devel-4.4.79-19.1
kernel-docs-pdf-4.4.79-19.2
kernel-macros-4.4.79-19.1

145685 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2306-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2306-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00111.html>

SuSE Linux 42.2

i586
postgresql93-devel-9.3.18-5.12.1
postgresql93-libs-debugsource-9.3.18-5.12.1
postgresql93-devel-debuginfo-9.3.18-5.12.1

noarch
postgresql93-docs-9.3.18-5.12.1

x86_64
postgresql93-debugsource-9.3.18-5.12.1
postgresql93-server-9.3.18-5.12.1
postgresql93-devel-debuginfo-9.3.18-5.12.1
postgresql93-plpython-9.3.18-5.12.1
postgresql93-debuginfo-9.3.18-5.12.1
postgresql93-test-9.3.18-5.12.1
postgresql93-plpython-debuginfo-9.3.18-5.12.1
postgresql93-libs-debugsource-9.3.18-5.12.1
postgresql93-plperl-9.3.18-5.12.1
postgresql93-devel-9.3.18-5.12.1
postgresql93-pltcl-debuginfo-9.3.18-5.12.1
postgresql93-contrib-9.3.18-5.12.1
postgresql93-contrib-debuginfo-9.3.18-5.12.1
postgresql93-9.3.18-5.12.1
postgresql93-plperl-debuginfo-9.3.18-5.12.1
postgresql93-pltcl-9.3.18-5.12.1
postgresql93-server-debuginfo-9.3.18-5.12.1

SuSE Linux 42.3

i586

postgresql93-libs-debugsource-9.3.18-8.1

postgresql93-devel-9.3.18-8.1

postgresql93-devel-debuginfo-9.3.18-8.1

noarch

postgresql93-docs-9.3.18-8.1

x86_64

postgresql93-contrib-9.3.18-8.1

postgresql93-plperl-9.3.18-8.1

postgresql93-server-9.3.18-8.1

postgresql93-devel-debuginfo-9.3.18-8.1

postgresql93-debuginfo-9.3.18-8.1

postgresql93-9.3.18-8.1

postgresql93-test-9.3.18-8.1

postgresql93-plperl-debuginfo-9.3.18-8.1

postgresql93-debugsource-9.3.18-8.1

postgresql93-server-debuginfo-9.3.18-8.1

postgresql93-contrib-debuginfo-9.3.18-8.1

postgresql93-plpython-9.3.18-8.1

postgresql93-pltcl-debuginfo-9.3.18-8.1

postgresql93-pltcl-9.3.18-8.1

postgresql93-plpython-debuginfo-9.3.18-8.1

postgresql93-libs-debugsource-9.3.18-8.1

postgresql93-devel-9.3.18-8.1

145690 - SuSE Linux 42.1 openSUSE-SU-2017:0391-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10048, CVE-2016-10050, CVE-2016-10051, CVE-2016-10052, CVE-2016-10059, CVE-2016-10064, CVE-2016-10065, CVE-2016-10068, CVE-2016-10069, CVE-2016-10070, CVE-2016-10146, CVE-2017-5511

Description

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

openSUSE-SU-2017:0391-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00028.html>

SuSE Linux 42.1

x86_64

libGraphicsMagickWand-Q16-2-1.3.21-26.1

GraphicsMagick-debuginfo-1.3.21-26.1

perl-GraphicsMagick-debuginfo-1.3.21-26.1

libGraphicsMagick++-Q16-11-1.3.21-26.1

libGraphicsMagick++-Q16-11-debuginfo-1.3.21-26.1

GraphicsMagick-debugsource-1.3.21-26.1

libGraphicsMagickWand-Q16-2-debuginfo-1.3.21-26.1

perl-GraphicsMagick-1.3.21-26.1

libGraphicsMagick3-config-1.3.21-26.1

GraphicsMagick-devel-1.3.21-26.1

libGraphicsMagick-Q16-3-debuginfo-1.3.21-26.1

GraphicsMagick-1.3.21-26.1
libGraphicsMagick-Q16-3-1.3.21-26.1
libGraphicsMagick++-devel-1.3.21-26.1

i586

libGraphicsMagickWand-Q16-2-1.3.21-26.1
GraphicsMagick-debuginfo-1.3.21-26.1
perl-GraphicsMagick-debuginfo-1.3.21-26.1
libGraphicsMagick++-Q16-11-1.3.21-26.1
libGraphicsMagick++-Q16-11-debuginfo-1.3.21-26.1
GraphicsMagick-debugsource-1.3.21-26.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.21-26.1
perl-GraphicsMagick-1.3.21-26.1
libGraphicsMagick3-config-1.3.21-26.1
GraphicsMagick-devel-1.3.21-26.1
libGraphicsMagick-Q16-3-debuginfo-1.3.21-26.1
GraphicsMagick-1.3.21-26.1
libGraphicsMagick-Q16-3-1.3.21-26.1
libGraphicsMagick++-devel-1.3.21-26.1

145691 - SuSE Linux 42.1 openSUSE-SU-2017:0674-1 Update Is Not Installed

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

Risk Level: High

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

Description

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

openSUSE-SU-2017:0674-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00032.html>

SuSE Linux 42.1

x86_64

openssh-fips-6.6p1-17.1
openssh-cavs-debuginfo-6.6p1-17.1
openssh-askpass-gnome-debuginfo-6.6p1-17.1
openssh-helpers-6.6p1-17.1
openssh-debugsource-6.6p1-17.1
openssh-helpers-debuginfo-6.6p1-17.1
openssh-askpass-gnome-6.6p1-17.1
openssh-cavs-6.6p1-17.1
openssh-6.6p1-17.1
openssh-debuginfo-6.6p1-17.1

i586

openssh-fips-6.6p1-17.1
openssh-cavs-debuginfo-6.6p1-17.1
openssh-askpass-gnome-debuginfo-6.6p1-17.1
openssh-helpers-6.6p1-17.1
openssh-debugsource-6.6p1-17.1
openssh-helpers-debuginfo-6.6p1-17.1
openssh-askpass-gnome-6.6p1-17.1
openssh-cavs-6.6p1-17.1

openssh-6.6p1-17.1
openssh-debuginfo-6.6p1-17.1

145692 - SuSE Linux 42.2 openSUSE-SU-2017:1459-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8798

Description

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

openSUSE-SU-2017:1459-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00110.html>

SuSE Linux 42.2

x86_64

python-miniupnpc-1.9-7.3.1

libminiupnpc10-1.9-7.3.1

miniupnpc-1.9-7.3.1

miniupnpc-debuginfo-1.9-7.3.1

libminiupnpc-devel-1.9-7.3.1

python-miniupnpc-debuginfo-1.9-7.3.1

libminiupnpc10-debuginfo-32bit-1.9-7.3.1

libminiupnpc10-32bit-1.9-7.3.1

libminiupnpc10-debuginfo-1.9-7.3.1

i586

python-miniupnpc-1.9-7.3.1

libminiupnpc10-1.9-7.3.1

miniupnpc-1.9-7.3.1

miniupnpc-debuginfo-1.9-7.3.1

libminiupnpc-devel-1.9-7.3.1

python-miniupnpc-debuginfo-1.9-7.3.1

libminiupnpc10-debuginfo-1.9-7.3.1

145694 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2364-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8146, CVE-2014-8147

Description

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

openSUSE-SU-2017:2364-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00014.html>

SuSE Linux 42.2

x86_64

libicu52_1-debuginfo-52.1-12.3.1

icu-52.1-12.3.1

icu-debugsource-52.1-12.3.1

libicu52_1-32bit-52.1-12.3.1

libicu52_1-debuginfo-32bit-52.1-12.3.1

libicu-doc-52.1-12.3.1

libicu52_1-data-52.1-12.3.1

libicu52_1-52.1-12.3.1

icu-debuginfo-52.1-12.3.1

libicu-devel-32bit-52.1-12.3.1

icu-data-52.1-12.3.1

libicu-devel-52.1-12.3.1

i586

libicu52_1-debuginfo-52.1-12.3.1

icu-52.1-12.3.1

icu-debugsource-52.1-12.3.1

libicu-doc-52.1-12.3.1

libicu52_1-data-52.1-12.3.1

libicu52_1-52.1-12.3.1

icu-debuginfo-52.1-12.3.1

icu-data-52.1-12.3.1

libicu-devel-52.1-12.3.1

SuSE Linux 42.3

x86_64

icu-data-52.1-15.1

libicu-devel-32bit-52.1-15.1

libicu-doc-52.1-15.1

libicu-devel-52.1-15.1

libicu52_1-52.1-15.1

icu-52.1-15.1

libicu52_1-debuginfo-52.1-15.1

libicu52_1-32bit-52.1-15.1

icu-debugsource-52.1-15.1

libicu52_1-debuginfo-32bit-52.1-15.1

libicu52_1-data-52.1-15.1

icu-debuginfo-52.1-15.1

i586

icu-data-52.1-15.1

libicu-doc-52.1-15.1

libicu-devel-52.1-15.1

libicu52_1-52.1-15.1

icu-52.1-15.1

libicu52_1-debuginfo-52.1-15.1

icu-debugsource-52.1-15.1

libicu52_1-data-52.1-15.1

icu-debuginfo-52.1-15.1

145695 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0765-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5428

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0765-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00070.html>

SuSE Linux 42.1

x86_64

MozillaFirefox-debuginfo-52.0.1-58.1
MozillaFirefox-buildsymbols-52.0.1-58.1
MozillaFirefox-debugsource-52.0.1-58.1
MozillaFirefox-translations-other-52.0.1-58.1
MozillaFirefox-branding-upstream-52.0.1-58.1
MozillaFirefox-52.0.1-58.1
MozillaFirefox-translations-common-52.0.1-58.1
MozillaFirefox-devel-52.0.1-58.1

SuSE Linux 42.2

x86_64

MozillaFirefox-buildsymbols-52.0.1-57.3.1
MozillaFirefox-translations-other-52.0.1-57.3.1
MozillaFirefox-translations-common-52.0.1-57.3.1
MozillaFirefox-devel-52.0.1-57.3.1
MozillaFirefox-debuginfo-52.0.1-57.3.1
MozillaFirefox-debugsource-52.0.1-57.3.1
MozillaFirefox-52.0.1-57.3.1
MozillaFirefox-branding-upstream-52.0.1-57.3.1

i586

MozillaFirefox-buildsymbols-52.0.1-57.3.1
MozillaFirefox-translations-other-52.0.1-57.3.1
MozillaFirefox-translations-common-52.0.1-57.3.1
MozillaFirefox-devel-52.0.1-57.3.1
MozillaFirefox-debuginfo-52.0.1-57.3.1
MozillaFirefox-debugsource-52.0.1-57.3.1
MozillaFirefox-52.0.1-57.3.1
MozillaFirefox-branding-upstream-52.0.1-57.3.1

145696 - SuSE Linux 42.2 openSUSE-SU-2017:1872-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10028, CVE-2016-10029, CVE-2016-9602, CVE-2016-9603, CVE-2017-5579, CVE-2017-5973, CVE-2017-5987, CVE-2017-6505, CVE-2017-7377, CVE-2017-7471, CVE-2017-7493, CVE-2017-7718, CVE-2017-7980, CVE-2017-8086, CVE-2017-8112, CVE-2017-8309, CVE-2017-8379, CVE-2017-8380, CVE-2017-9330, CVE-2017-9373, CVE-2017-9374, CVE-2017-9375, CVE-2017-9503

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1872-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00061.html>

SuSE Linux 42.2

i586

qemu-block-ssh-debuginfo-2.6.2-31.3.3
qemu-block-ssh-2.6.2-31.3.3
qemu-block-iscsi-2.6.2-31.3.3
qemu-testsuite-2.6.2-31.3.6
qemu-arm-2.6.2-31.3.3
qemu-debugsource-2.6.2-31.3.3
qemu-linux-user-2.6.2-31.3.1
qemu-guest-agent-2.6.2-31.3.3
qemu-ppc-debuginfo-2.6.2-31.3.3
qemu-linux-user-debuginfo-2.6.2-31.3.1
qemu-tools-debuginfo-2.6.2-31.3.3
qemu-linux-user-debugsource-2.6.2-31.3.1
qemu-kvm-2.6.2-31.3.3
qemu-block-iscsi-debuginfo-2.6.2-31.3.3
qemu-lang-2.6.2-31.3.3
qemu-arm-debuginfo-2.6.2-31.3.3
qemu-block-dmg-debuginfo-2.6.2-31.3.3
qemu-s390-2.6.2-31.3.3
qemu-x86-2.6.2-31.3.3
qemu-extra-debuginfo-2.6.2-31.3.3
qemu-tools-2.6.2-31.3.3
qemu-2.6.2-31.3.3
qemu-block-curl-2.6.2-31.3.3
qemu-guest-agent-debuginfo-2.6.2-31.3.3
qemu-block-dmg-2.6.2-31.3.3
qemu-x86-debuginfo-2.6.2-31.3.3
qemu-ppc-2.6.2-31.3.3
qemu-block-curl-debuginfo-2.6.2-31.3.3
qemu-s390-debuginfo-2.6.2-31.3.3
qemu-extra-2.6.2-31.3.3

noarch

qemu-ipxe-1.0.0-31.3.3
qemu-vgabios-1.9.1-31.3.3
qemu-sgabios-8-31.3.3
qemu-seabios-1.9.1-31.3.3

x86_64

qemu-block-ssh-debuginfo-2.6.2-31.3.3
qemu-block-ssh-2.6.2-31.3.3
qemu-block-iscsi-2.6.2-31.3.3
qemu-testsuite-2.6.2-31.3.6
qemu-arm-2.6.2-31.3.3
qemu-debugsource-2.6.2-31.3.3
qemu-block-rbd-debuginfo-2.6.2-31.3.3
qemu-linux-user-2.6.2-31.3.1
qemu-guest-agent-2.6.2-31.3.3
qemu-ppc-debuginfo-2.6.2-31.3.3
qemu-linux-user-debuginfo-2.6.2-31.3.1
qemu-tools-debuginfo-2.6.2-31.3.3
qemu-linux-user-debugsource-2.6.2-31.3.1
qemu-kvm-2.6.2-31.3.3
qemu-block-iscsi-debuginfo-2.6.2-31.3.3
qemu-lang-2.6.2-31.3.3
qemu-arm-debuginfo-2.6.2-31.3.3
qemu-block-dmg-debuginfo-2.6.2-31.3.3

qemu-s390-2.6.2-31.3.3
qemu-x86-2.6.2-31.3.3
qemu-extra-debuginfo-2.6.2-31.3.3
qemu-tools-2.6.2-31.3.3
qemu-2.6.2-31.3.3
qemu-block-rbd-2.6.2-31.3.3
qemu-block-curl-2.6.2-31.3.3
qemu-guest-agent-debuginfo-2.6.2-31.3.3
qemu-block-dmg-2.6.2-31.3.3
qemu-x86-debuginfo-2.6.2-31.3.3
qemu-ppc-2.6.2-31.3.3
qemu-block-curl-debuginfo-2.6.2-31.3.3
qemu-s390-debuginfo-2.6.2-31.3.3
qemu-extra-2.6.2-31.3.3

145700 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2318-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8146, CVE-2014-8147

Description

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

SUSE-SU-2017:2318-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003176.html>

SuSE SLED 12 SP2

x86_64
libicu52_1-data-52.1-8.3.1
libicu52_1-debuginfo-32bit-52.1-8.3.1
libicu52_1-52.1-8.3.1
libicu52_1-32bit-52.1-8.3.1
libicu52_1-debuginfo-52.1-8.3.1
icu-debuginfo-52.1-8.3.1
icu-debugsource-52.1-8.3.1
icu-52.1-8.3.1

SuSE SLES 12 SP3

x86_64
libicu52_1-data-52.1-8.3.1
libicu52_1-debuginfo-32bit-52.1-8.3.1
icu-debugsource-52.1-8.3.1
libicu52_1-debuginfo-52.1-8.3.1
libicu52_1-32bit-52.1-8.3.1
libicu-doc-52.1-8.3.1
libicu52_1-52.1-8.3.1
icu-debuginfo-52.1-8.3.1

SuSE SLES 12 SP2

x86_64
libicu52_1-data-52.1-8.3.1
libicu52_1-debuginfo-32bit-52.1-8.3.1
icu-debugsource-52.1-8.3.1

libicu52_1-debuginfo-52.1-8.3.1
libicu52_1-32bit-52.1-8.3.1
libicu-doc-52.1-8.3.1
libicu52_1-52.1-8.3.1
icu-debuginfo-52.1-8.3.1

SuSE SLED 12 SP3

x86_64
libicu52_1-data-52.1-8.3.1
libicu52_1-debuginfo-32bit-52.1-8.3.1
libicu52_1-52.1-8.3.1
libicu52_1-32bit-52.1-8.3.1
libicu52_1-debuginfo-52.1-8.3.1
icu-debuginfo-52.1-8.3.1
icu-debugsource-52.1-8.3.1
icu-52.1-8.3.1

145701 - SuSE Linux 42.1 openSUSE-SU-2017:0397-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10128, CVE-2016-10129, CVE-2016-10130, CVE-2017-5338, CVE-2017-5339

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0397-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00030.html>

SuSE Linux 42.1

x86_64
libgit2-debugsource-0.22.1-8.1
libgit2-22-debuginfo-0.22.1-8.1
libgit2-22-debuginfo-32bit-0.22.1-8.1
libgit2-devel-0.22.1-8.1
libgit2-22-32bit-0.22.1-8.1
libgit2-22-0.22.1-8.1

i586

libgit2-22-debuginfo-0.22.1-8.1
libgit2-devel-0.22.1-8.1
libgit2-debugsource-0.22.1-8.1
libgit2-22-0.22.1-8.1

145702 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0356-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6354

Description

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

openSUSE-SU-2017:0356-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00002.html>

SuSE Linux 42.1

x86_64

seamonkey-2.46-9.2

seamonkey-translations-other-2.46-9.2

seamonkey-translations-common-2.46-9.2

seamonkey-debuginfo-2.46-9.2

seamonkey-debugsource-2.46-9.2

i586

seamonkey-2.46-9.2

seamonkey-translations-other-2.46-9.2

seamonkey-translations-common-2.46-9.2

seamonkey-debuginfo-2.46-9.2

seamonkey-debugsource-2.46-9.2

SuSE Linux 42.2

x86_64

seamonkey-2.46-9.2

seamonkey-translations-other-2.46-9.2

seamonkey-translations-common-2.46-9.2

seamonkey-debuginfo-2.46-9.2

seamonkey-debugsource-2.46-9.2

i586

seamonkey-2.46-9.2

seamonkey-translations-other-2.46-9.2

seamonkey-translations-common-2.46-9.2

seamonkey-debuginfo-2.46-9.2

seamonkey-debugsource-2.46-9.2

145708 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2087-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10970, CVE-2017-11163, CVE-2017-11691, CVE-2017-12065

Description

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

openSUSE-SU-2017:2087-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00018.html>

SuSE Linux 42.2

i586

cacti-spine-1.1.16-7.3.1

cacti-spine-debugsource-1.1.16-7.3.1
cacti-spine-debuginfo-1.1.16-7.3.1

noarch
cacti-doc-1.1.16-16.3.1
cacti-1.1.16-16.3.1

x86_64
cacti-spine-1.1.16-7.3.1
cacti-spine-debugsource-1.1.16-7.3.1
cacti-spine-debuginfo-1.1.16-7.3.1

SuSE Linux 42.3
i586
cacti-spine-debuginfo-1.1.16-10.1
cacti-spine-debugsource-1.1.16-10.1
cacti-spine-1.1.16-10.1

noarch
cacti-1.1.16-19.1
cacti-doc-1.1.16-19.1

x86_64
cacti-spine-debuginfo-1.1.16-10.1
cacti-spine-debugsource-1.1.16-10.1
cacti-spine-1.1.16-10.1

145709 - SuSE Linux 42.1 openSUSE-SU-2017:0141-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808, CVE-2016-9810

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0141-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00074.html>

SuSE Linux 42.1
i586
gststreamer-plugins-good-debuginfo-1.4.5-5.1
gststreamer-plugins-good-1.4.5-5.1
gststreamer-plugins-good-extra-1.4.5-5.1
gststreamer-plugins-good-extra-debuginfo-1.4.5-5.1
gststreamer-plugins-good-doc-1.4.5-5.1
gststreamer-plugins-good-debugsource-1.4.5-5.1

noarch
gststreamer-plugins-good-lang-1.4.5-5.1

x86_64
gststreamer-plugins-good-debuginfo-1.4.5-5.1
gststreamer-plugins-good-1.4.5-5.1

gststreamer-plugins-good-extra-debuginfo-32bit-1.4.5-5.1
gststreamer-plugins-good-extra-1.4.5-5.1
gststreamer-plugins-good-debuginfo-32bit-1.4.5-5.1
gststreamer-plugins-good-extra-32bit-1.4.5-5.1
gststreamer-plugins-good-32bit-1.4.5-5.1
gststreamer-plugins-good-extra-debuginfo-1.4.5-5.1
gststreamer-plugins-good-doc-1.4.5-5.1
gststreamer-plugins-good-debugsource-1.4.5-5.1

145714 - SuSE Linux 42.2 openSUSE-SU-2017:0419-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9577, CVE-2016-9578

Description

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

openSUSE-SU-2017:0419-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00042.html>

SuSE Linux 42.2

x86_64

spice-debugsource-0.12.7-3.1

libspice-server1-debuginfo-0.12.7-3.1

libspice-server-devel-0.12.7-3.1

libspice-server1-0.12.7-3.1

spice-client-0.12.7-3.1

i586

spice-debugsource-0.12.7-3.1

libspice-server1-debuginfo-0.12.7-3.1

libspice-server-devel-0.12.7-3.1

libspice-server1-0.12.7-3.1

spice-client-0.12.7-3.1

145719 - SuSE Linux 42.2 openSUSE-SU-2017:0588-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-10162, CVE-2016-10166, CVE-2016-10167, CVE-2016-10168, CVE-2016-7478, CVE-2016-7479, CVE-2016-7480, CVE-2016-9138, CVE-2017-5340

Description

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

openSUSE-SU-2017:0588-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00001.html>

SuSE Linux 42.2

i586

php7-posix-7.0.7-12.1
php7-readline-debuginfo-7.0.7-12.1
php7-curl-7.0.7-12.1
php7-readline-7.0.7-12.1
php7-gmp-7.0.7-12.1
php7-pcntl-7.0.7-12.1
php7-debuginfo-7.0.7-12.1
php7-wddx-7.0.7-12.1
php7-intl-debuginfo-7.0.7-12.1
php7-opcache-debuginfo-7.0.7-12.1
php7-phar-7.0.7-12.1
php7-ldap-debuginfo-7.0.7-12.1
php7-bcmath-debuginfo-7.0.7-12.1
php7-xsl-7.0.7-12.1
php7-sqlite-debuginfo-7.0.7-12.1
php7-zip-7.0.7-12.1
php7-enchanted-7.0.7-12.1
php7-gd-7.0.7-12.1
php7-fileinfo-7.0.7-12.1
php7-imap-debuginfo-7.0.7-12.1
php7-sockets-debuginfo-7.0.7-12.1
php7-sockets-7.0.7-12.1
php7-ftp-7.0.7-12.1
php7-dom-7.0.7-12.1
php7-sysvshm-7.0.7-12.1
php7-pdo-7.0.7-12.1
php7-mysql-debuginfo-7.0.7-12.1
php7-snmp-debuginfo-7.0.7-12.1
php7-shmop-7.0.7-12.1
php7-dba-debuginfo-7.0.7-12.1
php7-debugsource-7.0.7-12.1
php7-gd-debuginfo-7.0.7-12.1
php7-zip-debuginfo-7.0.7-12.1
php7-fpm-debuginfo-7.0.7-12.1
php7-sysvmsg-debuginfo-7.0.7-12.1
php7-phar-debuginfo-7.0.7-12.1
php7-calendar-7.0.7-12.1
php7-xmlreader-7.0.7-12.1
php7-ctype-7.0.7-12.1
php7-tokenizer-7.0.7-12.1
php7-json-debuginfo-7.0.7-12.1
php7-posix-debuginfo-7.0.7-12.1
php7-bz2-7.0.7-12.1
php7-gettext-debuginfo-7.0.7-12.1
php7-xmlrpc-7.0.7-12.1
php7-zlib-7.0.7-12.1
php7-opcache-7.0.7-12.1
php7-ctype-debuginfo-7.0.7-12.1
php7-curl-debuginfo-7.0.7-12.1
php7-7.0.7-12.1
php7-exif-debuginfo-7.0.7-12.1
php7-sysvsem-7.0.7-12.1
php7-imap-7.0.7-12.1
php7-fastcgi-debuginfo-7.0.7-12.1
php7-snmp-7.0.7-12.1
php7-fastcgi-7.0.7-12.1
php7-shmop-debuginfo-7.0.7-12.1
php7-mcrypt-7.0.7-12.1

php7-ldap-7.0.7-12.1
php7-xmlreader-debuginfo-7.0.7-12.1
php7-iconv-debuginfo-7.0.7-12.1
php7-mbstring-7.0.7-12.1
php7-mcrypt-debuginfo-7.0.7-12.1
php7-soap-debuginfo-7.0.7-12.1
php7-sysvshm-debuginfo-7.0.7-12.1
php7-devel-7.0.7-12.1
php7-xmlrpc-debuginfo-7.0.7-12.1
php7-pspell-7.0.7-12.1
php7-fileinfo-debuginfo-7.0.7-12.1
php7-iconv-7.0.7-12.1
php7-exif-7.0.7-12.1
php7-pgsql-7.0.7-12.1
php7-mbstring-debuginfo-7.0.7-12.1
php7-gmp-debuginfo-7.0.7-12.1
php7-odbc-debuginfo-7.0.7-12.1
php7-pcntl-debuginfo-7.0.7-12.1
php7-dom-debuginfo-7.0.7-12.1
php7-mysql-7.0.7-12.1
php7-sysvsem-debuginfo-7.0.7-12.1
php7-calendar-debuginfo-7.0.7-12.1
php7-enchanted-debuginfo-7.0.7-12.1
php7-zlib-debuginfo-7.0.7-12.1
php7-firebird-7.0.7-12.1
php7-json-7.0.7-12.1
php7-firebird-debuginfo-7.0.7-12.1
php7-pdo-debuginfo-7.0.7-12.1
php7-pgsql-debuginfo-7.0.7-12.1
php7-odbc-7.0.7-12.1
php7-openssl-debuginfo-7.0.7-12.1
php7-bz2-debuginfo-7.0.7-12.1
php7-pspell-debuginfo-7.0.7-12.1
php7-xsl-debuginfo-7.0.7-12.1
php7-tokenizer-debuginfo-7.0.7-12.1
apache2-mod_php7-7.0.7-12.1
php7-gettext-7.0.7-12.1
php7-ftp-debuginfo-7.0.7-12.1
php7-wddx-debuginfo-7.0.7-12.1
php7-sysvmsg-7.0.7-12.1
php7-soap-7.0.7-12.1
php7-dba-7.0.7-12.1
php7-bcmath-7.0.7-12.1
php7-tidy-7.0.7-12.1
php7-xmlwriter-7.0.7-12.1
php7-fpm-7.0.7-12.1
php7-tidy-debuginfo-7.0.7-12.1
apache2-mod_php7-debuginfo-7.0.7-12.1
php7-xmlwriter-debuginfo-7.0.7-12.1
php7-sqlite-7.0.7-12.1
php7-intl-7.0.7-12.1
php7-openssl-7.0.7-12.1

noarch

php7-pear-Archive_Tar-7.0.7-12.1
php7-pear-7.0.7-12.1

x86_64

php7-posix-7.0.7-12.1
php7-readline-debuginfo-7.0.7-12.1

php7-curl-7.0.7-12.1
php7-readline-7.0.7-12.1
php7-gmp-7.0.7-12.1
php7-pcntl-7.0.7-12.1
php7-debuginfo-7.0.7-12.1
php7-wddx-7.0.7-12.1
php7-intl-debuginfo-7.0.7-12.1
php7-opcache-debuginfo-7.0.7-12.1
php7-phar-7.0.7-12.1
php7-ldap-debuginfo-7.0.7-12.1
php7-bcmath-debuginfo-7.0.7-12.1
php7-xsl-7.0.7-12.1
php7-sqlite-debuginfo-7.0.7-12.1
php7-zip-7.0.7-12.1
php7-enchanted-7.0.7-12.1
php7-gd-7.0.7-12.1
php7-fileinfo-7.0.7-12.1
php7-ldap-debuginfo-7.0.7-12.1
php7-sockets-debuginfo-7.0.7-12.1
php7-sockets-7.0.7-12.1
php7-ftp-7.0.7-12.1
php7-dom-7.0.7-12.1
php7-sysvshm-7.0.7-12.1
php7-pdo-7.0.7-12.1
php7-mysql-debuginfo-7.0.7-12.1
php7-snmp-debuginfo-7.0.7-12.1
php7-shmop-7.0.7-12.1
php7-dba-debuginfo-7.0.7-12.1
php7-debugsource-7.0.7-12.1
php7-gd-debuginfo-7.0.7-12.1
php7-zip-debuginfo-7.0.7-12.1
php7-fpm-debuginfo-7.0.7-12.1
php7-sysvmsg-debuginfo-7.0.7-12.1
php7-phar-debuginfo-7.0.7-12.1
php7-calendar-7.0.7-12.1
php7-xmlreader-7.0.7-12.1
php7-ctype-7.0.7-12.1
php7-tokenizer-7.0.7-12.1
php7-json-debuginfo-7.0.7-12.1
php7-posix-debuginfo-7.0.7-12.1
php7-bz2-7.0.7-12.1
php7-gettext-debuginfo-7.0.7-12.1
php7-xmlrpc-7.0.7-12.1
php7-zlib-7.0.7-12.1
php7-opcache-7.0.7-12.1
php7-ctype-debuginfo-7.0.7-12.1
php7-curl-debuginfo-7.0.7-12.1
php7-7.0.7-12.1
php7-exif-debuginfo-7.0.7-12.1
php7-sysvsem-7.0.7-12.1
php7-ldap-7.0.7-12.1
php7-fastcgi-debuginfo-7.0.7-12.1
php7-snmp-7.0.7-12.1
php7-fastcgi-7.0.7-12.1
php7-shmop-debuginfo-7.0.7-12.1
php7-mcrypt-7.0.7-12.1
php7-ldap-7.0.7-12.1
php7-xmlreader-debuginfo-7.0.7-12.1
php7-iconv-debuginfo-7.0.7-12.1
php7-mbstring-7.0.7-12.1

php7-mcrypt-debuginfo-7.0.7-12.1
php7-soap-debuginfo-7.0.7-12.1
php7-sysvshm-debuginfo-7.0.7-12.1
php7-devel-7.0.7-12.1
php7-xmlrpc-debuginfo-7.0.7-12.1
php7-pspell-7.0.7-12.1
php7-fileinfo-debuginfo-7.0.7-12.1
php7-iconv-7.0.7-12.1
php7-exif-7.0.7-12.1
php7-pgsql-7.0.7-12.1
php7-mbstring-debuginfo-7.0.7-12.1
php7-gmp-debuginfo-7.0.7-12.1
php7-odbc-debuginfo-7.0.7-12.1
php7-pcntl-debuginfo-7.0.7-12.1
php7-dom-debuginfo-7.0.7-12.1
php7-mysql-7.0.7-12.1
php7-sysvsem-debuginfo-7.0.7-12.1
php7-calendar-debuginfo-7.0.7-12.1
php7-enchanted-debuginfo-7.0.7-12.1
php7-zlib-debuginfo-7.0.7-12.1
php7-firebird-7.0.7-12.1
php7-json-7.0.7-12.1
php7-firebird-debuginfo-7.0.7-12.1
php7-pdo-debuginfo-7.0.7-12.1
php7-pgsql-debuginfo-7.0.7-12.1
php7-odbc-7.0.7-12.1
php7-openssl-debuginfo-7.0.7-12.1
php7-bz2-debuginfo-7.0.7-12.1
php7-pspell-debuginfo-7.0.7-12.1
php7-xsl-debuginfo-7.0.7-12.1
php7-tokenizer-debuginfo-7.0.7-12.1
apache2-mod_php7-7.0.7-12.1
php7-gettext-7.0.7-12.1
php7-ftp-debuginfo-7.0.7-12.1
php7-wddx-debuginfo-7.0.7-12.1
php7-sysvmsg-7.0.7-12.1
php7-soap-7.0.7-12.1
php7-dba-7.0.7-12.1
php7-bcmath-7.0.7-12.1
php7-tidy-7.0.7-12.1
php7-xmlwriter-7.0.7-12.1
php7-fpm-7.0.7-12.1
php7-tidy-debuginfo-7.0.7-12.1
apache2-mod_php7-debuginfo-7.0.7-12.1
php7-xmlwriter-debuginfo-7.0.7-12.1
php7-sqlite-7.0.7-12.1
php7-intl-7.0.7-12.1
php7-openssl-7.0.7-12.1

145720 - SuSE Linux 42.2 openSUSE-SU-2017:1507-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3509, CVE-2017-3511, CVE-2017-3512, CVE-2017-3514, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1507-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00021.html>

SuSE Linux 42.2

i586

java-1_8_0-openjdk-headless-1.8.0.131-10.8.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.131-10.8.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.131-10.8.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.131-10.8.1
java-1_8_0-openjdk-accessibility-1.8.0.131-10.8.1
java-1_8_0-openjdk-debuginfo-1.8.0.131-10.8.1
java-1_8_0-openjdk-devel-1.8.0.131-10.8.1
java-1_8_0-openjdk-debugsource-1.8.0.131-10.8.1
java-1_8_0-openjdk-src-1.8.0.131-10.8.1
java-1_8_0-openjdk-1.8.0.131-10.8.1
java-1_8_0-openjdk-demo-1.8.0.131-10.8.1

noarch

java-1_8_0-openjdk-javadoc-1.8.0.131-10.8.1

x86_64

java-1_8_0-openjdk-headless-1.8.0.131-10.8.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.131-10.8.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.131-10.8.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.131-10.8.1
java-1_8_0-openjdk-accessibility-1.8.0.131-10.8.1
java-1_8_0-openjdk-debuginfo-1.8.0.131-10.8.1
java-1_8_0-openjdk-devel-1.8.0.131-10.8.1
java-1_8_0-openjdk-debugsource-1.8.0.131-10.8.1
java-1_8_0-openjdk-src-1.8.0.131-10.8.1
java-1_8_0-openjdk-1.8.0.131-10.8.1
java-1_8_0-openjdk-demo-1.8.0.131-10.8.1

145721 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:1984-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:1984-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00100.html>

SuSE Linux 42.2

x86_64

the_silver_searcher-debuginfo-2.0.0-3.3.1
the_silver_searcher-2.0.0-3.3.1
the_silver_searcher-debugsource-2.0.0-3.3.1

i586
the_silver_searcher-debuginfo-2.0.0-3.3.1
the_silver_searcher-2.0.0-3.3.1
the_silver_searcher-debugsource-2.0.0-3.3.1

SuSE Linux 42.3
x86_64
the_silver_searcher-2.0.0-6.1
the_silver_searcher-debugsource-2.0.0-6.1
the_silver_searcher-debuginfo-2.0.0-6.1

i586
the_silver_searcher-2.0.0-6.1
the_silver_searcher-debugsource-2.0.0-6.1
the_silver_searcher-debuginfo-2.0.0-6.1

145725 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:2326-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2326-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-September/003179.html>

SuSE SLED 12 SP2
x86_64
xen-libs-debuginfo-4.7.3_03-43.9.1
xen-4.7.3_03-43.9.1
xen-debugsource-4.7.3_03-43.9.1
xen-libs-debuginfo-32bit-4.7.3_03-43.9.1
xen-libs-4.7.3_03-43.9.1
xen-libs-32bit-4.7.3_03-43.9.1

SuSE SLES 12 SP2
x86_64
xen-libs-debuginfo-4.7.3_03-43.9.1
xen-tools-debuginfo-4.7.3_03-43.9.1
xen-tools-domU-debuginfo-4.7.3_03-43.9.1
xen-doc-html-4.7.3_03-43.9.1
xen-4.7.3_03-43.9.1
xen-debugsource-4.7.3_03-43.9.1
xen-libs-debuginfo-32bit-4.7.3_03-43.9.1
xen-libs-4.7.3_03-43.9.1
xen-tools-domU-4.7.3_03-43.9.1
xen-libs-32bit-4.7.3_03-43.9.1
xen-tools-4.7.3_03-43.9.1

145726 - SuSE Linux 42.2 openSUSE-SU-2017:2331-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2331-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00000.html>

SuSE Linux 42.2

x86_64

git-daemon-debuginfo-2.12.3-5.10.1

git-credential-gnome-keyring-debuginfo-2.12.3-5.10.1

git-gui-2.12.3-5.10.1

git-svn-2.12.3-5.10.1

git-core-2.12.3-5.10.1

git-debugsource-2.12.3-5.10.1

git-email-2.12.3-5.10.1

git-cvs-2.12.3-5.10.1

git-svn-debuginfo-2.12.3-5.10.1

git-2.12.3-5.10.1

git-credential-gnome-keyring-2.12.3-5.10.1

git-core-debuginfo-2.12.3-5.10.1

git-daemon-2.12.3-5.10.1

gitk-2.12.3-5.10.1

git-arch-2.12.3-5.10.1

git-web-2.12.3-5.10.1

noarch

git-doc-2.12.3-5.10.1

145730 - SuSE Linux 42.2 openSUSE-SU-2017:0847-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808, CVE-2016-9810

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0847-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00105.html>

SuSE Linux 42.2

i586

gststreamer-0_10-plugins-good-extra-debuginfo-0.10.31-17.3.1
gststreamer-0_10-plugins-good-debuginfo-0.10.31-17.3.1
gststreamer-0_10-plugins-good-extra-0.10.31-17.3.1
gststreamer-0_10-plugins-good-debugsource-0.10.31-17.3.1
gststreamer-0_10-plugins-good-doc-0.10.31-17.3.1
gststreamer-0_10-plugin-esd-debuginfo-0.10.31-17.3.1
gststreamer-0_10-plugins-good-0.10.31-17.3.1
gststreamer-0_10-plugin-esd-0.10.31-17.3.1

noarch

gststreamer-0_10-plugins-good-lang-0.10.31-17.3.1

x86_64

gststreamer-0_10-plugins-good-0.10.31-17.3.1
gststreamer-0_10-plugins-good-extra-0.10.31-17.3.1
gststreamer-0_10-plugins-good-debuginfo-32bit-0.10.31-17.3.1
gststreamer-0_10-plugin-esd-debuginfo-32bit-0.10.31-17.3.1
gststreamer-0_10-plugins-good-extra-debuginfo-0.10.31-17.3.1
gststreamer-0_10-plugin-esd-32bit-0.10.31-17.3.1
gststreamer-0_10-plugins-good-32bit-0.10.31-17.3.1
gststreamer-0_10-plugins-good-debuginfo-0.10.31-17.3.1
gststreamer-0_10-plugins-good-extra-debuginfo-32bit-0.10.31-17.3.1
gststreamer-0_10-plugins-good-debugsource-0.10.31-17.3.1
gststreamer-0_10-plugin-esd-0.10.31-17.3.1
gststreamer-0_10-plugins-good-extra-32bit-0.10.31-17.3.1
gststreamer-0_10-plugins-good-doc-0.10.31-17.3.1
gststreamer-0_10-plugin-esd-debuginfo-0.10.31-17.3.1

145731 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0081-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9933, CVE-2016-9934, CVE-2016-9935

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0081-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00054.html>

SuSE Linux 42.1

i586

php5-gd-debuginfo-5.5.14-71.1
php5-mcrypt-5.5.14-71.1
php5-mysql-5.5.14-71.1
php5-sysvmsg-debuginfo-5.5.14-71.1
php5-opcache-5.5.14-71.1
php5-sysvsem-debuginfo-5.5.14-71.1
php5-pgsql-debuginfo-5.5.14-71.1
php5-debuginfo-5.5.14-71.1
php5-xsl-debuginfo-5.5.14-71.1
php5-dom-5.5.14-71.1
php5-soap-debuginfo-5.5.14-71.1
php5-sysvshm-debuginfo-5.5.14-71.1

php5-dba-debuginfo-5.5.14-71.1
php5-devel-5.5.14-71.1
php5-zlib-debuginfo-5.5.14-71.1
php5-xmlreader-debuginfo-5.5.14-71.1
php5-gd-5.5.14-71.1
php5-bcmath-debuginfo-5.5.14-71.1
php5-odbc-debuginfo-5.5.14-71.1
php5-5.5.14-71.1
php5-pspell-debuginfo-5.5.14-71.1
php5-tokenizer-debuginfo-5.5.14-71.1
php5-wddx-5.5.14-71.1
php5-json-5.5.14-71.1
php5-zip-debuginfo-5.5.14-71.1
php5-zlib-5.5.14-71.1
php5-phar-5.5.14-71.1
php5-gmp-debuginfo-5.5.14-71.1
php5-pdo-debuginfo-5.5.14-71.1
php5-mbstring-5.5.14-71.1
php5-readline-5.5.14-71.1
php5-opcache-debuginfo-5.5.14-71.1
php5-fastcgi-5.5.14-71.1
php5-tokenizer-5.5.14-71.1
php5-odbc-5.5.14-71.1
php5-tidy-5.5.14-71.1
php5-bz2-5.5.14-71.1
php5-calendar-debuginfo-5.5.14-71.1
php5-ctype-debuginfo-5.5.14-71.1
php5-ftp-5.5.14-71.1
php5-shmop-debuginfo-5.5.14-71.1
php5-phar-debuginfo-5.5.14-71.1
php5-dba-5.5.14-71.1
php5-intl-debuginfo-5.5.14-71.1
php5-mbstring-debuginfo-5.5.14-71.1
php5-openssl-5.5.14-71.1
php5-enchanted-debuginfo-5.5.14-71.1
php5-json-debuginfo-5.5.14-71.1
php5-openssl-debuginfo-5.5.14-71.1
php5-mysql-5.5.14-71.1
apache2-mod_php5-5.5.14-71.1
php5-sqlite-debuginfo-5.5.14-71.1
php5-sqlite-5.5.14-71.1
php5-suhosin-5.5.14-71.1
php5-gettext-debuginfo-5.5.14-71.1
php5-shmop-5.5.14-71.1
php5-sysvshm-5.5.14-71.1
php5-xsl-5.5.14-71.1
php5-ldap-debuginfo-5.5.14-71.1
php5-ldap-5.5.14-71.1
php5-sockets-5.5.14-71.1
php5-tidy-debuginfo-5.5.14-71.1
php5-fileinfo-5.5.14-71.1
php5-gettext-5.5.14-71.1
php5-iconv-debuginfo-5.5.14-71.1
php5-xmlwriter-5.5.14-71.1
php5-wddx-debuginfo-5.5.14-71.1
php5-posix-5.5.14-71.1
php5-bz2-debuginfo-5.5.14-71.1
php5-enchanted-5.5.14-71.1
php5-xmlrpc-debuginfo-5.5.14-71.1
php5-firebird-5.5.14-71.1

php5-dom-debuginfo-5.5.14-71.1
php5-ldap-5.5.14-71.1
php5-zip-5.5.14-71.1
php5-snmp-5.5.14-71.1
php5-fpm-debuginfo-5.5.14-71.1
php5-posix-debuginfo-5.5.14-71.1
php5-ftp-debuginfo-5.5.14-71.1
php5-curl-debuginfo-5.5.14-71.1
php5-xmlwriter-debuginfo-5.5.14-71.1
php5-mysql-debuginfo-5.5.14-71.1
php5-firebird-debuginfo-5.5.14-71.1
php5-sockets-debuginfo-5.5.14-71.1
php5-exif-5.5.14-71.1
php5-xmlrpc-5.5.14-71.1
php5-xmlreader-5.5.14-71.1
php5-gmp-5.5.14-71.1
php5-pcntl-debuginfo-5.5.14-71.1
php5-sysvmsg-5.5.14-71.1
php5-sysvsem-5.5.14-71.1
php5-fastcgi-debuginfo-5.5.14-71.1
php5-ctype-5.5.14-71.1
php5-mcrypt-debuginfo-5.5.14-71.1
php5-pdo-5.5.14-71.1
php5-bcmath-5.5.14-71.1
php5-calendar-5.5.14-71.1
php5-suhosin-debuginfo-5.5.14-71.1
php5-mssql-debuginfo-5.5.14-71.1
php5-pspell-5.5.14-71.1
php5-pgsql-5.5.14-71.1
php5-soap-5.5.14-71.1
php5-readline-debuginfo-5.5.14-71.1
php5-iconv-5.5.14-71.1
php5-pcntl-5.5.14-71.1
php5-debugsource-5.5.14-71.1
php5-intl-5.5.14-71.1
php5-fileinfo-debuginfo-5.5.14-71.1
php5-fpm-5.5.14-71.1
php5-curl-5.5.14-71.1
php5-ldap-debuginfo-5.5.14-71.1
php5-snmp-debuginfo-5.5.14-71.1
apache2-mod_php5-debuginfo-5.5.14-71.1
php5-exif-debuginfo-5.5.14-71.1

noarch

php5-pear-5.5.14-71.1

x86_64

php5-gd-debuginfo-5.5.14-71.1
php5-mcrypt-5.5.14-71.1
php5-mysql-5.5.14-71.1
php5-sysvmsg-debuginfo-5.5.14-71.1
php5-opcache-5.5.14-71.1
php5-sysvsem-debuginfo-5.5.14-71.1
php5-pgsql-debuginfo-5.5.14-71.1
php5-debuginfo-5.5.14-71.1
php5-xsl-debuginfo-5.5.14-71.1
php5-dom-5.5.14-71.1
php5-soap-debuginfo-5.5.14-71.1
php5-sysvshm-debuginfo-5.5.14-71.1
php5-dba-debuginfo-5.5.14-71.1

php5-devel-5.5.14-71.1
php5-zlib-debuginfo-5.5.14-71.1
php5-xmlreader-debuginfo-5.5.14-71.1
php5-gd-5.5.14-71.1
php5-bcmath-debuginfo-5.5.14-71.1
php5-odbc-debuginfo-5.5.14-71.1
php5-5.5.14-71.1
php5-pspell-debuginfo-5.5.14-71.1
php5-tokenizer-debuginfo-5.5.14-71.1
php5-wddx-5.5.14-71.1
php5-json-5.5.14-71.1
php5-zip-debuginfo-5.5.14-71.1
php5-zlib-5.5.14-71.1
php5-phar-5.5.14-71.1
php5-gmp-debuginfo-5.5.14-71.1
php5-pdo-debuginfo-5.5.14-71.1
php5-mbstring-5.5.14-71.1
php5-readline-5.5.14-71.1
php5-opcache-debuginfo-5.5.14-71.1
php5-fastcgi-5.5.14-71.1
php5-tokenizer-5.5.14-71.1
php5-odbc-5.5.14-71.1
php5-tidy-5.5.14-71.1
php5-bz2-5.5.14-71.1
php5-calendar-debuginfo-5.5.14-71.1
php5-ctype-debuginfo-5.5.14-71.1
php5-ftp-5.5.14-71.1
php5-shmop-debuginfo-5.5.14-71.1
php5-phar-debuginfo-5.5.14-71.1
php5-dba-5.5.14-71.1
php5-intl-debuginfo-5.5.14-71.1
php5-mbstring-debuginfo-5.5.14-71.1
php5-openssl-5.5.14-71.1
php5-enchanted-debuginfo-5.5.14-71.1
php5-json-debuginfo-5.5.14-71.1
php5-openssl-debuginfo-5.5.14-71.1
php5-mssql-5.5.14-71.1
apache2-mod_php5-5.5.14-71.1
php5-sqlite-debuginfo-5.5.14-71.1
php5-sqlite-5.5.14-71.1
php5-suhosin-5.5.14-71.1
php5-gettext-debuginfo-5.5.14-71.1
php5-shmop-5.5.14-71.1
php5-sysvshm-5.5.14-71.1
php5-xsl-5.5.14-71.1
php5-imap-debuginfo-5.5.14-71.1
php5-imap-5.5.14-71.1
php5-sockets-5.5.14-71.1
php5-tidy-debuginfo-5.5.14-71.1
php5-fileinfo-5.5.14-71.1
php5-gettext-5.5.14-71.1
php5-iconv-debuginfo-5.5.14-71.1
php5-xmlwriter-5.5.14-71.1
php5-wddx-debuginfo-5.5.14-71.1
php5-posix-5.5.14-71.1
php5-bz2-debuginfo-5.5.14-71.1
php5-enchanted-5.5.14-71.1
php5-xmlrpc-debuginfo-5.5.14-71.1
php5-firebird-5.5.14-71.1
php5-dom-debuginfo-5.5.14-71.1

php5-ldap-5.5.14-71.1
php5-zip-5.5.14-71.1
php5-snmp-5.5.14-71.1
php5-fpm-debuginfo-5.5.14-71.1
php5-posix-debuginfo-5.5.14-71.1
php5-ftp-debuginfo-5.5.14-71.1
php5-curl-debuginfo-5.5.14-71.1
php5-xmlwriter-debuginfo-5.5.14-71.1
php5-mysql-debuginfo-5.5.14-71.1
php5-firebird-debuginfo-5.5.14-71.1
php5-sockets-debuginfo-5.5.14-71.1
php5-exif-5.5.14-71.1
php5-xmlrpc-5.5.14-71.1
php5-xmlreader-5.5.14-71.1
php5-gmp-5.5.14-71.1
php5-pcntl-debuginfo-5.5.14-71.1
php5-sysvmsg-5.5.14-71.1
php5-sysvsem-5.5.14-71.1
php5-fastcgi-debuginfo-5.5.14-71.1
php5-ctype-5.5.14-71.1
php5-mcrypt-debuginfo-5.5.14-71.1
php5-pdo-5.5.14-71.1
php5-bcmath-5.5.14-71.1
php5-calendar-5.5.14-71.1
php5-suhosin-debuginfo-5.5.14-71.1
php5-mssql-debuginfo-5.5.14-71.1
php5-ispell-5.5.14-71.1
php5-pgsql-5.5.14-71.1
php5-soap-5.5.14-71.1
php5-readline-debuginfo-5.5.14-71.1
php5-iconv-5.5.14-71.1
php5-pcntl-5.5.14-71.1
php5-debugsource-5.5.14-71.1
php5-intl-5.5.14-71.1
php5-fileinfo-debuginfo-5.5.14-71.1
php5-fpm-5.5.14-71.1
php5-curl-5.5.14-71.1
php5-ldap-debuginfo-5.5.14-71.1
php5-snmp-debuginfo-5.5.14-71.1
apache2-mod_php5-debuginfo-5.5.14-71.1
php5-exif-debuginfo-5.5.14-71.1

SuSE Linux 42.2

i586

php5-opcache-5.5.14-72.1
php5-mcrypt-debuginfo-5.5.14-72.1
php5-gettext-debuginfo-5.5.14-72.1
php5-calendar-5.5.14-72.1
php5-5.5.14-72.1
php5-soap-debuginfo-5.5.14-72.1
php5-xmlwriter-debuginfo-5.5.14-72.1
php5-odbc-5.5.14-72.1

145732 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1088-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9574

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1088-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00089.html>

SuSE Linux 42.1

i586

mozilla-nss-debugsource-3.28.4-41.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-25.1
libsoftoken3-debuginfo-3.28.4-41.1
mozilla-nss-tools-debuginfo-3.28.4-41.1
java-1_8_0-openjdk-debugsource-1.8.0.121-25.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-25.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-25.1
mozilla-nss-devel-3.28.4-41.1
libfreebl3-debuginfo-3.28.4-41.1
mozilla-nss-certs-3.28.4-41.1
mozilla-nss-certs-debuginfo-3.28.4-41.1
java-1_8_0-openjdk-debuginfo-1.8.0.121-25.1
mozilla-nss-sysinit-debuginfo-3.28.4-41.1
java-1_8_0-openjdk-headless-1.8.0.121-25.1
mozilla-nss-sysinit-3.28.4-41.1
mozilla-nss-tools-3.28.4-41.1
java-1_8_0-openjdk-src-1.8.0.121-25.1
java-1_8_0-openjdk-1.8.0.121-25.1
java-1_8_0-openjdk-devel-1.8.0.121-25.1
java-1_8_0-openjdk-demo-1.8.0.121-25.1
libfreebl3-3.28.4-41.1
mozilla-nss-3.28.4-41.1
java-1_8_0-openjdk-accessibility-1.8.0.121-25.1
mozilla-nss-debuginfo-3.28.4-41.1
libsoftoken3-3.28.4-41.1

noarch

java-1_8_0-openjdk-javadoc-1.8.0.121-25.1

x86_64

libsoftoken3-3.28.4-41.1
mozilla-nss-debuginfo-3.28.4-41.1
libsoftoken3-debuginfo-32bit-3.28.4-41.1
libfreebl3-debuginfo-32bit-3.28.4-41.1
libfreebl3-debuginfo-3.28.4-41.1
libfreebl3-3.28.4-41.1
java-1_8_0-openjdk-accessibility-1.8.0.121-25.1
mozilla-nss-tools-3.28.4-41.1
mozilla-nss-certs-debuginfo-3.28.4-41.1
java-1_8_0-openjdk-debugsource-1.8.0.121-25.1
mozilla-nss-devel-3.28.4-41.1
java-1_8_0-openjdk-devel-1.8.0.121-25.1
mozilla-nss-certs-32bit-3.28.4-41.1
libfreebl3-32bit-3.28.4-41.1
java-1_8_0-openjdk-headless-1.8.0.121-25.1
libsoftoken3-32bit-3.28.4-41.1
java-1_8_0-openjdk-src-1.8.0.121-25.1

java-1_8_0-openjdk-debuginfo-1.8.0.121-25.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-25.1
mozilla-nss-certs-3.28.4-41.1
mozilla-nss-certs-debuginfo-32bit-3.28.4-41.1
mozilla-nss-sysinit-32bit-3.28.4-41.1
libsoftokn3-debuginfo-3.28.4-41.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-25.1
java-1_8_0-openjdk-demo-1.8.0.121-25.1
mozilla-nss-debuginfo-32bit-3.28.4-41.1
mozilla-nss-sysinit-3.28.4-41.1
mozilla-nss-sysinit-debuginfo-3.28.4-41.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-25.1
mozilla-nss-32bit-3.28.4-41.1
mozilla-nss-3.28.4-41.1
mozilla-nss-tools-debuginfo-3.28.4-41.1
java-1_8_0-openjdk-1.8.0.121-25.1
mozilla-nss-debugsource-3.28.4-41.1
mozilla-nss-sysinit-debuginfo-32bit-3.28.4-41.1

SuSE Linux 42.2

i586

java-1_8_0-openjdk-1.8.0.121-10.2.1
libsoftokn3-debuginfo-3.28.4-40.3.1
mozilla-nss-certs-3.28.4-40.3.1
java-1_8_0-openjdk-devel-1.8.0.121-10.2.1
mozilla-nss-tools-3.28.4-40.3.1
mozilla-nss-sysinit-3.28.4-40.3.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-10.2.1
java-1_8_0-openjdk-headless-1.8.0.121-10.2.1
mozilla-nss-devel-3.28.4-40.3.1
mozilla-nss-certs-debuginfo-3.28.4-40.3.1
libfreebl3-3.28.4-40.3.1
java-1_8_0-openjdk-debuginfo-1.8.0.121-10.2.1
mozilla-nss-3.28.4-40.3.1
mozilla-nss-sysinit-debuginfo-3.28.4-40.3.1
java-1_8_0-openjdk-debugsource-1.8.0.121-10.2.1
java-1_8_0-openjdk-accessibility-1.8.0.121-10.2.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-10.2.1
java-1_8_0-openjdk-demo-1.8.0.121-10.2.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-10.2.1
java-1_8_0-openjdk-src-1.8.0.121-10.2.1
mozilla-nss-debuginfo-3.28.4-40.3.1
mozilla-nss-tools-debuginfo-3.28.4-40.3.1
libsoftokn3-3.28.4-40.3.1
libfreebl3-debuginfo-3.28.4-40.3.1
mozilla-nss-debugsource-3.28.4-40.3.1

noarch

java-1_8_0-openjdk-javadoc-1.8.0.121-10.2.1

x86_64

mozilla-nss-tools-3.28.4-40.3.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-10.2.1
mozilla-nss-certs-debuginfo-32bit-3.28.4-40.3.1
java-1_8_0-openjdk-demo-1.8.0.121-10.2.1
libfreebl3-32bit-3.28.4-40.3.1
mozilla-nss-devel-3.28.4-40.3.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-10.2.1
java-1_8_0-openjdk-debugsource-1.8.0.121-10.2.1
libsoftokn3-32bit-3.28.4-40.3.1

java-1_8_0-openjdk-debuginfo-1.8.0.121-10.2.1
mozilla-nss-certs-32bit-3.28.4-40.3.1
java-1_8_0-openjdk-headless-1.8.0.121-10.2.1
mozilla-nss-tools-debuginfo-3.28.4-40.3.1
libsoftokn3-debuginfo-3.28.4-40.3.1
mozilla-nss-3.28.4-40.3.1
mozilla-nss-certs-debuginfo-3.28.4-40.3.1
mozilla-nss-sysinit-debuginfo-3.28.4-40.3.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-10.2.1
mozilla-nss-debuginfo-32bit-3.28.4-40.3.1
mozilla-nss-sysinit-32bit-3.28.4-40.3.1
libfreebl3-debuginfo-3.28.4-40.3.1
mozilla-nss-debuginfo-3.28.4-40.3.1
libsoftokn3-debuginfo-32bit-3.28.4-40.3.1
java-1_8_0-openjdk-accessibility-1.8.0.121-10.2.1
java-1_8_0-openjdk-devel-1.8.0.121-10.2.1
mozilla-nss-sysinit-3.28.4-40.3.1
libfreebl3-3.28.4-40.3.1
mozilla-nss-sysinit-debuginfo-32bit-3.28.4-40.3.1
java-1_8_0-openjdk-1.8.0.121-10.2.1
libsoftokn3-3.28.4-40.3.1
mozilla-nss-certs-3.28.4-40.3.1
java-1_8_0-openjdk-src-1.8.0.121-10.2.1
mozilla-nss-debugsource-3.28.4-40.3.1
libfreebl3-debuginfo-32bit-3.28.4-40.3.1
mozilla-nss-32bit-3.28.4-40.3.1

145733 - SuSE Linux 42.2 openSUSE-SU-2017:1851-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10327, CVE-2017-7870, CVE-2017-7882, CVE-2017-8358, CVE-2017-9433

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1851-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00055.html>

SuSE Linux 42.2

i586

myspell-lightproof-en-20170511-6.3.1
libstaroffice-0_0-0-debuginfo-0.0.3-2.3.1
libmwaw-tools-0.3.11-6.3.1
libixion-tools-0.12.1-8.3.1
libixion-0_12-0-debuginfo-0.12.1-8.3.1
libzmf-tools-debuginfo-0.0.1-2.1
liborcus-0_12-0-0.12.1-9.3.1
liborcus-tools-debuginfo-0.12.1-9.3.1
liborcus-tools-0.12.1-9.3.1
libmwaw-0_3-3-0.3.11-6.3.1
libstaroffice-tools-debuginfo-0.0.3-2.3.1
libzmf-0_0-0-0.0.1-2.1
libixion-python3-0.12.1-8.3.1

liborcus-python3-0.12.1-9.3.1
libzmf-devel-0.0.1-2.1
libmwaw-tools-debuginfo-0.3.11-6.3.1
myspell-lightproof-pt_BR-20170511-6.3.1
libixion-0_12-0-0.12.1-8.3.1
libmwaw-debugsource-0.3.11-6.3.1
libzmf-0_0-0-debuginfo-0.0.1-2.1
liborcus-python3-debuginfo-0.12.1-9.3.1
libmwaw-devel-0.3.11-6.3.1
libstaroffice-debugsource-0.0.3-2.3.1
libixion-debugsource-0.12.1-8.3.1
libstaroffice-0_0-0-0.0.3-2.3.1
libstaroffice-tools-0.0.3-2.3.1
libzmf-debugsource-0.0.1-2.1
libixion-python3-debuginfo-0.12.1-8.3.1
liborcus-devel-0.12.1-9.3.1
libzmf-tools-0.0.1-2.1
myspell-lightproof-ru_RU-20170511-6.3.1
libstaroffice-devel-0.0.3-2.3.1
libmwaw-0_3-3-debuginfo-0.3.11-6.3.1
myspell-dictionaries-20170511-6.3.1
libixion-devel-0.12.1-8.3.1
liborcus-debugsource-0.12.1-9.3.1
liborcus-0_12-0-debuginfo-0.12.1-9.3.1
myspell-lightproof-hu_HU-20170511-6.3.1
libixion-tools-debuginfo-0.12.1-8.3.1

noarch

libreoffice-l10n-nb-5.3.3.2-18.6.2
myspell-lo_LA-20170511-6.3.1
myspell-ar_OM-20170511-6.3.1
myspell-is-20170511-6.3.1
myspell-nb_NO-20170511-6.3.1
myspell-fr_CH-20170511-6.3.1
myspell-en_AU-20170511-6.3.1
myspell-ca_ES-20170511-6.3.1
myspell-en_ZA-20170511-6.3.1
libreoffice-l10n-sl-5.3.3.2-18.6.2
libreoffice-l10n-nn-5.3.3.2-18.6.2
libreoffice-l10n-gl-5.3.3.2-18.6.2
libreoffice-l10n-cy-5.3.3.2-18.6.2
myspell-pl_PL-20170511-6.3.1
myspell-sw_TZ-20170511-6.3.1
myspell-ro-20170511-6.3.1
myspell-oc_FR-20170511-6.3.1
libreoffice-l10n-nr-5.3.3.2-18.6.2
libreoffice-l10n-ja-5.3.3.2-18.6.2
libreoffice-l10n-xh-5.3.3.2-18.6.2
libreoffice-l10n-pl-5.3.3.2-18.6.2
libreoffice-l10n-hr-5.3.3.2-18.6.2
libreoffice-l10n-nso-5.3.3.2-18.6.2
myspell-pt_AO-20170511-6.3.1
libreoffice-icon-theme-tango-5.3.3.2-18.6.2
libreoffice-l10n-ga-5.3.3.2-18.6.2
libreoffice-l10n-kn-5.3.3.2-18.6.2
libreoffice-gdb-pretty-printers-5.3.3.2-18.6.2
myspell-de_DE-20170511-6.3.1
myspell-hi_IN-20170511-6.3.1
libreoffice-icon-theme-breeze-5.3.3.2-18.6.2
libreoffice-icon-theme-oxygen-5.3.3.2-18.6.2

libreoffice-l10n-zu-5.3.3.2-18.6.2
myspell-ca-20170511-6.3.1
myspell-en-20170511-6.3.1
libreoffice-l10n-fa-5.3.3.2-18.6.2
libzmf-devel-doc-0.0.1-2.1
libmwaw-devel-doc-0.3.11-6.3.1
libreoffice-l10n-da-5.3.3.2-18.6.2
libreoffice-l10n-hu-5.3.3.2-18.6.2
libreoffice-l10n-lv-5.3.3.2-18.6.2
libreoffice-l10n-he-5.3.3.2-18.6.2
libreoffice-l10n-sr-5.3.3.2-18.6.2
libreoffice-l10n-bn-5.3.3.2-18.6.2
myspell-de_AT-20170511-6.3.1
myspell-ar_BH-20170511-6.3.1
libreoffice-l10n-ca-5.3.3.2-18.6.2
myspell-sr-20170511-6.3.1
myspell-fr_LU-20170511-6.3.1
libreoffice-l10n-ar-5.3.3.2-18.6.2
myspell-en_NZ-20170511-6.3.1
myspell-en_IN-20170511-6.3.1
libreoffice-l10n-it-5.3.3.2-18.6.2
myspell-ar_JO-20170511-6.3.1
myspell-ar_DZ-20170511-6.3.1
myspell-ar_MA-20170511-6.3.1
libreoffice-icon-theme-sifr-5.3.3.2-18.6.2
myspell-de_CH-20170511-6.3.1
myspell-ca_AD-20170511-6.3.1
myspell-ca_ES_valencia-20170511-6.3.1
myspell-sr_RS-20170511-6.3.1
myspell-bo_CN-20170511-6.3.1
myspell-en_MW-20170511-6.3.1
myspell-es_CL-20170511-6.3.1
myspell-ar_SA-20170511-6.3.1
myspell-te-20170511-6.3.1
myspell-el_GR-20170511-6.3.1
myspell-sv_SE-20170511-6.3.1
myspell-es_PR-20170511-6.3.1
myspell-ar_IQ-20170511-6.3.1
libreoffice-branding-upstream-5.3.3.2-18.6.2
myspell-es-20170511-6.3.1
myspell-en_BS-20170511-6.3.1
myspell-es_AR-20170511-6.3.1
myspell-ar_KW-20170511-6.3.1
libreoffice-l10n-ml-5.3.3.2-18.6.2
myspell-en_BZ-20170511-6.3.1
libstaroffice-devel-doc-0.0.3-2.3.1
myspell-ar_AE-20170511-6.3.1
myspell-da_DK-20170511-6.3.1
libreoffice-icon-theme-galaxy-5.3.3.2-18.6.2
myspell-nl_BE-20170511-6.3.1
myspell-it_IT-20170511-6.3.1
libreoffice-l10n-kk-5.3.3.2-18.6.2
myspell-en_GH-20170511-6.3.1
myspell-gl-20170511-6.3.1
myspell-ar-20170511-6.3.1
libreoffice-l10n-ta-5.3.3.2-18.6.2
myspell-ne_NP-20170511-6.3.1
libreoffice-l10n-zh_CN-5.3.3.2-18.6.2
myspell-th_TH-20170511-6.3.1
myspell-sr_Latn_CS-20170511-6.3.1

myspell-no-20170511-6.3.1
myspell-an-20170511-6.3.1
myspell-ar_SD-20170511-6.3.1
libreoffice-l10n-fi-5.3.3.2-18.6.2
myspell-es_MX-20170511-6.3.1
myspell-ca_IT-20170511-6.3.1
libreoffice-l10n-dz-5.3.3.2-18.6.2
myspell-sv_FI-20170511-6.3.1
libreoffice-l10n-eu-5.3.3.2-18.6.2
myspell-gu_IN-20170511-6.3.1
myspell-en_CA-20170511-6.3.1
myspell-es_VE-20170511-6.3.1
myspell-cs_CZ-20170511-6.3.1
myspell-et_EE-20170511-6.3.1
myspell-vi-20170511-6.3.1
myspell-es_BO-20170511-6.3.1
myspell-ru_RU-20170511-6.3.1
libreoffice-l10n-tr-5.3.3.2-18.6.2
libreoffice-l10n-pa-5.3.3.2-18.6.2
myspell-kmr_Latn-20170511-6.3.1
myspell-bs-20170511-6.3.1
myspell-lv_LV-20170511-6.3.1
myspell-he_IL-20170511-6.3.1
myspell-gd_GB-20170511-6.3.1
libreoffice-l10n-mr-5.3.3.2-18.6.2
myspell-ro_RO-20170511-6.3.1
libreoffice-l10n-zh_TW-5.3.3.2-18.6.2
myspell-ar_EG-20170511-6.3.1
myspell-af_NA-20170511-6.3.1
myspell-es_PY-20170511-6.3.1
libreoffice-l10n-af-5.3.3.2-18.6.2
myspell-fr_FR-20170511-6.3.1
myspell-an_ES-20170511-6.3.1
libreoffice-l10n-en-5.3.3.2-18.6.2
myspell-pt_PT-20170511-6.3.1
myspell-ar_SY-20170511-6.3.1
myspell-sl_SI-20170511-6.3.1
myspell-es_PE-20170511-6.3.1
myspell-fr_MC-20170511-6.3.1
libreoffice-l10n-ko-5.3.3.2-18.6.2
myspell-ar_TN-20170511-6.3.1
myspell-ar_LB-20170511-6.3.1
libreoffice-l10n-te-5.3.3.2-18.6.2
libreoffice-l10n-es-5.3.3.2-18.6.2
libreoffice-l10n-or-5.3.3.2-18.6.2
libreoffice-l10n-it-5.3.3.2-18.6.2
myspell-be_BY-20170511-6.3.1
libreoffice-l10n-nl-5.3.3.2-18.6.2
myspell-es_HN-20170511-6.3.1
myspell-en_PH-20170511-6.3.1
libreoffice-l10n-el-5.3.3.2-18.6.2
myspell-nn_NO-20170511-6.3.1
myspell-bg_BG-20170511-6.3.1
myspell-en_JM-20170511-6.3.1
libreoffice-l10n-mai-5.3.3.2-18.6.2
myspell-en_NA-20170511-6.3.1
libreoffice-l10n-ss-5.3.3.2-18.6.2
myspell-gug_PY-20170511-6.3.1
myspell-es_EC-20170511-6.3.1
libreoffice-l10n-ve-5.3.3.2-18.6.2

myspell-sr_Latn_RS-20170511-6.3.1
myspell-en_GB-20170511-6.3.1
myspell-es_NI-20170511-6.3.1
libreoffice-l10n-fr-5.3.3.2-18.6.2
libreoffice-l10n-uk-5.3.3.2-18.6.2
libreoffice-l10n-as-5.3.3.2-18.6.2
myspell-fr_BE-20170511-6.3.1
libreoffice-l10n-de-5.3.3.2-18.6.2
myspell-en_ZW-20170511-6.3.1
myspell-en_TT-20170511-6.3.1
myspell-sk_SK-20170511-6.3.1
myspell-hu_HU-20170511-6.3.1
myspell-lt_LT-20170511-6.3.1
myspell-nl_NL-20170511-6.3.1
myspell-sr_CS-20170511-6.3.1
libreoffice-l10n-sv-5.3.3.2-18.6.2
libreoffice-l10n-tn-5.3.3.2-18.6.2
myspell-kmr_Latn_TR-20170511-6.3.1
libreoffice-l10n-ru-5.3.3.2-18.6.2
libreoffice-l10n-et-5.3.3.2-18.6.2
myspell-gl_ES-20170511-6.3.1

145734 - SuSE Linux 42.2 openSUSE-SU-2017:1485-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6255, CVE-2016-8863

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1485-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00006.html>

SuSE Linux 42.2

x86_64

libupnp6-32bit-1.6.21-4.3.1

libupnp-devel-1.6.21-4.3.1

libupnp6-debuginfo-32bit-1.6.21-4.3.1

libupnp6-debugsource-1.6.21-4.3.1

libupnp6-debuginfo-1.6.21-4.3.1

libupnp6-1.6.21-4.3.1

i586

libupnp-devel-1.6.21-4.3.1

libupnp6-debuginfo-1.6.21-4.3.1

libupnp6-1.6.21-4.3.1

libupnp6-debugsource-1.6.21-4.3.1

145740 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2249-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11636, CVE-2017-11643

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2249-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00095.html>

SuSE Linux 42.2

x86_64

libGraphicsMagick-Q16-3-1.3.25-11.18.1
GraphicsMagick-1.3.25-11.18.1
libGraphicsMagick++-devel-1.3.25-11.18.1
perl-GraphicsMagick-debuginfo-1.3.25-11.18.1
GraphicsMagick-debuginfo-1.3.25-11.18.1
libGraphicsMagick3-config-1.3.25-11.18.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.18.1
GraphicsMagick-debugsource-1.3.25-11.18.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.18.1
perl-GraphicsMagick-1.3.25-11.18.1
libGraphicsMagickWand-Q16-2-1.3.25-11.18.1
GraphicsMagick-devel-1.3.25-11.18.1
libGraphicsMagick++-Q16-12-1.3.25-11.18.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.18.1

i586

libGraphicsMagick-Q16-3-1.3.25-11.18.1
GraphicsMagick-1.3.25-11.18.1
libGraphicsMagick++-devel-1.3.25-11.18.1
perl-GraphicsMagick-debuginfo-1.3.25-11.18.1
GraphicsMagick-debuginfo-1.3.25-11.18.1
libGraphicsMagick3-config-1.3.25-11.18.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.18.1
GraphicsMagick-debugsource-1.3.25-11.18.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.18.1
perl-GraphicsMagick-1.3.25-11.18.1
libGraphicsMagickWand-Q16-2-1.3.25-11.18.1
GraphicsMagick-devel-1.3.25-11.18.1
libGraphicsMagick++-Q16-12-1.3.25-11.18.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.18.1

SuSE Linux 42.3

x86_64

libGraphicsMagick++-Q16-12-debuginfo-1.3.25-20.1
GraphicsMagick-debuginfo-1.3.25-20.1
perl-GraphicsMagick-debuginfo-1.3.25-20.1
libGraphicsMagick3-config-1.3.25-20.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-20.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-20.1
GraphicsMagick-debugsource-1.3.25-20.1
libGraphicsMagickWand-Q16-2-1.3.25-20.1
GraphicsMagick-devel-1.3.25-20.1
libGraphicsMagick++-devel-1.3.25-20.1
libGraphicsMagick-Q16-3-1.3.25-20.1
GraphicsMagick-1.3.25-20.1

perl-GraphicsMagick-1.3.25-20.1
libGraphicsMagick++-Q16-12-1.3.25-20.1

i586

libGraphicsMagick++-Q16-12-debuginfo-1.3.25-20.1
GraphicsMagick-debuginfo-1.3.25-20.1
perl-GraphicsMagick-debuginfo-1.3.25-20.1
libGraphicsMagick3-config-1.3.25-20.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-20.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-20.1
GraphicsMagick-debugsource-1.3.25-20.1
libGraphicsMagickWand-Q16-2-1.3.25-20.1
GraphicsMagick-devel-1.3.25-20.1
libGraphicsMagick++-devel-1.3.25-20.1
libGraphicsMagick-Q16-3-1.3.25-20.1
GraphicsMagick-1.3.25-20.1
perl-GraphicsMagick-1.3.25-20.1
libGraphicsMagick++-Q16-12-1.3.25-20.1

145741 - SuSE Linux 42.3 openSUSE-SU-2017:2370-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7436

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2370-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00020.html>

SuSE Linux 42.3

i586

zypper-debugsource-1.13.32-8.1
libzypp-debugsource-16.15.6-12.1
libzypp-16.15.6-12.1
zypper-1.13.32-8.1
zypper-debuginfo-1.13.32-8.1
libzypp-devel-doc-16.15.6-12.1
libzypp-devel-16.15.6-12.1
libzypp-debuginfo-16.15.6-12.1

noarch

zypper-aptitude-1.13.32-8.1
zypper-log-1.13.32-8.1

x86_64

zypper-debugsource-1.13.32-8.1
libzypp-debugsource-16.15.6-12.1
libzypp-16.15.6-12.1
zypper-1.13.32-8.1
zypper-debuginfo-1.13.32-8.1
libzypp-devel-doc-16.15.6-12.1
libzypp-devel-16.15.6-12.1

145743 - SuSE Linux 42.2 openSUSE-SU-2017:0061-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9933, CVE-2016-9934, CVE-2016-9935, CVE-2016-9936

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0061-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00034.html>

SuSE Linux 42.2

i586

php7-ftp-7.0.7-9.1

php7-mbstring-debuginfo-7.0.7-9.1

php7-enchanted-debuginfo-7.0.7-9.1

php7-xmlrpc-debuginfo-7.0.7-9.1

php7-enchanted-7.0.7-9.1

php7-sqlite-debuginfo-7.0.7-9.1

php7-gd-7.0.7-9.1

php7-tidy-debuginfo-7.0.7-9.1

php7-curl-7.0.7-9.1

php7-firebird-debuginfo-7.0.7-9.1

php7-sqlite-7.0.7-9.1

php7-zlib-7.0.7-9.1

php7-pcntl-7.0.7-9.1

php7-snmp-debuginfo-7.0.7-9.1

php7-pspell-debuginfo-7.0.7-9.1

php7-shmop-7.0.7-9.1

php7-ftp-debuginfo-7.0.7-9.1

php7-sysvsem-debuginfo-7.0.7-9.1

php7-7.0.7-9.1

php7-posix-7.0.7-9.1

php7-openssl-debuginfo-7.0.7-9.1

php7-xmlrpc-7.0.7-9.1

php7-fastcgi-7.0.7-9.1

php7-xmlwriter-debuginfo-7.0.7-9.1

php7-mbstring-7.0.7-9.1

php7-imap-debuginfo-7.0.7-9.1

php7-xsl-debuginfo-7.0.7-9.1

php7-ldap-7.0.7-9.1

php7-soap-7.0.7-9.1

php7-gettext-7.0.7-9.1

php7-tidy-7.0.7-9.1

php7-curl-debuginfo-7.0.7-9.1

php7-opcache-debuginfo-7.0.7-9.1

apache2-mod_php7-debuginfo-7.0.7-9.1

php7-sysvmsg-debuginfo-7.0.7-9.1

php7-mysql-7.0.7-9.1

php7-phar-7.0.7-9.1

php7-fpm-7.0.7-9.1

php7-json-debuginfo-7.0.7-9.1
php7-zlib-debuginfo-7.0.7-9.1
php7-bz2-7.0.7-9.1
php7-iconv-debuginfo-7.0.7-9.1
php7-json-7.0.7-9.1
php7-sockets-debuginfo-7.0.7-9.1
php7-dba-debuginfo-7.0.7-9.1
php7-bcmath-7.0.7-9.1
php7-dba-7.0.7-9.1
php7-bz2-debuginfo-7.0.7-9.1
php7-shmop-debuginfo-7.0.7-9.1
php7-ldap-debuginfo-7.0.7-9.1
php7-sockets-7.0.7-9.1
php7-posix-debuginfo-7.0.7-9.1
php7-dom-debuginfo-7.0.7-9.1
php7-tokenizer-debuginfo-7.0.7-9.1
php7-pgsql-7.0.7-9.1
php7-mcrypt-debuginfo-7.0.7-9.1
php7-pdo-7.0.7-9.1
php7-calendar-debuginfo-7.0.7-9.1
php7-gmp-7.0.7-9.1
php7-ctype-debuginfo-7.0.7-9.1
php7-zip-debuginfo-7.0.7-9.1
php7-xmlwriter-7.0.7-9.1
php7-fileinfo-7.0.7-9.1
php7-iconv-7.0.7-9.1
php7-sysvshm-debuginfo-7.0.7-9.1
php7-calendar-7.0.7-9.1
php7-pspell-7.0.7-9.1
php7-devel-7.0.7-9.1
php7-sysvmsg-7.0.7-9.1
php7-exif-7.0.7-9.1
apache2-mod_php7-7.0.7-9.1
php7-debugsource-7.0.7-9.1
php7-odbc-debuginfo-7.0.7-9.1
php7-fastcgi-debuginfo-7.0.7-9.1
php7-debuginfo-7.0.7-9.1
php7-xsl-7.0.7-9.1
php7-odbc-7.0.7-9.1
php7-wddx-7.0.7-9.1
php7-firebird-7.0.7-9.1
php7-intl-debuginfo-7.0.7-9.1
php7-gettext-debuginfo-7.0.7-9.1
php7-mcrypt-7.0.7-9.1
php7-ctype-7.0.7-9.1
php7-snmp-7.0.7-9.1
php7-openssl-7.0.7-9.1
php7-fileinfo-debuginfo-7.0.7-9.1
php7-mysql-debuginfo-7.0.7-9.1
php7-soap-debuginfo-7.0.7-9.1
php7-intl-7.0.7-9.1
php7-xmlreader-debuginfo-7.0.7-9.1
php7-bcmath-debuginfo-7.0.7-9.1
php7-phar-debuginfo-7.0.7-9.1
php7-fpm-debuginfo-7.0.7-9.1
php7-zip-7.0.7-9.1
php7-opcache-7.0.7-9.1
php7-tokenizer-7.0.7-9.1
php7-imap-7.0.7-9.1
php7-sysvsem-7.0.7-9.1

php7-gd-debuginfo-7.0.7-9.1
php7-pgsql-debuginfo-7.0.7-9.1
php7-pcntl-debuginfo-7.0.7-9.1
php7-xmlreader-7.0.7-9.1
php7-wddx-debuginfo-7.0.7-9.1
php7-exif-debuginfo-7.0.7-9.1
php7-gmp-debuginfo-7.0.7-9.1
php7-pdo-debuginfo-7.0.7-9.1
php7-dom-7.0.7-9.1
php7-readline-debuginfo-7.0.7-9.1
php7-readline-7.0.7-9.1
php7-sysvshm-7.0.7-9.1

noarch

php7-pear-7.0.7-9.1
php7-pear-Archive_Tar-7.0.7-9.1

x86_64

php7-ftp-7.0.7-9.1
php7-mbstring-debuginfo-7.0.7-9.1
php7-enchanted-debuginfo-7.0.7-9.1
php7-xmlrpc-debuginfo-7.0.7-9.1
php7-enchanted-7.0.7-9.1
php7-sqlite-debuginfo-7.0.7-9.1
php7-gd-7.0.7-9.1
php7-tidy-debuginfo-7.0.7-9.1
php7-curl-7.0.7-9.1
php7-firebird-debuginfo-7.0.7-9.1
php7-sqlite-7.0.7-9.1
php7-zlib-7.0.7-9.1
php7-pcntl-7.0.7-9.1
php7-snmp-debuginfo-7.0.7-9.1
php7-pspell-debuginfo-7.0.7-9.1
php7-shmop-7.0.7-9.1
php7-ftp-debuginfo-7.0.7-9.1
php7-sysvsem-debuginfo-7.0.7-9.1
php7-7.0.7-9.1
php7-posix-7.0.7-9.1
php7-openssl-debuginfo-7.0.7-9.1
php7-xmlrpc-7.0.7-9.1
php7-fastcgi-7.0.7-9.1
php7-xmlwriter-debuginfo-7.0.7-9.1
php7-mbstring-7.0.7-9.1
php7-imap-debuginfo-7.0.7-9.1
php7-xsl-debuginfo-7.0.7-9.1
php7-ldap-7.0.7-9.1
php7-soap-7.0.7-9.1
php7-gettext-7.0.7-9.1
php7-tidy-7.0.7-9.1
php7-curl-debuginfo-7.0.7-9.1
php7-opcache-debuginfo-7.0.7-9.1
apache2-mod_php7-debuginfo-7.0.7-9.1
php7-sysvmsg-debuginfo-7.0.7-9.1
php7-mysql-7.0.7-9.1
php7-phar-7.0.7-9.1
php7-fpm-7.0.7-9.1
php7-json-debuginfo-7.0.7-9.1
php7-zlib-debuginfo-7.0.7-9.1
php7-bz2-7.0.7-9.1
php7-iconv-debuginfo-7.0.7-9.1

php7-json-7.0.7-9.1
php7-sockets-debuginfo-7.0.7-9.1
php7-dba-debuginfo-7.0.7-9.1
php7-bcmath-7.0.7-9.1
php7-dba-7.0.7-9.1
php7-bz2-debuginfo-7.0.7-9.1
php7-shmop-debuginfo-7.0.7-9.1
php7-ldap-debuginfo-7.0.7-9.1
php7-sockets-7.0.7-9.1
php7-posix-debuginfo-7.0.7-9.1
php7-dom-debuginfo-7.0.7-9.1
php7-tokenizer-debuginfo-7.0.7-9.1
php7-pgsql-7.0.7-9.1
php7-mcrypt-debuginfo-7.0.7-9.1
php7-pdo-7.0.7-9.1
php7-calendar-debuginfo-7.0.7-9.1
php7-gmp-7.0.7-9.1
php7-ctype-debuginfo-7.0.7-9.1
php7-zip-debuginfo-7.0.7-9.1
php7-xmlwriter-7.0.7-9.1
php7-fileinfo-7.0.7-9.1
php7-iconv-7.0.7-9.1
php7-sysvshm-debuginfo-7.0.7-9.1
php7-calendar-7.0.7-9.1
php7-ispell-7.0.7-9.1
php7-devel-7.0.7-9.1
php7-sysvmsg-7.0.7-9.1
php7-exif-7.0.7-9.1
apache2-mod_php7-7.0.7-9.1
php7-debugsource-7.0.7-9.1
php7-odbc-debuginfo-7.0.7-9.1
php7-fastcgi-debuginfo-7.0.7-9.1
php7-debuginfo-7.0.7-9.1
php7-xsl-7.0.7-9.1
php7-odbc-7.0.7-9.1
php7-wddx-7.0.7-9.1
php7-firebird-7.0.7-9.1
php7-intl-debuginfo-7.0.7-9.1
php7-gettext-debuginfo-7.0.7-9.1
php7-mcrypt-7.0.7-9.1
php7-ctype-7.0.7-9.1
php7-snmp-7.0.7-9.1
php7-openssl-7.0.7-9.1
php7-fileinfo-debuginfo-7.0.7-9.1
php7-mysql-debuginfo-7.0.7-9.1
php7-soap-debuginfo-7.0.7-9.1
php7-intl-7.0.7-9.1
php7-xmlreader-debuginfo-7.0.7-9.1
php7-bcmath-debuginfo-7.0.7-9.1
php7-phar-debuginfo-7.0.7-9.1
php7-fpm-debuginfo-7.0.7-9.1
php7-zip-7.0.7-9.1
php7-opcache-7.0.7-9.1
php7-tokenizer-7.0.7-9.1
php7-ldap-7.0.7-9.1
php7-sysvsem-7.0.7-9.1
php7-gd-debuginfo-7.0.7-9.1
php7-pgsql-debuginfo-7.0.7-9.1
php7-pcntl-debuginfo-7.0.7-9.1
php7-xmlreader-7.0.7-9.1

php7-wddx-debuginfo-7.0.7-9.1
php7-exif-debuginfo-7.0.7-9.1
php7-gmp-debuginfo-7.0.7-9.1
php7-pdo-debuginfo-7.0.7-9.1
php7-dom-7.0.7-9.1
php7-readline-debuginfo-7.0.7-9.1
php7-readline-7.0.7-9.1
php7-sysvshm-7.0.7-9.1

145746 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2337-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10397, CVE-2016-5766, CVE-2017-11142, CVE-2017-11144, CVE-2017-11145, CVE-2017-11146, CVE-2017-11147, CVE-2017-11628, CVE-2017-7890

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2337-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00005.html>

SuSE Linux 42.2

i586

php7-tokenizer-7.0.7-14.9.1
php7-snmp-debuginfo-7.0.7-14.9.1
php7-sysvmsg-debuginfo-7.0.7-14.9.1
php7-mysql-debuginfo-7.0.7-14.9.1
php7-sysvshm-debuginfo-7.0.7-14.9.1
php7-shmop-debuginfo-7.0.7-14.9.1
php7-dba-debuginfo-7.0.7-14.9.1
php7-fastcgi-debuginfo-7.0.7-14.9.1
php7-zip-7.0.7-14.9.1
php7-bcmath-debuginfo-7.0.7-14.9.1
php7-calendar-debuginfo-7.0.7-14.9.1
php7-gd-debuginfo-7.0.7-14.9.1
php7-ftp-debuginfo-7.0.7-14.9.1
php7-imap-debuginfo-7.0.7-14.9.1
php7-ldap-debuginfo-7.0.7-14.9.1
php7-mcrypt-debuginfo-7.0.7-14.9.1
apache2-mod_php7-7.0.7-14.9.1
php7-openssl-7.0.7-14.9.1
php7-exif-debuginfo-7.0.7-14.9.1
php7-json-7.0.7-14.9.1
php7-xmlrpc-7.0.7-14.9.1
php7-sysvmsg-7.0.7-14.9.1
php7-pdo-7.0.7-14.9.1
php7-7.0.7-14.9.1
php7-zlib-7.0.7-14.9.1
php7-bz2-debuginfo-7.0.7-14.9.1
php7-calendar-7.0.7-14.9.1
php7-pgsql-debuginfo-7.0.7-14.9.1
php7-shmop-7.0.7-14.9.1
php7-readline-debuginfo-7.0.7-14.9.1

php7-fileinfo-7.0.7-14.9.1
php7-gettext-7.0.7-14.9.1
php7-iconv-7.0.7-14.9.1
php7-debuginfo-7.0.7-14.9.1
php7-opcache-7.0.7-14.9.1
php7-ctype-debuginfo-7.0.7-14.9.1
php7-sysvshm-7.0.7-14.9.1
php7-xmlreader-7.0.7-14.9.1
php7-curl-debuginfo-7.0.7-14.9.1
php7-zip-debuginfo-7.0.7-14.9.1
php7-opcache-debuginfo-7.0.7-14.9.1
php7-sysvsem-debuginfo-7.0.7-14.9.1
php7-sqlite-debuginfo-7.0.7-14.9.1
php7-exif-7.0.7-14.9.1
apache2-mod_php7-debuginfo-7.0.7-14.9.1
php7-pcntl-7.0.7-14.9.1
php7-bz2-7.0.7-14.9.1
php7-xmlrpc-debuginfo-7.0.7-14.9.1
php7-fileinfo-debuginfo-7.0.7-14.9.1
php7-fastcgi-7.0.7-14.9.1
php7-devel-7.0.7-14.9.1
php7-pcntl-debuginfo-7.0.7-14.9.1
php7-fpm-debuginfo-7.0.7-14.9.1
php7-debugsource-7.0.7-14.9.1
php7-fpm-7.0.7-14.9.1
php7-xmlwriter-debuginfo-7.0.7-14.9.1
php7-firebird-7.0.7-14.9.1
php7-wddx-debuginfo-7.0.7-14.9.1
php7-posix-7.0.7-14.9.1
php7-odbc-debuginfo-7.0.7-14.9.1
php7-ftp-7.0.7-14.9.1
php7-wddx-7.0.7-14.9.1
php7-phar-debuginfo-7.0.7-14.9.1
php7-tokenizer-debuginfo-7.0.7-14.9.1
php7-tidy-debuginfo-7.0.7-14.9.1
php7-xmlwriter-7.0.7-14.9.1
php7-pspell-7.0.7-14.9.1
php7-mcrypt-7.0.7-14.9.1
php7-sqlite-7.0.7-14.9.1
php7-json-debuginfo-7.0.7-14.9.1
php7-bcmath-7.0.7-14.9.1
php7-mysql-7.0.7-14.9.1
php7-soap-7.0.7-14.9.1
php7-snmp-7.0.7-14.9.1
php7-gd-7.0.7-14.9.1
php7-sysvsem-7.0.7-14.9.1
php7-xsl-7.0.7-14.9.1
php7-sockets-7.0.7-14.9.1
php7-curl-7.0.7-14.9.1
php7-posix-debuginfo-7.0.7-14.9.1
php7-dba-7.0.7-14.9.1
php7-phar-7.0.7-14.9.1
php7-intl-7.0.7-14.9.1
php7-iconv-debuginfo-7.0.7-14.9.1
php7-gettext-debuginfo-7.0.7-14.9.1
php7-gmp-debuginfo-7.0.7-14.9.1
php7-pdo-debuginfo-7.0.7-14.9.1
php7-ldap-7.0.7-14.9.1
php7-enchanted-debuginfo-7.0.7-14.9.1
php7-sockets-debuginfo-7.0.7-14.9.1

php7-soap-debuginfo-7.0.7-14.9.1
php7-xmlreader-debuginfo-7.0.7-14.9.1
php7-dom-7.0.7-14.9.1
php7-mbstring-debuginfo-7.0.7-14.9.1
php7-tidy-7.0.7-14.9.1
php7-gmp-7.0.7-14.9.1
php7-openssl-debuginfo-7.0.7-14.9.1
php7-zlib-debuginfo-7.0.7-14.9.1
php7-pspell-debuginfo-7.0.7-14.9.1
php7-intl-debuginfo-7.0.7-14.9.1
php7-mbstring-7.0.7-14.9.1
php7-readline-7.0.7-14.9.1
php7-pgsql-7.0.7-14.9.1
php7-imap-7.0.7-14.9.1
php7-enchanted-7.0.7-14.9.1
php7-odbc-7.0.7-14.9.1
php7-firebird-debuginfo-7.0.7-14.9.1
php7-ctype-7.0.7-14.9.1
php7-dom-debuginfo-7.0.7-14.9.1
php7-xsl-debuginfo-7.0.7-14.9.1

noarch

php7-pear-7.0.7-14.9.1
php7-pear-Archive_Tar-7.0.7-14.9.1

x86_64

php7-tokenizer-7.0.7-14.9.1
php7-snmp-debuginfo-7.0.7-14.9.1
php7-sysvmsg-debuginfo-7.0.7-14.9.1
php7-mysql-debuginfo-7.0.7-14.9.1
php7-sysvshm-debuginfo-7.0.7-14.9.1
php7-shmop-debuginfo-7.0.7-14.9.1
php7-dba-debuginfo-7.0.7-14.9.1
php7-fastcgi-debuginfo-7.0.7-14.9.1
php7-zip-7.0.7-14.9.1
php7-bcmath-debuginfo-7.0.7-14.9.1
php7-calendar-debuginfo-7.0.7-14.9.1
php7-gd-debuginfo-7.0.7-14.9.1
php7-ftp-debuginfo-7.0.7-14.9.1
php7-imap-debuginfo-7.0.7-14.9.1
php7-ldap-debuginfo-7.0.7-14.9.1
php7-mcrypt-debuginfo-7.0.7-14.9.1
apache2-mod_php7-7.0.7-14.9.1
php7-openssl-7.0.7-14.9.1
php7-exif-debuginfo-7.0.7-14.9.1
php7-json-7.0.7-14.9.1
php7-xmlrpc-7.0.7-14.9.1
php7-sysvmsg-7.0.7-14.9.1
php7-pdo-7.0.7-14.9.1
php7-7.0.7-14.9.1
php7-zlib-7.0.7-14.9.1
php7-bz2-debuginfo-7.0.7-14.9.1
php7-calendar-7.0.7-14.9.1
php7-pgsql-debuginfo-7.0.7-14.9.1
php7-shmop-7.0.7-14.9.1
php7-readline-debuginfo-7.0.7-14.9.1
php7-fileinfo-7.0.7-14.9.1
php7-gettext-7.0.7-14.9.1
php7-iconv-7.0.7-14.9.1
php7-debuginfo-7.0.7-14.9.1

php7-opcache-7.0.7-14.9.1
php7-ctype-debuginfo-7.0.7-14.9.1
php7-sysvshm-7.0.7-14.9.1
php7-xmlreader-7.0.7-14.9.1
php7-curl-debuginfo-7.0.7-14.9.1
php7-zip-debuginfo-7.0.7-14.9.1
php7-opcache-debuginfo-7.0.7-14.9.1
php7-sysvsem-debuginfo-7.0.7-14.9.1
php7-sqlite-debuginfo-7.0.7-14.9.1
php7-exif-7.0.7-14.9.1
apache2-mod_php7-debuginfo-7.0.7-14.9.1
php7-pcntl-7.0.7-14.9.1
php7-bz2-7.0.7-14.9.1
php7-xmlrpc-debuginfo-7.0.7-14.9.1
php7-fileinfo-debuginfo-7.0.7-14.9.1
php7-fastcgi-7.0.7-14.9.1
php7-devel-7.0.7-14.9.1
php7-pcntl-debuginfo-7.0.7-14.9.1
php7-fpm-debuginfo-7.0.7-14.9.1
php7-debugsource-7.0.7-14.9.1
php7-fpm-7.0.7-14.9.1
php7-xmlwriter-debuginfo-7.0.7-14.9.1
php7-firebird-7.0.7-14.9.1
php7-wddx-debuginfo-7.0.7-14.9.1
php7-posix-7.0.7-14.9.1
php7-odbc-debuginfo-7.0.7-14.9.1
php7-ftp-7.0.7-14.9.1
php7-wddx-7.0.7-14.9.1
php7-phar-debuginfo-7.0.7-14.9.1
php7-tokenizer-debuginfo-7.0.7-14.9.1
php7-tidy-debuginfo-7.0.7-14.9.1
php7-xmlwriter-7.0.7-14.9.1
php7-pspell-7.0.7-14.9.1
php7-mcrypt-7.0.7-14.9.1
php7-sqlite-7.0.7-14.9.1
php7-json-debuginfo-7.0.7-14.9.1
php7-bcmath-7.0.7-14.9.1
php7-mysql-7.0.7-14.9.1
php7-soap-7.0.7-14.9.1
php7-snmp-7.0.7-14.9.1
php7-gd-7.0.7-14.9.1
php7-sysvsem-7.0.7-14.9.1
php7-xsl-7.0.7-14.9.1
php7-sockets-7.0.7-14.9.1
php7-curl-7.0.7-14.9.1
php7-posix-debuginfo-7.0.7-14.9.1
php7-dba-7.0.7-14.9.1
php7-phar-7.0.7-14.9.1
php7-intl-7.0.7-14.9.1
php7-iconv-debuginfo-7.0.7-14.9.1
php7-gettext-debuginfo-7.0.7-14.9.1
php7-gmp-debuginfo-7.0.7-14.9.1
php7-pdo-debuginfo-7.0.7-14.9.1
php7-ldap-7.0.7-14.9.1
php7-enchanted-debuginfo-7.0.7-14.9.1
php7-sockets-debuginfo-7.0.7-14.9.1
php7-soap-debuginfo-7.0.7-14.9.1
php7-xmlreader-debuginfo-7.0.7-14.9.1
php7-dom-7.0.7-14.9.1
php7-mbstring-debuginfo-7.0.7-14.9.1

php7-tidy-7.0.7-14.9.1
php7-gmp-7.0.7-14.9.1
php7-openssl-debuginfo-7.0.7-14.9.1
php7-zlib-debuginfo-7.0.7-14.9.1
php7-pspell-debuginfo-7.0.7-14.9.1
php7-intl-debuginfo-7.0.7-14.9.1
php7-mbstring-7.0.7-14.9.1
php7-readline-7.0.7-14.9.1
php7-pgsql-7.0.7-14.9.1
php7-imap-7.0.7-14.9.1
php7-enchanted-7.0.7-14.9.1
php7-odbc-7.0.7-14.9.1
php7-firebird-debuginfo-7.0.7-14.9.1
php7-ctype-7.0.7-14.9.1
php7-dom-debuginfo-7.0.7-14.9.1
php7-xsl-debuginfo-7.0.7-14.9.1

SuSE Linux 42.3

i586

php7-pgsql-debuginfo-7.0.7-19.1
php7-ftp-debuginfo-7.0.7-19.1
php7-pspell-debuginfo-7.0.7-19.1
php7-fastcgi-7.0.7-19.1
php7-json-debuginfo-7.0.7-19.1
php7-readline-7.0.7-19.1
php7-ldap-7.0.7-19.1
php7-dba-debuginfo-7.0.7-19.1

145747 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0358-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5373, CVE-2017-5374, CVE-2017-5375, CVE-2017-5376, CVE-2017-5377, CVE-2017-5378, CVE-2017-5379, CVE-2017-5380, CVE-2017-5381, CVE-2017-5382, CVE-2017-5383, CVE-2017-5384, CVE-2017-5385, CVE-2017-5386, CVE-2017-5387, CVE-2017-5388, CVE-2017-5389, CVE-2017-5390, CVE-2017-5391, CVE-2017-5392, CVE-2017-5393, CVE-2017-5394, CVE-2017-5395, CVE-2017-5396

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0358-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00004.html>

SuSE Linux 42.1

x86_64

MozillaFirefox-debuginfo-51.0.1-50.2
MozillaFirefox-buildsymbols-51.0.1-50.2
MozillaFirefox-51.0.1-50.2
MozillaFirefox-branding-upstream-51.0.1-50.2
MozillaFirefox-devel-51.0.1-50.2
MozillaFirefox-translations-common-51.0.1-50.2
MozillaFirefox-translations-other-51.0.1-50.2
MozillaFirefox-debugsource-51.0.1-50.2

SuSE Linux 42.2
x86_64
MozillaFirefox-debuginfo-51.0.1-50.2
MozillaFirefox-buildsymbols-51.0.1-50.2
MozillaFirefox-51.0.1-50.2
MozillaFirefox-branding-upstream-51.0.1-50.2
MozillaFirefox-devel-51.0.1-50.2
MozillaFirefox-translations-common-51.0.1-50.2
MozillaFirefox-translations-other-51.0.1-50.2
MozillaFirefox-debugsource-51.0.1-50.2

i586
MozillaFirefox-debuginfo-51.0.1-50.2
MozillaFirefox-buildsymbols-51.0.1-50.2
MozillaFirefox-51.0.1-50.2
MozillaFirefox-branding-upstream-51.0.1-50.2
MozillaFirefox-devel-51.0.1-50.2
MozillaFirefox-translations-common-51.0.1-50.2
MozillaFirefox-translations-other-51.0.1-50.2
MozillaFirefox-debugsource-51.0.1-50.2

145748 - SuSE Linux 42.1 openSUSE-SU-2017:0590-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0590-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00003.html>

SuSE Linux 42.1
i586
python-libmount-debuginfo-2.25-21.1
libblkid-devel-2.25-21.1
python-libmount-debugsource-2.25-21.1
libuuid1-debuginfo-2.25-21.1
libsmartcols-devel-2.25-21.1
libblkid1-debuginfo-2.25-21.1
util-linux-debuginfo-2.25-21.1
uuidd-debuginfo-2.25-21.1
libmount1-debuginfo-2.25-21.1
libmount1-2.25-21.1
libuuid1-2.25-21.1
util-linux-debugsource-2.25-21.1
util-linux-2.25-21.1
uuidd-2.25-21.1
libsmartcols1-2.25-21.1
libblkid1-2.25-21.1
libsmartcols1-debuginfo-2.25-21.1
libuuid-devel-2.25-21.1
libmount-devel-2.25-21.1

python-libmount-2.25-21.1
util-linux-systemd-debuginfo-2.25-21.1
util-linux-systemd-2.25-21.1
util-linux-systemd-debugsource-2.25-21.1

noarch
util-linux-lang-2.25-21.1

x86_64
libblkid-devel-32bit-2.25-21.1
libuuid-devel-32bit-2.25-21.1
libuuid-devel-2.25-21.1
libuuid1-32bit-2.25-21.1
libuuid1-2.25-21.1
libsmartcols-devel-2.25-21.1
util-linux-debuginfo-2.25-21.1
python-libmount-2.25-21.1
uuidd-debuginfo-2.25-21.1
libblkid1-debuginfo-2.25-21.1
util-linux-systemd-debugsource-2.25-21.1
python-libmount-debuginfo-2.25-21.1
util-linux-debugsource-2.25-21.1
libmount1-debuginfo-32bit-2.25-21.1
libsmartcols1-2.25-21.1
libsmartcols1-debuginfo-2.25-21.1
libmount1-2.25-21.1
util-linux-systemd-2.25-21.1
libmount-devel-32bit-2.25-21.1
util-linux-2.25-21.1
libblkid1-debuginfo-32bit-2.25-21.1
libuuid1-debuginfo-32bit-2.25-21.1
util-linux-systemd-debuginfo-2.25-21.1
python-libmount-debugsource-2.25-21.1
libmount1-32bit-2.25-21.1
libmount-devel-2.25-21.1
uuidd-2.25-21.1
libuuid1-debuginfo-2.25-21.1
libblkid1-32bit-2.25-21.1
libblkid1-2.25-21.1
libmount1-debuginfo-2.25-21.1
libblkid-devel-2.25-21.1

145757 - SuSE Linux 42.2 openSUSE-SU-2017:1502-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Description

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

openSUSE-SU-2017:1502-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00018.html>

SuSE Linux 42.2

x86_64

chromium-debuginfo-59.0.3071.86-104.15.1

chromedriver-debuginfo-59.0.3071.86-104.15.1

chromium-59.0.3071.86-104.15.1

chromedriver-59.0.3071.86-104.15.1

chromium-debugsource-59.0.3071.86-104.15.1

145758 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0146-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8010, CVE-2016-9566

Description

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

openSUSE-SU-2017:0146-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00078.html>

SuSE Linux 42.1

x86_64

icinga-idoutils-1.14.0-3.1

monitoring-tools-debuginfo-1.14.0-3.1

icinga-plugins-downtimes-1.14.0-3.1

icinga-doc-1.14.0-3.1

icinga-www-config-1.14.0-3.1

monitoring-tools-1.14.0-3.1

icinga-www-debuginfo-1.14.0-3.1

icinga-plugins-eventhandlers-1.14.0-3.1

icinga-www-1.14.0-3.1

icinga-idoutils-mysql-1.14.0-3.1

icinga-debuginfo-1.14.0-3.1

icinga-idoutils-pgsql-1.14.0-3.1

icinga-debugsource-1.14.0-3.1

icinga-1.14.0-3.1

icinga-idoutils-debuginfo-1.14.0-3.1

icinga-devel-1.14.0-3.1

icinga-idoutils-oracle-1.14.0-3.1

i586

icinga-idoutils-1.14.0-3.1

monitoring-tools-debuginfo-1.14.0-3.1

icinga-plugins-downtimes-1.14.0-3.1

icinga-doc-1.14.0-3.1

icinga-www-config-1.14.0-3.1

monitoring-tools-1.14.0-3.1

icinga-www-debuginfo-1.14.0-3.1

icinga-plugins-eventhandlers-1.14.0-3.1

icinga-www-1.14.0-3.1

icinga-idoutils-mysql-1.14.0-3.1

icinga-debuginfo-1.14.0-3.1

icinga-idoutils-pgsql-1.14.0-3.1
icinga-debugsource-1.14.0-3.1
icinga-1.14.0-3.1
icinga-idoutils-debuginfo-1.14.0-3.1
icinga-devel-1.14.0-3.1
icinga-idoutils-oracle-1.14.0-3.1

SuSE Linux 42.2

x86_64

icinga-plugins-eventhandlers-1.14.0-4.1
icinga-plugins-downtimes-1.14.0-4.1
icinga-idoutils-mysql-1.14.0-4.1
icinga-idoutils-pgsql-1.14.0-4.1
icinga-doc-1.14.0-4.1
icinga-idoutils-debuginfo-1.14.0-4.1
icinga-debugsource-1.14.0-4.1
icinga-idoutils-1.14.0-4.1
monitoring-tools-1.14.0-4.1
icinga-idoutils-oracle-1.14.0-4.1
icinga-www-debuginfo-1.14.0-4.1
icinga-devel-1.14.0-4.1
icinga-www-config-1.14.0-4.1
icinga-www-1.14.0-4.1
monitoring-tools-debuginfo-1.14.0-4.1
icinga-debuginfo-1.14.0-4.1
icinga-1.14.0-4.1

145759 - SuSE Linux 42.2 openSUSE-SU-2017:1698-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2581, CVE-2017-2586, CVE-2017-2587

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1698-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00105.html>

SuSE Linux 42.2

x86_64

netpbm-10.66.3-8.3.1
libnetpbm11-debuginfo-10.66.3-8.3.1
libnetpbm11-debuginfo-32bit-10.66.3-8.3.1
libnetpbm11-32bit-10.66.3-8.3.1
libnetpbm-devel-10.66.3-8.3.1
libnetpbm11-10.66.3-8.3.1
netpbm-debugsource-10.66.3-8.3.1
netpbm-debuginfo-10.66.3-8.3.1

i586

netpbm-10.66.3-8.3.1
libnetpbm11-debuginfo-10.66.3-8.3.1
libnetpbm-devel-10.66.3-8.3.1

libnetpbm11-10.66.3-8.3.1
netpbm-debugsource-10.66.3-8.3.1
netpbm-debuginfo-10.66.3-8.3.1

145761 - SuSE Linux 42.1 openSUSE-SU-2017:1215-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10318, CVE-2017-2671, CVE-2017-7187, CVE-2017-7261, CVE-2017-7294, CVE-2017-7308, CVE-2017-7616, CVE-2017-7618

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1215-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00031.html>

SuSE Linux 42.1

i586

kernel-obs-qa-4.1.39-56.1
kernel-default-4.1.39-56.1
kernel-default-devel-4.1.39-56.1
kernel-syms-4.1.39-56.1
kernel-default-base-4.1.39-56.1
kernel-obs-build-4.1.39-56.3
kernel-obs-build-debugsource-4.1.39-56.3
kernel-default-debugsource-4.1.39-56.1
kernel-default-debuginfo-4.1.39-56.1
kernel-default-base-debuginfo-4.1.39-56.1

i686

kernel-debug-devel-debuginfo-4.1.39-56.1
kernel-vanilla-debuginfo-4.1.39-56.1
kernel-xen-base-4.1.39-56.1
kernel-pae-base-4.1.39-56.1
kernel-ec2-debuginfo-4.1.39-56.1
kernel-pae-devel-4.1.39-56.1
kernel-ec2-base-4.1.39-56.1
kernel-vanilla-4.1.39-56.1
kernel-vanilla-debugsource-4.1.39-56.1
kernel-ec2-base-debuginfo-4.1.39-56.1
kernel-pv-4.1.39-56.1
kernel-xen-devel-4.1.39-56.1
kernel-ec2-4.1.39-56.1
kernel-pae-debugsource-4.1.39-56.1
kernel-xen-debuginfo-4.1.39-56.1
kernel-ec2-debugsource-4.1.39-56.1
kernel-xen-debugsource-4.1.39-56.1
kernel-ec2-devel-4.1.39-56.1
kernel-debug-debugsource-4.1.39-56.1
kernel-debug-debuginfo-4.1.39-56.1
kernel-vanilla-devel-4.1.39-56.1
kernel-xen-base-debuginfo-4.1.39-56.1
kernel-debug-devel-4.1.39-56.1

kernel-xen-4.1.39-56.1
kernel-pae-4.1.39-56.1
kernel-debug-base-debuginfo-4.1.39-56.1
kernel-pae-base-debuginfo-4.1.39-56.1
kernel-debug-4.1.39-56.1
kernel-pae-debuginfo-4.1.39-56.1
kernel-pv-base-debuginfo-4.1.39-56.1
kernel-pv-base-4.1.39-56.1
kernel-debug-base-4.1.39-56.1
kernel-pv-debugsource-4.1.39-56.1
kernel-pv-debuginfo-4.1.39-56.1
kernel-pv-devel-4.1.39-56.1

noarch

kernel-macros-4.1.39-56.1
kernel-docs-4.1.39-56.2
kernel-docs-html-4.1.39-56.2
kernel-source-vanilla-4.1.39-56.1
kernel-docs-pdf-4.1.39-56.2
kernel-devel-4.1.39-56.1
kernel-source-4.1.39-56.1

x86_64

kernel-obs-qa-4.1.39-56.1
kernel-debug-devel-debuginfo-4.1.39-56.1
kernel-syms-4.1.39-56.1
kernel-vanilla-debuginfo-4.1.39-56.1
kernel-default-base-4.1.39-56.1
kernel-xen-base-4.1.39-56.1
kernel-obs-build-debugsource-4.1.39-56.3
kernel-ec2-debuginfo-4.1.39-56.1
kernel-default-debuginfo-4.1.39-56.1
kernel-ec2-base-4.1.39-56.1
kernel-vanilla-4.1.39-56.1
kernel-vanilla-debugsource-4.1.39-56.1
kernel-ec2-base-debuginfo-4.1.39-56.1
kernel-pv-4.1.39-56.1
kernel-xen-devel-4.1.39-56.1
kernel-ec2-4.1.39-56.1
kernel-default-base-debuginfo-4.1.39-56.1
kernel-obs-build-4.1.39-56.3
kernel-xen-debuginfo-4.1.39-56.1
kernel-ec2-debugsource-4.1.39-56.1
kernel-xen-debugsource-4.1.39-56.1
kernel-default-debugsource-4.1.39-56.1
kernel-ec2-devel-4.1.39-56.1
kernel-debug-debugsource-4.1.39-56.1
kernel-debug-debuginfo-4.1.39-56.1
kernel-vanilla-devel-4.1.39-56.1
kernel-xen-base-debuginfo-4.1.39-56.1
kernel-debug-devel-4.1.39-56.1
kernel-xen-4.1.39-56.1
kernel-default-devel-4.1.39-56.1
kernel-debug-base-debuginfo-4.1.39-56.1
kernel-default-4.1.39-56.1
kernel-debug-4.1.39-56.1
kernel-pv-base-debuginfo-4.1.39-56.1
kernel-pv-base-4.1.39-56.1
kernel-debug-base-4.1.39-56.1
kernel-pv-debugsource-4.1.39-56.1

kernel-pv-debuginfo-4.1.39-56.1
kernel-pv-devel-4.1.39-56.1

145763 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1190-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5068

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1190-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00010.html>

SuSE Linux 42.1

x86_64

chromedriver-58.0.3029.96-114.1

chromium-debugsource-58.0.3029.96-114.1

chromium-58.0.3029.96-114.1

chromedriver-debuginfo-58.0.3029.96-114.1

chromium-debuginfo-58.0.3029.96-114.1

SuSE Linux 42.2

x86_64

chromedriver-debuginfo-58.0.3029.96-104.12.1

chromedriver-58.0.3029.96-104.12.1

chromium-debuginfo-58.0.3029.96-104.12.1

chromium-58.0.3029.96-104.12.1

chromium-debugsource-58.0.3029.96-104.12.1

145765 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0082-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5180

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0082-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00055.html>

SuSE Linux 42.1

x86_64

libcares2-32bit-1.9.1-5.1

libcares2-debuginfo-1.9.1-5.1

libcares2-debuginfo-32bit-1.9.1-5.1

libcares2-debugsource-1.9.1-5.1
libcares-devel-1.9.1-5.1
libcares2-1.9.1-5.1

i586
libcares-devel-1.9.1-5.1
libcares2-debuginfo-1.9.1-5.1
libcares2-debugsource-1.9.1-5.1
libcares2-1.9.1-5.1

SuSE Linux 42.2
x86_64
libcares2-1.9.1-6.1
libcares2-debugsource-1.9.1-6.1
libcares2-32bit-1.9.1-6.1
libcares2-debuginfo-32bit-1.9.1-6.1
libcares2-debuginfo-1.9.1-6.1
libcares-devel-1.9.1-6.1

i586
libcares-devel-1.9.1-6.1
libcares2-debuginfo-1.9.1-6.1
libcares2-debugsource-1.9.1-6.1
libcares2-1.9.1-6.1

145772 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:1958-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11406, CVE-2017-11407, CVE-2017-11408, CVE-2017-11410, CVE-2017-11411, CVE-2017-7702, CVE-2017-9350

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1958-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00090.html>

SuSE Linux 42.2
x86_64
wireshark-ui-gtk-2.2.8-14.9.1
wireshark-debugsource-2.2.8-14.9.1
wireshark-ui-qt-2.2.8-14.9.1
wireshark-ui-qt-debuginfo-2.2.8-14.9.1
wireshark-devel-2.2.8-14.9.1
wireshark-2.2.8-14.9.1
wireshark-debuginfo-2.2.8-14.9.1
wireshark-ui-gtk-debuginfo-2.2.8-14.9.1

SuSE Linux 42.3
x86_64
wireshark-ui-qt-debuginfo-2.2.8-17.1
wireshark-ui-gtk-2.2.8-17.1
wireshark-2.2.8-17.1
wireshark-debuginfo-2.2.8-17.1

wireshark-debugsource-2.2.8-17.1
wireshark-devel-2.2.8-17.1
wireshark-ui-qt-2.2.8-17.1
wireshark-ui-gtk-debuginfo-2.2.8-17.1

145774 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0514-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:0514-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00093.html>

SuSE Linux 42.1

i586

libfbembed-devel-2.5.6.27020-10.1
firebird-superserver-2.5.6.27020-10.1
firebird-classic-2.5.6.27020-10.1
firebird-2.5.6.27020-10.1
firebird-debugsource-2.5.6.27020-10.1
firebird-classic-debugsource-2.5.6.27020-10.1
firebird-debuginfo-2.5.6.27020-10.1
libfbembed2_5-debuginfo-2.5.6.27020-10.1
firebird-superserver-debuginfo-2.5.6.27020-10.1
libfbclient2-2.5.6.27020-10.1
firebird-devel-2.5.6.27020-10.1
firebird-classic-debuginfo-2.5.6.27020-10.1
libfbclient2-debuginfo-2.5.6.27020-10.1
libfbembed2_5-2.5.6.27020-10.1
libfbclient2-devel-2.5.6.27020-10.1

noarch

firebird-doc-2.5.6.27020-10.1

x86_64

libfbembed-devel-2.5.6.27020-10.1
firebird-superserver-2.5.6.27020-10.1
firebird-classic-2.5.6.27020-10.1
firebird-2.5.6.27020-10.1
firebird-debugsource-2.5.6.27020-10.1
firebird-classic-debugsource-2.5.6.27020-10.1
libfbembed2_5-debuginfo-32bit-2.5.6.27020-10.1
firebird-debuginfo-2.5.6.27020-10.1
firebird-debuginfo-32bit-2.5.6.27020-10.1
libfbembed2_5-debuginfo-2.5.6.27020-10.1
firebird-32bit-2.5.6.27020-10.1
firebird-superserver-debuginfo-2.5.6.27020-10.1
libfbclient2-2.5.6.27020-10.1
firebird-devel-2.5.6.27020-10.1
libfbembed2_5-32bit-2.5.6.27020-10.1

firebird-classic-debuginfo-2.5.6.27020-10.1
libfbclient2-debuginfo-32bit-2.5.6.27020-10.1
libfbclient2-debuginfo-2.5.6.27020-10.1
libfbclient2-32bit-2.5.6.27020-10.1
libfbembed2_5-2.5.6.27020-10.1
libfbclient2-devel-2.5.6.27020-10.1

SuSE Linux 42.2

i586

libfbembed-devel-2.5.6.27020-10.1
firebird-superserver-2.5.6.27020-10.1
firebird-classic-2.5.6.27020-10.1
firebird-2.5.6.27020-10.1
firebird-debugsource-2.5.6.27020-10.1
firebird-classic-debugsource-2.5.6.27020-10.1
firebird-debuginfo-2.5.6.27020-10.1
libfbembed2_5-debuginfo-2.5.6.27020-10.1
firebird-superserver-debuginfo-2.5.6.27020-10.1
libfbclient2-2.5.6.27020-10.1
firebird-devel-2.5.6.27020-10.1
firebird-classic-debuginfo-2.5.6.27020-10.1
libfbclient2-debuginfo-2.5.6.27020-10.1
libfbembed2_5-2.5.6.27020-10.1
libfbclient2-devel-2.5.6.27020-10.1

noarch

firebird-doc-2.5.6.27020-10.1

x86_64

libfbembed-devel-2.5.6.27020-10.1
firebird-superserver-2.5.6.27020-10.1
firebird-classic-2.5.6.27020-10.1
firebird-2.5.6.27020-10.1
firebird-debugsource-2.5.6.27020-10.1
firebird-classic-debugsource-2.5.6.27020-10.1
libfbembed2_5-debuginfo-32bit-2.5.6.27020-10.1
firebird-debuginfo-2.5.6.27020-10.1
firebird-debuginfo-32bit-2.5.6.27020-10.1
libfbembed2_5-debuginfo-2.5.6.27020-10.1
firebird-32bit-2.5.6.27020-10.1
firebird-superserver-debuginfo-2.5.6.27020-10.1
libfbclient2-2.5.6.27020-10.1
firebird-devel-2.5.6.27020-10.1
libfbembed2_5-32bit-2.5.6.27020-10.1
firebird-classic-debuginfo-2.5.6.27020-10.1
libfbclient2-debuginfo-32bit-2.5.6.27020-10.1
libfbclient2-debuginfo-2.5.6.27020-10.1
libfbclient2-32bit-2.5.6.27020-10.1
libfbembed2_5-2.5.6.27020-10.1
libfbclient2-devel-2.5.6.27020-10.1

145775 - SuSE Linux 42.2 openSUSE-SU-2017:0306-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9877

Description

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

openSUSE-SU-2017:0306-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00151.html>

SuSE Linux 42.2
x86_64
rabbitmq-server-3.5.8-3.2
rabbitmq-server-plugins-3.5.8-3.2
erlang-rabbitmq-client-3.5.8-3.2

145777 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0917-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0917-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00006.html>

SuSE Linux 42.1
x86_64
geotiff-debugsource-1.4.2-4.1
geotiff-debuginfo-1.4.2-4.1
geotiff-devel-1.4.2-4.1
libgeotiff2-debuginfo-1.4.2-4.1
geotiff-1.4.2-4.1
libgeotiff2-1.4.2-4.1

i586
geotiff-debugsource-1.4.2-4.1
geotiff-debuginfo-1.4.2-4.1
geotiff-devel-1.4.2-4.1
libgeotiff2-debuginfo-1.4.2-4.1
geotiff-1.4.2-4.1
libgeotiff2-1.4.2-4.1

SuSE Linux 42.2
x86_64
geotiff-debuginfo-1.4.2-4.3.1
geotiff-devel-1.4.2-4.3.1
geotiff-debugsource-1.4.2-4.3.1
libgeotiff2-1.4.2-4.3.1
geotiff-1.4.2-4.3.1
libgeotiff2-debuginfo-1.4.2-4.3.1

145781 - SuSE Linux 42.2 openSUSE-SU-2017:0958-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10190

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0958-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00031.html>

SuSE Linux 42.2

x86_64

libavresample3-debuginfo-32bit-3.2.4-6.3.1

libpostproc54-debuginfo-32bit-3.2.4-6.3.1

libavformat57-32bit-3.2.4-6.3.1

libavfilter6-debuginfo-3.2.4-6.3.1

libswscale4-32bit-3.2.4-6.3.1

libswscale4-debuginfo-32bit-3.2.4-6.3.1

libavutil55-debuginfo-3.2.4-6.3.1

libavcodec57-debuginfo-3.2.4-6.3.1

libavresample3-debuginfo-3.2.4-6.3.1

libswscale-devel-3.2.4-6.3.1

libavresample3-3.2.4-6.3.1

libpostproc-devel-3.2.4-6.3.1

libavcodec57-debuginfo-32bit-3.2.4-6.3.1

libswresample-devel-3.2.4-6.3.1

ffmpeg-debugsource-3.2.4-6.3.1

libavutil55-3.2.4-6.3.1

libavresample-devel-3.2.4-6.3.1

libavcodec-devel-3.2.4-6.3.1

libavformat57-debuginfo-32bit-3.2.4-6.3.1

libavutil-devel-3.2.4-6.3.1

libavfilter6-debuginfo-32bit-3.2.4-6.3.1

libavformat-devel-3.2.4-6.3.1

libpostproc54-32bit-3.2.4-6.3.1

libavdevice57-debuginfo-3.2.4-6.3.1

libswscale4-3.2.4-6.3.1

libavdevice57-32bit-3.2.4-6.3.1

libavcodec57-3.2.4-6.3.1

libswscale4-debuginfo-3.2.4-6.3.1

libavfilter6-3.2.4-6.3.1

libavfilter6-32bit-3.2.4-6.3.1

libavformat57-3.2.4-6.3.1

libavdevice-devel-3.2.4-6.3.1

libswresample2-debuginfo-3.2.4-6.3.1

libswresample2-3.2.4-6.3.1

libavfilter-devel-3.2.4-6.3.1

libavdevice57-3.2.4-6.3.1

libavcodec57-32bit-3.2.4-6.3.1

libavformat57-debuginfo-3.2.4-6.3.1

libpostproc54-3.2.4-6.3.1

libavresample3-32bit-3.2.4-6.3.1

ffmpeg-debuginfo-3.2.4-6.3.1

ffmpeg-3.2.4-6.3.1

libswresample2-debuginfo-32bit-3.2.4-6.3.1
libavdevice57-debuginfo-32bit-3.2.4-6.3.1
libswresample2-32bit-3.2.4-6.3.1
libpostproc54-debuginfo-3.2.4-6.3.1
libavutil55-debuginfo-32bit-3.2.4-6.3.1
libavutil55-32bit-3.2.4-6.3.1

i586

libavfilter6-debuginfo-3.2.4-6.3.1
libavutil55-debuginfo-3.2.4-6.3.1
libavcodec57-debuginfo-3.2.4-6.3.1
libavresample3-debuginfo-3.2.4-6.3.1
libswscale-devel-3.2.4-6.3.1
libavresample3-3.2.4-6.3.1
libpostproc-devel-3.2.4-6.3.1
libswresample-devel-3.2.4-6.3.1
ffmpeg-debugsource-3.2.4-6.3.1
libavutil55-3.2.4-6.3.1
libavresample-devel-3.2.4-6.3.1
libavcodec-devel-3.2.4-6.3.1
libavutil-devel-3.2.4-6.3.1
libavformat-devel-3.2.4-6.3.1
libavdevice57-debuginfo-3.2.4-6.3.1
libswscale4-3.2.4-6.3.1
libavcodec57-3.2.4-6.3.1
libswscale4-debuginfo-3.2.4-6.3.1
libavfilter6-3.2.4-6.3.1
libavformat57-3.2.4-6.3.1
libavdevice-devel-3.2.4-6.3.1
libswresample2-debuginfo-3.2.4-6.3.1
libswresample2-3.2.4-6.3.1
libavfilter-devel-3.2.4-6.3.1
libavdevice57-3.2.4-6.3.1
libavformat57-debuginfo-3.2.4-6.3.1
libpostproc54-3.2.4-6.3.1
ffmpeg-debuginfo-3.2.4-6.3.1
ffmpeg-3.2.4-6.3.1
libpostproc54-debuginfo-3.2.4-6.3.1

145783 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0815-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4570, CVE-2016-4571

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0815-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00081.html>

SuSE Linux 42.1

x86_64

libxml1-debuginfo-2.9-5.1

mxml-debuginfo-2.9-5.1
libmxml1-2.9-5.1
mxml-2.9-5.1
mxml-devel-2.9-5.1
mxml-debugsource-2.9-5.1
libmxml1-32bit-2.9-5.1
libmxml1-debuginfo-32bit-2.9-5.1

i586
libmxml1-debuginfo-2.9-5.1
mxml-debuginfo-2.9-5.1
libmxml1-2.9-5.1
mxml-2.9-5.1
mxml-devel-2.9-5.1
mxml-debugsource-2.9-5.1

SuSE Linux 42.2
x86_64
mxml-2.9-5.3.1
mxml-debugsource-2.9-5.3.1
mxml-devel-2.9-5.3.1
libmxml1-2.9-5.3.1
libmxml1-debuginfo-32bit-2.9-5.3.1
mxml-debuginfo-2.9-5.3.1
libmxml1-32bit-2.9-5.3.1
libmxml1-debuginfo-2.9-5.3.1

i586
mxml-2.9-5.3.1
mxml-debugsource-2.9-5.3.1
mxml-devel-2.9-5.3.1
libmxml1-2.9-5.3.1
mxml-debuginfo-2.9-5.3.1
libmxml1-debuginfo-2.9-5.3.1

145788 - SuSE Linux 42.2 openSUSE-SU-2017:0344-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-8858

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0344-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00178.html>

SuSE Linux 42.2
x86_64
openssh-7.2p2-9.1
openssh-debuginfo-7.2p2-9.1
openssh-helpers-debuginfo-7.2p2-9.1
openssh-askpass-gnome-7.2p2-9.1
openssh-helpers-7.2p2-9.1

openssh-cavs-7.2p2-9.1
openssh-fips-7.2p2-9.1
openssh-debugsource-7.2p2-9.1
openssh-askpass-gnome-debuginfo-7.2p2-9.1

i586

openssh-7.2p2-9.1
openssh-debuginfo-7.2p2-9.1
openssh-helpers-debuginfo-7.2p2-9.1
openssh-askpass-gnome-7.2p2-9.1
openssh-helpers-7.2p2-9.1
openssh-cavs-7.2p2-9.1
openssh-fips-7.2p2-9.1
openssh-debugsource-7.2p2-9.1
openssh-askpass-gnome-debuginfo-7.2p2-9.1

145789 - SuSE Linux 42.2 openSUSE-SU-2017:0287-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10156

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0287-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00145.html>

SuSE Linux 42.2

i586

nss-myhostname-228-22.1
udev-228-22.1
systemd-logger-228-22.1
libsystemd0-mini-debuginfo-228-22.1
systemd-mini-devel-228-22.1
udev-mini-228-22.1
libudev-mini-devel-228-22.1
libudev-mini1-debuginfo-228-22.1
nss-mymachines-debuginfo-228-22.1
nss-mymachines-228-22.1
systemd-mini-debuginfo-228-22.1
libsystemd0-debuginfo-228-22.1
libudev1-debuginfo-228-22.1
libudev-devel-228-22.1
libsystemd0-228-22.1
systemd-debugsource-228-22.1
nss-myhostname-debuginfo-228-22.1
libudev-mini1-228-22.1
systemd-mini-228-22.1
systemd-sysvinit-228-22.1
systemd-mini-debugsource-228-22.1
libsystemd0-mini-228-22.1
systemd-228-22.1
udev-debuginfo-228-22.1

udev-mini-debuginfo-228-22.1
libudev1-228-22.1
systemd-mini-sysvinit-228-22.1
systemd-debuginfo-228-22.1
systemd-devel-228-22.1

noarch
systemd-mini-bash-completion-228-22.1
systemd-bash-completion-228-22.1

x86_64
nss-myhostname-228-22.1
libsystemd0-debuginfo-32bit-228-22.1
udev-228-22.1
systemd-logger-228-22.1
systemd-32bit-228-22.1
libudev1-debuginfo-32bit-228-22.1
nss-myhostname-debuginfo-32bit-228-22.1
libsystemd0-mini-debuginfo-228-22.1
systemd-mini-devel-228-22.1
udev-mini-228-22.1
nss-myhostname-32bit-228-22.1
libudev-mini-devel-228-22.1
libudev-mini1-debuginfo-228-22.1
nss-mymachines-debuginfo-228-22.1
nss-mymachines-228-22.1
systemd-mini-debuginfo-228-22.1
libsystemd0-debuginfo-228-22.1
libudev1-debuginfo-228-22.1
libudev-devel-228-22.1
libsystemd0-228-22.1
systemd-debugsource-228-22.1
nss-myhostname-debuginfo-228-22.1
libudev-mini1-228-22.1
systemd-mini-228-22.1
systemd-sysvinit-228-22.1
systemd-mini-debugsource-228-22.1
libudev1-32bit-228-22.1
systemd-debuginfo-32bit-228-22.1
libsystemd0-mini-228-22.1
libsystemd0-32bit-228-22.1
systemd-228-22.1
udev-debuginfo-228-22.1
udev-mini-debuginfo-228-22.1
libudev1-228-22.1
systemd-mini-sysvinit-228-22.1
systemd-debuginfo-228-22.1
systemd-devel-228-22.1

145790 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0598-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9933, CVE-2016-9934, CVE-2016-9935

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0598-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00005.html>

SuSE Linux 42.1

i586

php5-ldap-5.5.14-75.1

php5-zip-5.5.14-75.1

php5-phar-debuginfo-5.5.14-75.1

php5-ftp-debuginfo-5.5.14-75.1

php5-bz2-5.5.14-75.1

php5-wddx-5.5.14-75.1

php5-intl-debuginfo-5.5.14-75.1

php5-bz2-debuginfo-5.5.14-75.1

php5-mysql-5.5.14-75.1

php5-dba-5.5.14-75.1

php5-enchanted-debuginfo-5.5.14-75.1

php5-exif-5.5.14-75.1

php5-gmp-5.5.14-75.1

php5-exif-debuginfo-5.5.14-75.1

php5-mssql-5.5.14-75.1

php5-xsl-debuginfo-5.5.14-75.1

php5-gettext-5.5.14-75.1

apache2-mod_php5-5.5.14-75.1

php5-sysvsem-5.5.14-75.1

php5-sysvmsg-5.5.14-75.1

php5-tokenizer-debuginfo-5.5.14-75.1

php5-fastcgi-debuginfo-5.5.14-75.1

php5-fpm-debuginfo-5.5.14-75.1

php5-sockets-debuginfo-5.5.14-75.1

php5-gettext-debuginfo-5.5.14-75.1

php5-readline-5.5.14-75.1

php5-tokenizer-5.5.14-75.1

php5-xmlreader-debuginfo-5.5.14-75.1

php5-pgsql-5.5.14-75.1

php5-soap-5.5.14-75.1

php5-debugsource-5.5.14-75.1

php5-xmlreader-5.5.14-75.1

php5-fileinfo-debuginfo-5.5.14-75.1

php5-dom-5.5.14-75.1

php5-enchanted-5.5.14-75.1

php5-ispell-5.5.14-75.1

php5-ldap-debuginfo-5.5.14-75.1

php5-firebird-5.5.14-75.1

php5-shmop-5.5.14-75.1

php5-gd-debuginfo-5.5.14-75.1

php5-mcrypt-5.5.14-75.1

php5-fileinfo-5.5.14-75.1

php5-pdo-5.5.14-75.1

php5-zip-debuginfo-5.5.14-75.1

php5-pcntl-5.5.14-75.1

php5-soap-debuginfo-5.5.14-75.1

php5-dom-debuginfo-5.5.14-75.1

php5-curl-debuginfo-5.5.14-75.1

php5-sysvsem-debuginfo-5.5.14-75.1

php5-firebird-debuginfo-5.5.14-75.1

php5-mbstring-debuginfo-5.5.14-75.1

php5-zlib-debuginfo-5.5.14-75.1

php5-devel-5.5.14-75.1
php5-mssql-debuginfo-5.5.14-75.1
php5-gd-5.5.14-75.1
php5-sysvmsg-debuginfo-5.5.14-75.1
php5-odbc-debuginfo-5.5.14-75.1
php5-xmlwriter-debuginfo-5.5.14-75.1
php5-xsl-5.5.14-75.1
php5-json-debuginfo-5.5.14-75.1
php5-zlib-5.5.14-75.1
php5-bcmath-5.5.14-75.1
php5-calendar-5.5.14-75.1
php5-json-5.5.14-75.1
php5-gmp-debuginfo-5.5.14-75.1
php5-sysvshm-5.5.14-75.1
php5-sysvshm-debuginfo-5.5.14-75.1
php5-xmlrpc-5.5.14-75.1
php5-iconv-5.5.14-75.1
php5-pcntl-debuginfo-5.5.14-75.1
php5-fastcgi-5.5.14-75.1
php5-intl-5.5.14-75.1
php5-posix-5.5.14-75.1
php5-fpm-5.5.14-75.1
php5-dba-debuginfo-5.5.14-75.1
php5-iconv-debuginfo-5.5.14-75.1
apache2-mod_php5-debuginfo-5.5.14-75.1
php5-shmop-debuginfo-5.5.14-75.1
php5-xmlrpc-debuginfo-5.5.14-75.1
php5-snmp-debuginfo-5.5.14-75.1
php5-tidy-5.5.14-75.1
php5-opcache-5.5.14-75.1
php5-opcache-debuginfo-5.5.14-75.1
php5-openssl-5.5.14-75.1
php5-curl-5.5.14-75.1
php5-mcrypt-debuginfo-5.5.14-75.1
php5-openssl-debuginfo-5.5.14-75.1
php5-pdo-debuginfo-5.5.14-75.1
php5-ctype-5.5.14-75.1
php5-sqlite-debuginfo-5.5.14-75.1
php5-pgsql-debuginfo-5.5.14-75.1
php5-suhosin-5.5.14-75.1
php5-bcmath-debuginfo-5.5.14-75.1
php5-posix-debuginfo-5.5.14-75.1
php5-suhosin-debuginfo-5.5.14-75.1
php5-5.5.14-75.1
php5-odbc-5.5.14-75.1
php5-ispell-debuginfo-5.5.14-75.1
php5-imap-debuginfo-5.5.14-75.1
php5-imap-5.5.14-75.1
php5-mysql-debuginfo-5.5.14-75.1
php5-ctype-debuginfo-5.5.14-75.1
php5-debuginfo-5.5.14-75.1
php5-ftp-5.5.14-75.1
php5-phar-5.5.14-75.1
php5-readline-debuginfo-5.5.14-75.1
php5-sockets-5.5.14-75.1
php5-mbstring-5.5.14-75.1
php5-wddx-debuginfo-5.5.14-75.1
php5-snmp-5.5.14-75.1
php5-sqlite-5.5.14-75.1
php5-tidy-debuginfo-5.5.14-75.1

php5-xmlwriter-5.5.14-75.1
php5-calendar-debuginfo-5.5.14-75.1

noarch
php5-pear-5.5.14-75.1

x86_64
php5-ldap-5.5.14-75.1
php5-zip-5.5.14-75.1
php5-phar-debuginfo-5.5.14-75.1
php5-ftp-debuginfo-5.5.14-75.1
php5-bz2-5.5.14-75.1
php5-wddx-5.5.14-75.1
php5-intl-debuginfo-5.5.14-75.1
php5-bz2-debuginfo-5.5.14-75.1
php5-mysql-5.5.14-75.1
php5-dba-5.5.14-75.1
php5-enchanted-debuginfo-5.5.14-75.1
php5-exif-5.5.14-75.1
php5-gmp-5.5.14-75.1
php5-exif-debuginfo-5.5.14-75.1
php5-mssql-5.5.14-75.1
php5-xsl-debuginfo-5.5.14-75.1
php5-gettext-5.5.14-75.1
apache2-mod_php5-5.5.14-75.1
php5-sysvsem-5.5.14-75.1
php5-sysvmsg-5.5.14-75.1
php5-tokenizer-debuginfo-5.5.14-75.1
php5-fastcgi-debuginfo-5.5.14-75.1
php5-fpm-debuginfo-5.5.14-75.1
php5-sockets-debuginfo-5.5.14-75.1
php5-gettext-debuginfo-5.5.14-75.1
php5-readline-5.5.14-75.1
php5-tokenizer-5.5.14-75.1
php5-xmlreader-debuginfo-5.5.14-75.1
php5-pgsql-5.5.14-75.1
php5-soap-5.5.14-75.1
php5-debugsource-5.5.14-75.1
php5-xmlreader-5.5.14-75.1
php5-fileinfo-debuginfo-5.5.14-75.1
php5-dom-5.5.14-75.1
php5-enchanted-5.5.14-75.1
php5-ispell-5.5.14-75.1
php5-ldap-debuginfo-5.5.14-75.1
php5-firebird-5.5.14-75.1
php5-shmop-5.5.14-75.1
php5-gd-debuginfo-5.5.14-75.1
php5-mcrypt-5.5.14-75.1
php5-fileinfo-5.5.14-75.1
php5-pdo-5.5.14-75.1
php5-zip-debuginfo-5.5.14-75.1
php5-pcntl-5.5.14-75.1
php5-soap-debuginfo-5.5.14-75.1
php5-dom-debuginfo-5.5.14-75.1
php5-curl-debuginfo-5.5.14-75.1
php5-sysvsem-debuginfo-5.5.14-75.1
php5-firebird-debuginfo-5.5.14-75.1
php5-mbstring-debuginfo-5.5.14-75.1
php5-zlib-debuginfo-5.5.14-75.1
php5-devel-5.5.14-75.1

php5-mssql-debuginfo-5.5.14-75.1
php5-gd-5.5.14-75.1
php5-sysvmsg-debuginfo-5.5.14-75.1
php5-odbc-debuginfo-5.5.14-75.1
php5-xmlwriter-debuginfo-5.5.14-75.1
php5-xsl-5.5.14-75.1
php5-json-debuginfo-5.5.14-75.1
php5-zlib-5.5.14-75.1
php5-bcmath-5.5.14-75.1
php5-calendar-5.5.14-75.1
php5-json-5.5.14-75.1
php5-gmp-debuginfo-5.5.14-75.1
php5-sysvshm-5.5.14-75.1
php5-sysvshm-debuginfo-5.5.14-75.1
php5-xmlrpc-5.5.14-75.1
php5-iconv-5.5.14-75.1
php5-pcntl-debuginfo-5.5.14-75.1
php5-fastcgi-5.5.14-75.1
php5-intl-5.5.14-75.1
php5-posix-5.5.14-75.1
php5-fpm-5.5.14-75.1
php5-dba-debuginfo-5.5.14-75.1
php5-iconv-debuginfo-5.5.14-75.1
apache2-mod_php5-debuginfo-5.5.14-75.1
php5-shmop-debuginfo-5.5.14-75.1
php5-xmlrpc-debuginfo-5.5.14-75.1
php5-snmp-debuginfo-5.5.14-75.1
php5-tidy-5.5.14-75.1
php5-opcache-5.5.14-75.1
php5-opcache-debuginfo-5.5.14-75.1
php5-openssl-5.5.14-75.1
php5-curl-5.5.14-75.1
php5-mcrypt-debuginfo-5.5.14-75.1
php5-openssl-debuginfo-5.5.14-75.1
php5-pdo-debuginfo-5.5.14-75.1
php5-ctype-5.5.14-75.1
php5-sqlite-debuginfo-5.5.14-75.1
php5-pgsql-debuginfo-5.5.14-75.1
php5-suhosin-5.5.14-75.1
php5-bcmath-debuginfo-5.5.14-75.1
php5-posix-debuginfo-5.5.14-75.1
php5-suhosin-debuginfo-5.5.14-75.1
php5-5.5.14-75.1
php5-odbc-5.5.14-75.1
php5-ispell-debuginfo-5.5.14-75.1
php5-imap-debuginfo-5.5.14-75.1
php5-imap-5.5.14-75.1
php5-mysql-debuginfo-5.5.14-75.1
php5-ctype-debuginfo-5.5.14-75.1
php5-debuginfo-5.5.14-75.1
php5-ftp-5.5.14-75.1
php5-phar-5.5.14-75.1
php5-readline-debuginfo-5.5.14-75.1
php5-sockets-5.5.14-75.1
php5-mbstring-5.5.14-75.1
php5-wddx-debuginfo-5.5.14-75.1
php5-snmp-5.5.14-75.1
php5-sqlite-5.5.14-75.1
php5-tidy-debuginfo-5.5.14-75.1
php5-xmlwriter-5.5.14-75.1

php5-calendar-debuginfo-5.5.14-75.1

SuSE Linux 42.2

i586

php5-mssql-debuginfo-5.5.14-75.2

php5-iconv-5.5.14-75.2

php5-json-5.5.14-75.2

php5-phar-debuginfo-5.5.14-75.2

php5-zlib-5.5.14-75.2

php5-zip-debuginfo-5.5.14-75.2

php5-mbstring-debuginfo-5.5.14-75.2

php5-suhosin-debuginfo-5.5.14-75.2

145792 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2192-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7467

Description

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

openSUSE-SU-2017:2192-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00069.html>

SuSE Linux 42.2

x86_64

minicom-debugsource-2.7-5.3.1

minicom-2.7-5.3.1

minicom-debuginfo-2.7-5.3.1

noarch

minicom-lang-2.7-5.3.1

SuSE Linux 42.3

x86_64

minicom-debugsource-2.7-8.1

minicom-debuginfo-2.7-8.1

minicom-2.7-8.1

noarch

minicom-lang-2.7-8.1

145794 - SuSE SLED 12 SP3 SUSE-SU-2017:2315-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8947, CVE-2016-10327, CVE-2016-2052, CVE-2017-7870, CVE-2017-7882, CVE-2017-8358, CVE-2017-9433

Description

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

SUSE-SU-2017:2315-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003174.html>

SuSE SLED 12 SP3

x86_64

libreoffice-officebean-debuginfo-5.3.5.2-43.5.4
libreoffice-writer-5.3.5.2-43.5.4
myspell-lightproof-pt_BR-20170511-16.2.1
libreoffice-base-drivers-mysql-debuginfo-5.3.5.2-43.5.4
libstaroffice-0_0-0-debuginfo-0.0.3-4.1
libreoffice-base-debuginfo-5.3.5.2-43.5.4
libreoffice-mailmerge-5.3.5.2-43.5.4
libreoffice-base-5.3.5.2-43.5.4
libreoffice-calc-extensions-5.3.5.2-43.5.4
libmwaw-0_3-3-0.3.11-7.5.1
libreoffice-writer-extensions-5.3.5.2-43.5.4
libreoffice-filters-optional-5.3.5.2-43.5.4
libreofficekit-5.3.5.2-43.5.4
myspell-lightproof-ru_RU-20170511-16.2.1
libzmf-0_0-0-0.0.1-4.1
libreoffice-calc-debuginfo-5.3.5.2-43.5.4
myspell-dictionaries-20170511-16.2.1
liborcus-0_12-0-0.12.1-10.5.1
libreoffice-draw-debuginfo-5.3.5.2-43.5.4
libreoffice-math-5.3.5.2-43.5.4
libreoffice-impress-debuginfo-5.3.5.2-43.5.4
libreoffice-base-drivers-postgresql-5.3.5.2-43.5.4
libreoffice-base-drivers-mysql-5.3.5.2-43.5.4
libmwaw-0_3-3-debuginfo-0.3.11-7.5.1
libreoffice-officebean-5.3.5.2-43.5.4
libixion-0_12-0-0.12.1-13.2.1
libixion-debugsource-0.12.1-13.2.1
libreoffice-gnome-debuginfo-5.3.5.2-43.5.4
libreoffice-debuginfo-5.3.5.2-43.5.4
libreoffice-math-debuginfo-5.3.5.2-43.5.4
libreoffice-debugsource-5.3.5.2-43.5.4
myspell-lightproof-en-20170511-16.2.1
libzmf-debugsource-0.0.1-4.1
libstaroffice-debugsource-0.0.3-4.1
libreoffice-writer-debuginfo-5.3.5.2-43.5.4
liborcus-debugsource-0.12.1-10.5.1
libreoffice-pyuno-debuginfo-5.3.5.2-43.5.4
libreoffice-pyuno-5.3.5.2-43.5.4
libreoffice-impress-5.3.5.2-43.5.4
myspell-lightproof-hu_HU-20170511-16.2.1
libstaroffice-0_0-0-0.0.3-4.1
libreoffice-gnome-5.3.5.2-43.5.4
libixion-0_12-0-debuginfo-0.12.1-13.2.1
liborcus-0_12-0-debuginfo-0.12.1-10.5.1
libmwaw-debugsource-0.3.11-7.5.1
libreoffice-5.3.5.2-43.5.4
libreoffice-draw-5.3.5.2-43.5.4
libreoffice-base-drivers-postgresql-debuginfo-5.3.5.2-43.5.4
libreoffice-calc-5.3.5.2-43.5.4
libzmf-0_0-0-debuginfo-0.0.1-4.1

noarch

myspell-es_BO-20170511-16.2.1
libreoffice-l10n-gu-5.3.5.2-43.5.4
myspell-ro_RO-20170511-16.2.1
myspell-es_CL-20170511-16.2.1
libreoffice-l10n-it-5.3.5.2-43.5.4
myspell-en_GH-20170511-16.2.1
myspell-en_BS-20170511-16.2.1
myspell-sv_FI-20170511-16.2.1
myspell-zu_ZA-20170511-16.2.1
myspell-es_CO-20170511-16.2.1
myspell-uk_UA-20170511-16.2.1
myspell-en_JM-20170511-16.2.1
myspell-en_PH-20170511-16.2.1
myspell-en_IN-20170511-16.2.1
myspell-es_PA-20170511-16.2.1
myspell-ar_AE-20170511-16.2.1
myspell-pt_PT-20170511-16.2.1
myspell-es_PY-20170511-16.2.1
myspell-ar_SD-20170511-16.2.1
myspell-ar_SA-20170511-16.2.1
myspell-te-20170511-16.2.1
myspell-ar_SY-20170511-16.2.1
myspell-bs_BA-20170511-16.2.1
myspell-sr_CS-20170511-16.2.1
libreoffice-icon-theme-galaxy-5.3.5.2-43.5.4
libreoffice-l10n-fr-5.3.5.2-43.5.4
myspell-es_DO-20170511-16.2.1
myspell-en_AU-20170511-16.2.1
libreoffice-l10n-ko-5.3.5.2-43.5.4
myspell-gu_IN-20170511-16.2.1
myspell-sv_SE-20170511-16.2.1
myspell-ru_RU-20170511-16.2.1
libreoffice-l10n-af-5.3.5.2-43.5.4
myspell-en_CA-20170511-16.2.1
myspell-fr_FR-20170511-16.2.1
libreoffice-l10n-da-5.3.5.2-43.5.4
myspell-pt_AO-20170511-16.2.1
myspell-bn_BD-20170511-16.2.1
myspell-sk_SK-20170511-16.2.1
myspell-en_US-20170511-16.2.1
myspell-ca_FR-20170511-16.2.1
libreoffice-l10n-pt_PT-5.3.5.2-43.5.4
libreoffice-l10n-bg-5.3.5.2-43.5.4
myspell-ar_OM-20170511-16.2.1
myspell-th_TH-20170511-16.2.1
myspell-es_VE-20170511-16.2.1
myspell-ar_DZ-20170511-16.2.1
myspell-ar_JO-20170511-16.2.1
myspell-vi_VN-20170511-16.2.1
myspell-de_CH-20170511-16.2.1
myspell-ar_LB-20170511-16.2.1
myspell-cs_CZ-20170511-16.2.1
myspell-da_DK-20170511-16.2.1
myspell-no-20170511-16.2.1
myspell-es_UY-20170511-16.2.1
myspell-vi-20170511-16.2.1
libreoffice-l10n-ca-5.3.5.2-43.5.4
myspell-ar_KW-20170511-16.2.1
myspell-es_CR-20170511-16.2.1
libreoffice-l10n-hr-5.3.5.2-43.5.4

myspell-el_GR-20170511-16.2.1
libreoffice-l10n-hi-5.3.5.2-43.5.4
myspell-es_CU-20170511-16.2.1
myspell-sr_Latn_RS-20170511-16.2.1
myspell-et_EE-20170511-16.2.1
libreoffice-l10n-zu-5.3.5.2-43.5.4
myspell-es_EC-20170511-16.2.1
myspell-be_BY-20170511-16.2.1
myspell-es_GT-20170511-16.2.1
myspell-es_SV-20170511-16.2.1
myspell-en_MW-20170511-16.2.1
myspell-sr_Latn_CS-20170511-16.2.1
myspell-lt_LT-20170511-16.2.1
myspell-pt_BR-20170511-16.2.1
myspell-es_ES-20170511-16.2.1
libreoffice-l10n-pt_BR-5.3.5.2-43.5.4
myspell-en_ZA-20170511-16.2.1
myspell-hi_IN-20170511-16.2.1
myspell-es_HN-20170511-16.2.1
myspell-ca_ES-20170511-16.2.1
myspell-ca-20170511-16.2.1
myspell-en_GB-20170511-16.2.1
libreoffice-l10n-zh_TW-5.3.5.2-43.5.4
libreoffice-l10n-nn-5.3.5.2-43.5.4
myspell-en_ZW-20170511-16.2.1
libreoffice-l10n-ro-5.3.5.2-43.5.4
myspell-ar_TN-20170511-16.2.1
libreoffice-l10n-ru-5.3.5.2-43.5.4
myspell-ca_IT-20170511-16.2.1
myspell-ca_AD-20170511-16.2.1
libreoffice-l10n-it-5.3.5.2-43.5.4
myspell-pl_PL-20170511-16.2.1
myspell-te_IN-20170511-16.2.1
myspell-en_BZ-20170511-16.2.1
myspell-fr_MC-20170511-16.2.1
myspell-ar_QA-20170511-16.2.1
libreoffice-l10n-de-5.3.5.2-43.5.4
myspell-sr-20170511-16.2.1
myspell-ca_ES_valencia-20170511-16.2.1
myspell-fr_BE-20170511-16.2.1
myspell-lv_LV-20170511-16.2.1
libreoffice-l10n-fi-5.3.5.2-43.5.4
myspell-nl_NL-20170511-16.2.1
myspell-lo_LA-20170511-16.2.1
libreoffice-l10n-uk-5.3.5.2-43.5.4
myspell-es_NI-20170511-16.2.1
myspell-es-20170511-16.2.1
libreoffice-icon-theme-tango-5.3.5.2-43.5.4
myspell-bg_BG-20170511-16.2.1
myspell-nn_NO-20170511-16.2.1
myspell-it_IT-20170511-16.2.1
libreoffice-l10n-ja-5.3.5.2-43.5.4
libreoffice-l10n-ar-5.3.5.2-43.5.4
myspell-nl_BE-20170511-16.2.1
myspell-en_IE-20170511-16.2.1
myspell-en_NA-20170511-16.2.1
libreoffice-l10n-zh_CN-5.3.5.2-43.5.4
myspell-bs-20170511-16.2.1
myspell-ar_BH-20170511-16.2.1
myspell-de-20170511-16.2.1

myspell-de_DE-20170511-16.2.1
myspell-en_TT-20170511-16.2.1
myspell-hu_HU-20170511-16.2.1
myspell-nb_NO-20170511-16.2.1
myspell-es_MX-20170511-16.2.1
myspell-sr_RS-20170511-16.2.1
myspell-ro-20170511-16.2.1
myspell-af_NA-20170511-16.2.1
myspell-fr_LU-20170511-16.2.1
myspell-fr_CA-20170511-16.2.1
myspell-es_AR-20170511-16.2.1
myspell-de_AT-20170511-16.2.1
myspell-ar_YE-20170511-16.2.1
libreoffice-l10n-sk-5.3.5.2-43.5.4
libreoffice-l10n-nl-5.3.5.2-43.5.4
myspell-en_NZ-20170511-16.2.1
libreoffice-l10n-en-5.3.5.2-43.5.4
myspell-sl_SI-20170511-16.2.1
libreoffice-l10n-pl-5.3.5.2-43.5.4
myspell-fr_CH-20170511-16.2.1
myspell-ar_IQ-20170511-16.2.1
myspell-es_PE-20170511-16.2.1
myspell-en-20170511-16.2.1
libreoffice-l10n-xh-5.3.5.2-43.5.4
libreoffice-l10n-nb-5.3.5.2-43.5.4
myspell-ar-20170511-16.2.1
myspell-af_ZA-20170511-16.2.1
myspell-ar_MA-20170511-16.2.1
myspell-es_PR-20170511-16.2.1
myspell-ar_LY-20170511-16.2.1
myspell-hr_HR-20170511-16.2.1
myspell-bn_IN-20170511-16.2.1
myspell-he_IL-20170511-16.2.1
libreoffice-l10n-es-5.3.5.2-43.5.4
myspell-ar_EG-20170511-16.2.1
libreoffice-l10n-hu-5.3.5.2-43.5.4

145795 - SuSE Linux 42.1 openSUSE-SU-2017:0547-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5897, CVE-2017-5970, CVE-2017-5986, CVE-2017-6074

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0547-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00100.html>

SuSE Linux 42.1

i586

kernel-default-base-debuginfo-4.1.38-50.1

kernel-default-debugsource-4.1.38-50.1

kernel-obs-build-4.1.38-50.2

kernel-syms-4.1.38-50.1
kernel-obs-qa-4.1.38-50.1
kernel-default-base-4.1.38-50.1
kernel-default-4.1.38-50.1
kernel-default-devel-4.1.38-50.1
kernel-default-debuginfo-4.1.38-50.1
kernel-obs-build-debugsource-4.1.38-50.2

i686

kernel-ec2-base-4.1.38-50.1
kernel-debug-base-debuginfo-4.1.38-50.1
kernel-pv-debugsource-4.1.38-50.1
kernel-pv-4.1.38-50.1
kernel-vanilla-debuginfo-4.1.38-50.1
kernel-xen-4.1.38-50.1
kernel-pae-base-debuginfo-4.1.38-50.1
kernel-pv-devel-4.1.38-50.1
kernel-debug-base-4.1.38-50.1
kernel-ec2-4.1.38-50.1
kernel-debug-devel-4.1.38-50.1
kernel-debug-devel-debuginfo-4.1.38-50.1
kernel-ec2-debugsource-4.1.38-50.1
kernel-xen-debugsource-4.1.38-50.1
kernel-xen-devel-4.1.38-50.1
kernel-debug-debugsource-4.1.38-50.1
kernel-debug-debuginfo-4.1.38-50.1
kernel-debug-4.1.38-50.1
kernel-xen-base-4.1.38-50.1
kernel-vanilla-debugsource-4.1.38-50.1
kernel-ec2-debuginfo-4.1.38-50.1
kernel-pv-debuginfo-4.1.38-50.1
kernel-pae-4.1.38-50.1
kernel-ec2-devel-4.1.38-50.1
kernel-vanilla-4.1.38-50.1
kernel-pae-debugsource-4.1.38-50.1
kernel-pv-base-debuginfo-4.1.38-50.1
kernel-pv-base-4.1.38-50.1
kernel-xen-debuginfo-4.1.38-50.1
kernel-vanilla-devel-4.1.38-50.1
kernel-pae-debuginfo-4.1.38-50.1
kernel-ec2-base-debuginfo-4.1.38-50.1
kernel-pae-base-4.1.38-50.1
kernel-xen-base-debuginfo-4.1.38-50.1
kernel-pae-devel-4.1.38-50.1

noarch

kernel-source-vanilla-4.1.38-50.1
kernel-devel-4.1.38-50.1
kernel-docs-4.1.38-50.3
kernel-source-4.1.38-50.1
kernel-macros-4.1.38-50.1
kernel-docs-html-4.1.38-50.3
kernel-docs-pdf-4.1.38-50.3

x86_64

kernel-ec2-base-4.1.38-50.1
kernel-default-debugsource-4.1.38-50.1
kernel-obs-build-debugsource-4.1.38-50.2
kernel-pv-4.1.38-50.1
kernel-vanilla-debuginfo-4.1.38-50.1

kernel-xen-4.1.38-50.1
kernel-pv-devel-4.1.38-50.1
kernel-debug-base-4.1.38-50.1
kernel-debug-base-debuginfo-4.1.38-50.1
kernel-ec2-4.1.38-50.1
kernel-debug-devel-4.1.38-50.1
kernel-debug-devel-debuginfo-4.1.38-50.1
kernel-ec2-debugsource-4.1.38-50.1
kernel-xen-debugsource-4.1.38-50.1
kernel-xen-devel-4.1.38-50.1
kernel-debug-debugsource-4.1.38-50.1
kernel-debug-debuginfo-4.1.38-50.1
kernel-default-debuginfo-4.1.38-50.1
kernel-syms-4.1.38-50.1
kernel-obs-build-4.1.38-50.2
kernel-default-base-debuginfo-4.1.38-50.1
kernel-xen-base-4.1.38-50.1
kernel-vanilla-debugsource-4.1.38-50.1
kernel-ec2-debuginfo-4.1.38-50.1
kernel-pv-debuginfo-4.1.38-50.1
kernel-ec2-devel-4.1.38-50.1
kernel-vanilla-4.1.38-50.1
kernel-vanilla-devel-4.1.38-50.1
kernel-pv-base-debuginfo-4.1.38-50.1
kernel-pv-base-4.1.38-50.1
kernel-debug-4.1.38-50.1
kernel-default-base-4.1.38-50.1
kernel-xen-debuginfo-4.1.38-50.1
kernel-obs-qa-4.1.38-50.1
kernel-pv-debugsource-4.1.38-50.1
kernel-ec2-base-debuginfo-4.1.38-50.1
kernel-default-devel-4.1.38-50.1
kernel-xen-base-debuginfo-4.1.38-50.1
kernel-default-4.1.38-50.1

145798 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1196-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5416, CVE-2017-5418, CVE-2017-5419, CVE-2017-5421, CVE-2017-5422, CVE-2017-5426, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1196-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00016.html>

SuSE Linux 42.1

x86_64
MozillaThunderbird-translations-other-52.1.0-42.1
MozillaThunderbird-52.1.0-42.1
MozillaThunderbird-debuginfo-52.1.0-42.1
MozillaThunderbird-translations-common-52.1.0-42.1
MozillaThunderbird-debugsource-52.1.0-42.1
MozillaThunderbird-devel-52.1.0-42.1
MozillaThunderbird-buildsymbols-52.1.0-42.1

SuSE Linux 42.2

x86_64
MozillaThunderbird-devel-52.1.0-41.3.1
MozillaThunderbird-debuginfo-52.1.0-41.3.1
MozillaThunderbird-buildsymbols-52.1.0-41.3.1
MozillaThunderbird-debugsource-52.1.0-41.3.1
MozillaThunderbird-translations-other-52.1.0-41.3.1
MozillaThunderbird-translations-common-52.1.0-41.3.1
MozillaThunderbird-52.1.0-41.3.1

i586

MozillaThunderbird-devel-52.1.0-41.3.1
MozillaThunderbird-debuginfo-52.1.0-41.3.1
MozillaThunderbird-buildsymbols-52.1.0-41.3.1
MozillaThunderbird-debugsource-52.1.0-41.3.1
MozillaThunderbird-translations-other-52.1.0-41.3.1
MozillaThunderbird-translations-common-52.1.0-41.3.1
MozillaThunderbird-52.1.0-41.3.1

145801 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1199-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8767, CVE-2014-8768, CVE-2014-8769, CVE-2015-0261, CVE-2015-2153, CVE-2015-2154, CVE-2015-2155, CVE-2015-3138, CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5341, CVE-2017-5342, CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1199-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00018.html>

SuSE Linux 42.1

x86_64
libpcap1-debuginfo-1.8.1-8.1
libpcap-devel-32bit-1.8.1-8.1
tcpdump-debuginfo-4.9.0-7.1
libpcap-devel-static-1.8.1-8.1
libpcap-debugsource-1.8.1-8.1
libpcap1-debuginfo-32bit-1.8.1-8.1

tcpdump-4.9.0-7.1
libpcap-devel-1.8.1-8.1
libpcap1-1.8.1-8.1
tcpdump-debugsource-4.9.0-7.1
libpcap1-32bit-1.8.1-8.1

i586
libpcap1-debuginfo-1.8.1-8.1
tcpdump-debuginfo-4.9.0-7.1
libpcap-devel-static-1.8.1-8.1
libpcap-debugsource-1.8.1-8.1
tcpdump-4.9.0-7.1
libpcap-devel-1.8.1-8.1
libpcap1-1.8.1-8.1
tcpdump-debugsource-4.9.0-7.1

SuSE Linux 42.2
x86_64
libpcap1-1.8.1-7.3.1
libpcap-devel-static-1.8.1-7.3.1
libpcap-debugsource-1.8.1-7.3.1
tcpdump-debugsource-4.9.0-6.3.1
libpcap-devel-1.8.1-7.3.1
tcpdump-4.9.0-6.3.1
libpcap1-32bit-1.8.1-7.3.1
libpcap1-debuginfo-32bit-1.8.1-7.3.1
libpcap1-debuginfo-1.8.1-7.3.1
tcpdump-debuginfo-4.9.0-6.3.1
libpcap-devel-32bit-1.8.1-7.3.1

i586
libpcap-devel-static-1.8.1-7.3.1
libpcap-debugsource-1.8.1-7.3.1
libpcap1-debuginfo-1.8.1-7.3.1
libpcap1-1.8.1-7.3.1
libpcap-devel-1.8.1-7.3.1

145803 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1127-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10324, CVE-2016-10325, CVE-2016-10326, CVE-2017-7853

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1127-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00109.html>

SuSE Linux 42.1
x86_64
libosip2-debugsource-4.1.0-5.1
libosip2-4.1.0-5.1
libosip2-debuginfo-4.1.0-5.1

libosip2-devel-4.1.0-5.1

i586

libosip2-debugsource-4.1.0-5.1

libosip2-4.1.0-5.1

libosip2-debuginfo-4.1.0-5.1

libosip2-devel-4.1.0-5.1

SuSE Linux 42.2

x86_64

libosip2-4.1.0-5.3.1

libosip2-debugsource-4.1.0-5.3.1

libosip2-devel-4.1.0-5.3.1

libosip2-debuginfo-4.1.0-5.3.1

145804 - SuSE Linux 42.2 openSUSE-SU-2017:0541-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5897, CVE-2017-5970, CVE-2017-5986, CVE-2017-6074

Description

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

openSUSE-SU-2017:0541-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00098.html>

SuSE Linux 42.2

x86_64

kernel-debug-devel-debuginfo-4.4.49-16.1

kernel-default-base-4.4.49-16.1

kernel-vanilla-debuginfo-4.4.49-16.1

kernel-vanilla-devel-4.4.49-16.1

kernel-syms-4.4.49-16.1

kernel-debug-4.4.49-16.1

kernel-debug-devel-4.4.49-16.1

kernel-default-base-debuginfo-4.4.49-16.1

kernel-vanilla-debugsource-4.4.49-16.1

kernel-default-devel-4.4.49-16.1

kernel-obs-build-debugsource-4.4.49-16.1

kernel-obs-qa-4.4.49-16.1

kernel-default-4.4.49-16.1

kernel-default-debuginfo-4.4.49-16.1

kernel-debug-base-4.4.49-16.1

kernel-vanilla-base-debuginfo-4.4.49-16.1

kernel-debug-base-debuginfo-4.4.49-16.1

kernel-default-debugsource-4.4.49-16.1

kernel-vanilla-4.4.49-16.1

kernel-vanilla-base-4.4.49-16.1

kernel-obs-build-4.4.49-16.1

kernel-debug-debugsource-4.4.49-16.1

kernel-debug-debuginfo-4.4.49-16.1

noarch

kernel-docs-pdf-4.4.49-16.2
kernel-macros-4.4.49-16.1
kernel-source-4.4.49-16.1
kernel-docs-4.4.49-16.2
kernel-source-vanilla-4.4.49-16.1
kernel-devel-4.4.49-16.1
kernel-docs-html-4.4.49-16.2

145805 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1139-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7875

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1139-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00000.html>

SuSE Linux 42.1
x86_64
feh-2.13.1-6.1
feh-debuginfo-2.13.1-6.1
feh-debugsource-2.13.1-6.1

i586
feh-2.13.1-6.1
feh-debuginfo-2.13.1-6.1
feh-debugsource-2.13.1-6.1

SuSE Linux 42.2
x86_64
feh-2.18.3-6.3.1
feh-debuginfo-2.18.3-6.3.1
feh-debugsource-2.18.3-6.3.1

i586
feh-2.18.3-6.3.1
feh-debuginfo-2.18.3-6.3.1
feh-debugsource-2.18.3-6.3.1

145806 - SuSE Linux 42.2 openSUSE-SU-2017:0071-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9807, CVE-2016-9808, CVE-2016-9810

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0071-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00044.html>

SuSE Linux 42.2

i586

gststreamer-plugins-good-extra-1.8.3-3.1
gststreamer-plugins-good-debugsource-1.8.3-3.1
gststreamer-plugins-good-doc-1.8.3-3.1
gststreamer-plugins-good-extra-debuginfo-1.8.3-3.1
gststreamer-plugins-good-debuginfo-1.8.3-3.1
gststreamer-plugins-good-1.8.3-3.1

noarch

gststreamer-plugins-good-lang-1.8.3-3.1

x86_64

gststreamer-plugins-good-extra-1.8.3-3.1
gststreamer-plugins-good-extra-32bit-1.8.3-3.1
gststreamer-plugins-good-debugsource-1.8.3-3.1
gststreamer-plugins-good-doc-1.8.3-3.1
gststreamer-plugins-good-extra-debuginfo-1.8.3-3.1
gststreamer-plugins-good-debuginfo-32bit-1.8.3-3.1
gststreamer-plugins-good-debuginfo-1.8.3-3.1
gststreamer-plugins-good-32bit-1.8.3-3.1
gststreamer-plugins-good-1.8.3-3.1
gststreamer-plugins-good-extra-debuginfo-32bit-1.8.3-3.1

145808 - SuSE Linux 42.2 openSUSE-SU-2017:1429-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3289, CVE-2017-3509, CVE-2017-3511, CVE-2017-3512, CVE-2017-3514, CVE-2017-3526, CVE-2017-3533, CVE-2017-3539, CVE-2017-3544

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1429-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00097.html>

SuSE Linux 42.2

i586

java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-src-1.7.0.141-42.3.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.141-42.3.1
java-1_7_0-openjdk-demo-1.7.0.141-42.3.1
java-1_7_0-openjdk-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.141-42.3.1
java-1_7_0-openjdk-headless-1.7.0.141-42.3.1

java-1_7_0-openjdk-debugsource-1.7.0.141-42.3.1
java-1_7_0-openjdk-devel-1.7.0.141-42.3.1
java-1_7_0-openjdk-accessibility-1.7.0.141-42.3.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.141-42.3.1

noarch

java-1_7_0-openjdk-javadoc-1.7.0.141-42.3.1

x86_64

java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-src-1.7.0.141-42.3.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.141-42.3.1
java-1_7_0-openjdk-demo-1.7.0.141-42.3.1
java-1_7_0-openjdk-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.141-42.3.1
java-1_7_0-openjdk-headless-1.7.0.141-42.3.1
java-1_7_0-openjdk-debugsource-1.7.0.141-42.3.1
java-1_7_0-openjdk-devel-1.7.0.141-42.3.1
java-1_7_0-openjdk-accessibility-1.7.0.141-42.3.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.141-42.3.1
java-1_7_0-openjdk-1.7.0.141-42.3.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.141-42.3.1

145810 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1273-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5436

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1273-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00053.html>

SuSE Linux 42.1

x86_64

graphite2-debugsource-1.3.1-6.1
libgraphite2-3-debuginfo-32bit-1.3.1-6.1
libgraphite2-3-32bit-1.3.1-6.1
graphite2-1.3.1-6.1
graphite2-devel-1.3.1-6.1
libgraphite2-3-1.3.1-6.1
libgraphite2-3-debuginfo-1.3.1-6.1

graphite2-debuginfo-1.3.1-6.1

i586

graphite2-debugsource-1.3.1-6.1

graphite2-1.3.1-6.1

graphite2-devel-1.3.1-6.1

libgraphite2-3-1.3.1-6.1

libgraphite2-3-debuginfo-1.3.1-6.1

graphite2-debuginfo-1.3.1-6.1

SuSE Linux 42.2

x86_64

graphite2-devel-1.3.1-4.3.1

libgraphite2-3-32bit-1.3.1-4.3.1

libgraphite2-3-debuginfo-1.3.1-4.3.1

graphite2-debuginfo-1.3.1-4.3.1

libgraphite2-3-1.3.1-4.3.1

graphite2-1.3.1-4.3.1

libgraphite2-3-debuginfo-32bit-1.3.1-4.3.1

graphite2-debugsource-1.3.1-4.3.1

i586

graphite2-devel-1.3.1-4.3.1

libgraphite2-3-debuginfo-1.3.1-4.3.1

graphite2-debuginfo-1.3.1-4.3.1

libgraphite2-3-1.3.1-4.3.1

graphite2-1.3.1-4.3.1

graphite2-debugsource-1.3.1-4.3.1

145811 - SuSE Linux 42.2 openSUSE-SU-2017:1412-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8779

Description

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

openSUSE-SU-2017:1412-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00084.html>

SuSE Linux 42.2

x86_64

rpcbind-debugsource-0.2.3-3.3.1

rpcbind-debuginfo-0.2.3-3.3.1

rpcbind-0.2.3-3.3.1

i586

rpcbind-debugsource-0.2.3-3.3.1

rpcbind-debuginfo-0.2.3-3.3.1

rpcbind-0.2.3-3.3.1

145815 - SuSE Linux 42.2 openSUSE-SU-2017:0080-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0080-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00053.html>

SuSE Linux 42.2

x86_64

zlib-devel-1.2.8-10.1

zlib-devel-static-32bit-1.2.8-10.1

libz1-debuginfo-32bit-1.2.8-10.1

libz1-1.2.8-10.1

libz1-debuginfo-1.2.8-10.1

zlib-devel-static-1.2.8-10.1

zlib-debugsource-1.2.8-10.1

zlib-devel-32bit-1.2.8-10.1

libminizip1-1.2.8-10.1

libminizip1-debuginfo-1.2.8-10.1

minizip-devel-1.2.8-10.1

libz1-32bit-1.2.8-10.1

i586

zlib-devel-1.2.8-10.1

libz1-1.2.8-10.1

libz1-debuginfo-1.2.8-10.1

zlib-devel-static-1.2.8-10.1

zlib-debugsource-1.2.8-10.1

libminizip1-1.2.8-10.1

libminizip1-debuginfo-1.2.8-10.1

minizip-devel-1.2.8-10.1

145816 - SuSE Linux 42.2 openSUSE-SU-2017:0589-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0589-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00002.html>

SuSE Linux 42.2

i586

uuid-2.28-10.1
libfdisk1-2.28-10.1
libblkid-devel-static-2.28-10.1
libmount-devel-static-2.28-10.1
libuuid1-2.28-10.1
libblkid-devel-2.28-10.1
python-libmount-debugsource-2.28-10.2
util-linux-debuginfo-2.28-10.1
libmount1-debuginfo-2.28-10.1
libfdisk-devel-2.28-10.1
libuuid-devel-static-2.28-10.1
libsmartcols1-debuginfo-2.28-10.1
util-linux-2.28-10.1
util-linux-systemd-debugsource-2.28-10.1
libfdisk-devel-static-2.28-10.1
libsmartcols1-2.28-10.1
libsmartcols-devel-static-2.28-10.1
libfdisk1-debuginfo-2.28-10.1
uuid-debuginfo-2.28-10.1
libuuid1-debuginfo-2.28-10.1
libmount1-2.28-10.1
python-libmount-2.28-10.2
libsmartcols-devel-2.28-10.1
util-linux-debugsource-2.28-10.1
util-linux-systemd-debuginfo-2.28-10.1
libmount-devel-2.28-10.1
python-libmount-debuginfo-2.28-10.2
libuuid-devel-2.28-10.1
libblkid1-2.28-10.1
util-linux-systemd-2.28-10.1
libblkid1-debuginfo-2.28-10.1

noarch

util-linux-lang-2.28-10.1

x86_64

libblkid1-debuginfo-32bit-2.28-10.1
libmount-devel-32bit-2.28-10.1
uuid-2.28-10.1
libfdisk1-2.28-10.1
libblkid-devel-static-2.28-10.1
libblkid1-32bit-2.28-10.1
libmount-devel-static-2.28-10.1
libuuid1-2.28-10.1
libblkid-devel-2.28-10.1
libblkid-devel-32bit-2.28-10.1
python-libmount-debugsource-2.28-10.2
util-linux-debuginfo-2.28-10.1
libmount1-debuginfo-2.28-10.1
libfdisk-devel-2.28-10.1
libuuid-devel-static-2.28-10.1
libsmartcols1-debuginfo-2.28-10.1
util-linux-2.28-10.1
util-linux-systemd-debugsource-2.28-10.1
libmount1-debuginfo-32bit-2.28-10.1
libfdisk-devel-static-2.28-10.1
libsmartcols1-2.28-10.1
libuuid-devel-32bit-2.28-10.1
libsmartcols-devel-static-2.28-10.1

libuuid1-debuginfo-32bit-2.28-10.1
libfdisk1-debuginfo-2.28-10.1
uuuid-debuginfo-2.28-10.1
libuuid1-debuginfo-2.28-10.1
libmount1-2.28-10.1
python-libmount-2.28-10.2
libsmartcols-devel-2.28-10.1
util-linux-debugsource-2.28-10.1
libuuid1-32bit-2.28-10.1
libmount1-32bit-2.28-10.1
util-linux-systemd-debuginfo-2.28-10.1
libmount-devel-2.28-10.1
python-libmount-debuginfo-2.28-10.2
libuuid-devel-2.28-10.1
libblkid1-2.28-10.1
util-linux-systemd-2.28-10.1
libblkid1-debuginfo-2.28-10.1

145817 - SuSE Linux 42.2 openSUSE-SU-2017:0484-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10128, CVE-2016-10129, CVE-2016-10130, CVE-2017-5338, CVE-2017-5339

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0484-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00072.html>

SuSE Linux 42.2

x86_64

libgit2-debugsource-0.24.1-6.1
libgit2-devel-0.24.1-6.1
libgit2-24-32bit-0.24.1-6.1
libgit2-24-debuginfo-32bit-0.24.1-6.1
libgit2-24-debuginfo-0.24.1-6.1
libgit2-24-0.24.1-6.1

i586

libgit2-devel-0.24.1-6.1
libgit2-debugsource-0.24.1-6.1
libgit2-24-0.24.1-6.1
libgit2-24-debuginfo-0.24.1-6.1

145820 - SuSE Linux 42.2 openSUSE-SU-2017:1620-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5470, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7755, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7760, CVE-2017-7761, CVE-2017-7764, CVE-2017-7765, CVE-2017-7766, CVE-2017-7767, CVE-2017-7768, CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1620-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00072.html>

SuSE Linux 42.2

i586

java-1_8_0-openjdk-headless-debuginfo-1.8.0.131-10.10.3

mozilla-nss-sysinit-3.28.5-40.6.1

libsoftokn3-3.28.5-40.6.1

MozillaThunderbird-52.2-41.9.2

java-1_8_0-openjdk-demo-debuginfo-1.8.0.131-10.10.3

mozilla-nss-sysinit-debuginfo-3.28.5-40.6.1

java-1_8_0-openjdk-accessibility-1.8.0.131-10.10.3

MozillaFirefox-devel-52.2-57.12.2

MozillaThunderbird-translations-common-52.2-41.9.2

mozilla-nss-debuginfo-3.28.5-40.6.1

mozilla-nss-devel-3.28.5-40.6.1

java-1_8_0-openjdk-1.8.0.131-10.10.3

java-1_8_0-openjdk-debuginfo-1.8.0.131-10.10.3

MozillaThunderbird-debuginfo-52.2-41.9.2

java-1_8_0-openjdk-headless-1.8.0.131-10.10.3

MozillaFirefox-debuginfo-52.2-57.12.2

MozillaFirefox-translations-other-52.2-57.12.2

MozillaFirefox-52.2-57.12.2

libsoftokn3-debuginfo-3.28.5-40.6.1

java-1_8_0-openjdk-devel-debuginfo-1.8.0.131-10.10.3

mozilla-nss-certs-debuginfo-3.28.5-40.6.1

MozillaFirefox-debugsource-52.2-57.12.2

MozillaThunderbird-debugsource-52.2-41.9.2

MozillaThunderbird-devel-52.2-41.9.2

mozilla-nss-tools-debuginfo-3.28.5-40.6.1

MozillaThunderbird-translations-other-52.2-41.9.2

MozillaFirefox-buildsymbols-52.2-57.12.2

mozilla-nss-tools-3.28.5-40.6.1

MozillaFirefox-translations-common-52.2-57.12.2

MozillaFirefox-branding-upstream-52.2-57.12.2

mozilla-nss-3.28.5-40.6.1

libfreebl3-debuginfo-3.28.5-40.6.1

java-1_8_0-openjdk-src-1.8.0.131-10.10.3

mozilla-nss-debugsource-3.28.5-40.6.1

java-1_8_0-openjdk-devel-1.8.0.131-10.10.3

java-1_8_0-openjdk-debugsource-1.8.0.131-10.10.3

java-1_8_0-openjdk-demo-1.8.0.131-10.10.3

mozilla-nss-certs-3.28.5-40.6.1

libfreebl3-3.28.5-40.6.1

MozillaThunderbird-buildsymbols-52.2-41.9.2

noarch

java-1_8_0-openjdk-javadoc-1.8.0.131-10.10.3

x86_64

java-1_8_0-openjdk-headless-debuginfo-1.8.0.131-10.10.3

mozilla-nss-sysinit-3.28.5-40.6.1

libsoftokn3-3.28.5-40.6.1
MozillaThunderbird-52.2-41.9.2
java-1_8_0-openjdk-demo-debuginfo-1.8.0.131-10.10.3
mozilla-nss-sysinit-debuginfo-3.28.5-40.6.1
java-1_8_0-openjdk-accessibility-1.8.0.131-10.10.3
MozillaFirefox-devel-52.2-57.12.2
MozillaThunderbird-translations-common-52.2-41.9.2
libsoftokn3-debuginfo-32bit-3.28.5-40.6.1
libfreebl3-debuginfo-32bit-3.28.5-40.6.1
mozilla-nss-debuginfo-3.28.5-40.6.1
mozilla-nss-devel-3.28.5-40.6.1
java-1_8_0-openjdk-1.8.0.131-10.10.3
java-1_8_0-openjdk-debuginfo-1.8.0.131-10.10.3
MozillaThunderbird-debuginfo-52.2-41.9.2
java-1_8_0-openjdk-headless-1.8.0.131-10.10.3
MozillaFirefox-debuginfo-52.2-57.12.2
MozillaFirefox-translations-other-52.2-57.12.2
MozillaFirefox-52.2-57.12.2
mozilla-nss-certs-32bit-3.28.5-40.6.1
libfreebl3-32bit-3.28.5-40.6.1
libsoftokn3-debuginfo-3.28.5-40.6.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.131-10.10.3
mozilla-nss-certs-debuginfo-3.28.5-40.6.1
MozillaFirefox-debugsource-52.2-57.12.2
MozillaThunderbird-debugsource-52.2-41.9.2
MozillaThunderbird-devel-52.2-41.9.2
mozilla-nss-tools-debuginfo-3.28.5-40.6.1
MozillaThunderbird-translations-other-52.2-41.9.2
mozilla-nss-sysinit-debuginfo-32bit-3.28.5-40.6.1
libsoftokn3-32bit-3.28.5-40.6.1
MozillaFirefox-buildsymbols-52.2-57.12.2
mozilla-nss-tools-3.28.5-40.6.1
MozillaFirefox-translations-common-52.2-57.12.2
mozilla-nss-32bit-3.28.5-40.6.1
MozillaFirefox-branding-upstream-52.2-57.12.2
mozilla-nss-3.28.5-40.6.1
mozilla-nss-sysinit-32bit-3.28.5-40.6.1
libfreebl3-debuginfo-3.28.5-40.6.1
java-1_8_0-openjdk-src-1.8.0.131-10.10.3
mozilla-nss-debuginfo-32bit-3.28.5-40.6.1
mozilla-nss-debugsource-3.28.5-40.6.1
java-1_8_0-openjdk-devel-1.8.0.131-10.10.3
java-1_8_0-openjdk-debugsource-1.8.0.131-10.10.3
java-1_8_0-openjdk-demo-1.8.0.131-10.10.3
mozilla-nss-certs-debuginfo-32bit-3.28.5-40.6.1
mozilla-nss-certs-3.28.5-40.6.1
libfreebl3-3.28.5-40.6.1
MozillaThunderbird-buildsymbols-52.2-41.9.2

145821 - SuSE SLED 12 SP2, 12 SP3 SUSE-SU-2017:2300-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3885, CVE-2015-8367, CVE-2017-6886, CVE-2017-6887, CVE-2017-6889, CVE-2017-6890, CVE-2017-6899

Description

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

SUSE-SU-2017:2300-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003170.html>

SuSE SLED 12 SP3

x86_64

libraw9-debuginfo-0.15.4-9.2

libraw9-0.15.4-9.2

libraw-debugsource-0.15.4-9.2

SuSE SLED 12 SP2

x86_64

libraw9-debuginfo-0.15.4-9.2

libraw9-0.15.4-9.2

libraw-debugsource-0.15.4-9.2

145822 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0557-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10164

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0557-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00103.html>

SuSE Linux 42.1

x86_64

libXpm4-debuginfo-32bit-3.5.11-7.1

libXpm4-3.5.11-7.1

libXpm-tools-debuginfo-3.5.11-7.1

libXpm-devel-3.5.11-7.1

libXpm4-32bit-3.5.11-7.1

libXpm-devel-32bit-3.5.11-7.1

libXpm-debugsource-3.5.11-7.1

libXpm4-debuginfo-3.5.11-7.1

libXpm-tools-3.5.11-7.1

i586

libXpm4-3.5.11-7.1

libXpm-tools-debuginfo-3.5.11-7.1

libXpm-devel-3.5.11-7.1

libXpm-debugsource-3.5.11-7.1

libXpm4-debuginfo-3.5.11-7.1

libXpm-tools-3.5.11-7.1

SuSE Linux 42.2

x86_64

libXpm-tools-3.5.11-8.1

libXpm4-3.5.11-8.1

libXpm-devel-32bit-3.5.11-8.1
libXpm4-debuginfo-3.5.11-8.1
libXpm-debugsource-3.5.11-8.1
libXpm4-debuginfo-32bit-3.5.11-8.1
libXpm-tools-debuginfo-3.5.11-8.1
libXpm-devel-3.5.11-8.1
libXpm4-32bit-3.5.11-8.1

i586
libXpm-tools-3.5.11-8.1
libXpm4-3.5.11-8.1
libXpm4-debuginfo-3.5.11-8.1
libXpm-debugsource-3.5.11-8.1
libXpm-tools-debuginfo-3.5.11-8.1
libXpm-devel-3.5.11-8.1

145825 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1005-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1005-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00049.html>

SuSE Linux 42.1
noarch
phpMyAdmin-4.4.15.10-37.1

SuSE Linux 42.2
noarch
phpMyAdmin-4.4.15.10-33.6.1

145826 - SuSE Linux 42.1 openSUSE-SU-2017:0421-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9577, CVE-2016-9578

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0421-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00044.html>

SuSE Linux 42.1
x86_64
spice-client-debuginfo-0.12.5-11.1
spice-debugsource-0.12.5-11.1
libspice-server-devel-0.12.5-11.1
libspice-server1-0.12.5-11.1
libspice-server1-debuginfo-0.12.5-11.1
spice-client-0.12.5-11.1

i586
spice-client-debuginfo-0.12.5-11.1
spice-debugsource-0.12.5-11.1
libspice-server-devel-0.12.5-11.1
libspice-server1-0.12.5-11.1
libspice-server1-debuginfo-0.12.5-11.1
spice-client-0.12.5-11.1

145827 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1272-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8422

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1272-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00052.html>

SuSE Linux 42.1
i586
libksuseinstall1-4.14.18-18.1
libKF5Auth5-5.21.0-16.1
kdelibs4-4.14.18-18.1
kdelibs4-branding-upstream-4.14.18-18.1
libkdecore4-devel-debuginfo-4.14.18-18.1
libkdecore4-devel-4.14.18-18.1
libkdecore4-4.14.18-18.1
kauth-devel-5.21.0-16.1
kdelibs4-core-debuginfo-4.14.18-18.1
libkde4-debuginfo-4.14.18-18.1
libksuseinstall-devel-4.14.18-18.1
libkdecore4-debuginfo-4.14.18-18.1
kdelibs4-debuginfo-4.14.18-18.1
libkde4-devel-4.14.18-18.1
libKF5Auth5-debuginfo-5.21.0-16.1
libkde4-4.14.18-18.1
libksuseinstall1-debuginfo-4.14.18-18.1
kdelibs4-core-4.14.18-18.1
kdelibs4-doc-debuginfo-4.14.18-18.1
kdelibs4-doc-4.14.18-18.1
kdelibs4-debugsource-4.14.18-18.1
kauth-debugsource-5.21.0-16.1

noarch
libKF5Auth5-lang-5.21.0-16.1
kdelibs4-apidocs-4.14.18-18.1

x86_64
libKF5Auth5-debuginfo-5.21.0-16.1
libkdecore4-devel-4.14.18-18.1
kauth-debugsource-5.21.0-16.1
libkde4-debuginfo-4.14.18-18.1
kdelibs4-core-4.14.18-18.1
kdelibs4-branding-upstream-4.14.18-18.1
libkdecore4-devel-debuginfo-4.14.18-18.1
libkde4-devel-4.14.18-18.1
kdelibs4-debuginfo-4.14.18-18.1
kdelibs4-4.14.18-18.1
libksuseinstall1-debuginfo-4.14.18-18.1
libKF5Auth5-32bit-5.21.0-16.1
libkdecore4-debuginfo-4.14.18-18.1
libkdecore4-4.14.18-18.1
kdelibs4-doc-debuginfo-4.14.18-18.1
libkdecore4-debuginfo-32bit-4.14.18-18.1
kdelibs4-debugsource-4.14.18-18.1
kauth-devel-5.21.0-16.1
libksuseinstall1-4.14.18-18.1
libKF5Auth5-5.21.0-16.1
libKF5Auth5-debuginfo-32bit-5.21.0-16.1
kdelibs4-doc-4.14.18-18.1
libkdecore4-32bit-4.14.18-18.1
kdelibs4-core-debuginfo-4.14.18-18.1
libkde4-32bit-4.14.18-18.1
libksuseinstall1-32bit-4.14.18-18.1
kauth-devel-32bit-5.21.0-16.1
libkde4-4.14.18-18.1
libksuseinstall1-debuginfo-32bit-4.14.18-18.1
libksuseinstall-devel-4.14.18-18.1
libkde4-debuginfo-32bit-4.14.18-18.1

SuSE Linux 42.2

i586
libkdecore4-devel-4.14.25-7.4.1
kauth-debugsource-5.26.0-2.3.1
kdelibs4-core-4.14.25-7.4.1
kdelibs4-core-debuginfo-4.14.25-7.4.1
libksuseinstall1-debuginfo-4.14.25-7.4.1
libkde4-4.14.25-7.4.1
libksuseinstall-devel-4.14.25-7.4.1
kdelibs4-doc-4.14.25-7.4.1
kdelibs4-debuginfo-4.14.25-7.4.1
kdelibs4-doc-debuginfo-4.14.25-7.4.1
libkdecore4-debuginfo-4.14.25-7.4.1
libkdecore4-devel-debuginfo-4.14.25-7.4.1
libkde4-devel-4.14.25-7.4.1
kdelibs4-branding-upstream-4.14.25-7.4.1
kdelibs4-4.14.25-7.4.1
kdelibs4-debugsource-4.14.25-7.4.1
libksuseinstall1-4.14.25-7.4.1
libKF5Auth5-5.26.0-2.3.1
libkdecore4-4.14.25-7.4.1
libKF5Auth5-debuginfo-5.26.0-2.3.1
kauth-devel-5.26.0-2.3.1

libkde4-debuginfo-4.14.25-7.4.1

noarch

libKF5Auth5-lang-5.26.0-2.3.1

kdelibs4-apidocs-4.14.25-7.4.1

x86_64

libksuseinstall-devel-4.14.25-7.4.1

kdelibs4-doc-4.14.25-7.4.1

libkdecore4-devel-4.14.25-7.4.1

libkdecore4-debuginfo-32bit-4.14.25-7.4.1

kdelibs4-debugsource-4.14.25-7.4.1

libkde4-debuginfo-4.14.25-7.4.1

libKF5Auth5-debuginfo-32bit-5.26.0-2.3.1

libksuseinstall1-4.14.25-7.4.1

kauth-devel-5.26.0-2.3.1

libksuseinstall1-debuginfo-4.14.25-7.4.1

libksuseinstall1-debuginfo-32bit-4.14.25-7.4.1

libkdecore4-4.14.25-7.4.1

libkde4-debuginfo-32bit-4.14.25-7.4.1

kdelibs4-core-debuginfo-4.14.25-7.4.1

kdelibs4-4.14.25-7.4.1

kauth-devel-32bit-5.26.0-2.3.1

libkdecore4-32bit-4.14.25-7.4.1

kdelibs4-debuginfo-4.14.25-7.4.1

libKF5Auth5-5.26.0-2.3.1

kauth-debugsource-5.26.0-2.3.1

kdelibs4-core-4.14.25-7.4.1

libKF5Auth5-32bit-5.26.0-2.3.1

libkde4-4.14.25-7.4.1

kdelibs4-doc-debuginfo-4.14.25-7.4.1

libkde4-devel-4.14.25-7.4.1

libksuseinstall1-32bit-4.14.25-7.4.1

libkde4-32bit-4.14.25-7.4.1

libKF5Auth5-debuginfo-5.26.0-2.3.1

libkdecore4-devel-debuginfo-4.14.25-7.4.1

kdelibs4-branding-upstream-4.14.25-7.4.1

libkdecore4-debuginfo-4.14.25-7.4.1

145829 - SuSE Linux 42.1 openSUSE-SU-2017:0336-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:0336-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00174.html>

SuSE Linux 42.1

i586

lcms2-debugsource-2.8-3.1

liblcms2-devel-2.8-3.1
liblcms2-2-debuginfo-2.8-3.1
lcms2-2.8-3.1
lcms2-debuginfo-2.8-3.1
liblcms2-2-2.8-3.1

noarch
liblcms2-doc-2.8-3.1

x86_64
lcms2-debugsource-2.8-3.1
liblcms2-devel-2.8-3.1
liblcms2-2-32bit-2.8-3.1
liblcms2-2-debuginfo-2.8-3.1
liblcms2-devel-32bit-2.8-3.1
lcms2-2.8-3.1
liblcms2-2-debuginfo-32bit-2.8-3.1
lcms2-debuginfo-2.8-3.1
liblcms2-2-2.8-3.1

145831 - SuSE Linux 42.2 openSUSE-SU-2017:1560-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6502, CVE-2017-7606, CVE-2017-7941, CVE-2017-7942, CVE-2017-7943, CVE-2017-8343, CVE-2017-8344, CVE-2017-8345, CVE-2017-8346, CVE-2017-8347, CVE-2017-8348, CVE-2017-8349, CVE-2017-8350, CVE-2017-8351, CVE-2017-8352, CVE-2017-8353, CVE-2017-8354, CVE-2017-8355, CVE-2017-8356, CVE-2017-8357, CVE-2017-8765, CVE-2017-8830, CVE-2017-9098, CVE-2017-9141, CVE-2017-9142, CVE-2017-9143, CVE-2017-9144

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1560-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00045.html>

SuSE Linux 42.2

i586
ImageMagick-debugsource-6.8.8.1-30.3.1
perl-PerlMagick-debuginfo-6.8.8.1-30.3.1
libMagick++-devel-6.8.8.1-30.3.1
ImageMagick-extra-debuginfo-6.8.8.1-30.3.1
libMagickCore-6_Q16-1-6.8.8.1-30.3.1
libMagickWand-6_Q16-1-6.8.8.1-30.3.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.3.1
ImageMagick-6.8.8.1-30.3.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.3.1
ImageMagick-devel-6.8.8.1-30.3.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.3.1
perl-PerlMagick-6.8.8.1-30.3.1
ImageMagick-extra-6.8.8.1-30.3.1
ImageMagick-debuginfo-6.8.8.1-30.3.1
libMagick++-6_Q16-3-6.8.8.1-30.3.1

noarch

ImageMagick-doc-6.8.8.1-30.3.1

x86_64

libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-30.3.1
ImageMagick-debugsource-6.8.8.1-30.3.1
perl-PerlMagick-debuginfo-6.8.8.1-30.3.1
libMagick++-devel-6.8.8.1-30.3.1
ImageMagick-extra-debuginfo-6.8.8.1-30.3.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-30.3.1
libMagickCore-6_Q16-1-6.8.8.1-30.3.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-30.3.1
libMagickWand-6_Q16-1-6.8.8.1-30.3.1
libMagick++-devel-32bit-6.8.8.1-30.3.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.3.1
ImageMagick-6.8.8.1-30.3.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.3.1
ImageMagick-devel-32bit-6.8.8.1-30.3.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-30.3.1
ImageMagick-devel-6.8.8.1-30.3.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.3.1
perl-PerlMagick-6.8.8.1-30.3.1
ImageMagick-extra-6.8.8.1-30.3.1
ImageMagick-debuginfo-6.8.8.1-30.3.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-30.3.1
libMagick++-6_Q16-3-32bit-6.8.8.1-30.3.1
libMagick++-6_Q16-3-6.8.8.1-30.3.1

145834 - SuSE Linux 42.2 openSUSE-SU-2017:1534-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9343, CVE-2017-9344, CVE-2017-9345, CVE-2017-9346, CVE-2017-9347, CVE-2017-9348, CVE-2017-9349, CVE-2017-9350, CVE-2017-9351, CVE-2017-9352, CVE-2017-9353, CVE-2017-9354

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1534-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00033.html>

SuSE Linux 42.2

x86_64

wireshark-2.2.7-14.6.1
wireshark-ui-gtk-2.2.7-14.6.1
wireshark-ui-qt-debuginfo-2.2.7-14.6.1
wireshark-debugsource-2.2.7-14.6.1
wireshark-ui-qt-2.2.7-14.6.1
wireshark-devel-2.2.7-14.6.1
wireshark-ui-gtk-debuginfo-2.2.7-14.6.1
wireshark-debuginfo-2.2.7-14.6.1

145838 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0687-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0687-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00041.html>

SuSE Linux 42.1

x86_64

MozillaThunderbird-translations-common-45.8.0-39.1

MozillaThunderbird-buildsymbols-45.8.0-39.1

MozillaThunderbird-45.8.0-39.1

MozillaThunderbird-devel-45.8.0-39.1

MozillaThunderbird-debuginfo-45.8.0-39.1

MozillaThunderbird-debugsource-45.8.0-39.1

MozillaThunderbird-translations-other-45.8.0-39.1

i586

MozillaThunderbird-translations-common-45.8.0-39.1

MozillaThunderbird-buildsymbols-45.8.0-39.1

MozillaThunderbird-45.8.0-39.1

MozillaThunderbird-devel-45.8.0-39.1

MozillaThunderbird-debuginfo-45.8.0-39.1

MozillaThunderbird-debugsource-45.8.0-39.1

MozillaThunderbird-translations-other-45.8.0-39.1

SuSE Linux 42.2

x86_64

MozillaThunderbird-translations-common-45.8.0-39.1

MozillaThunderbird-buildsymbols-45.8.0-39.1

MozillaThunderbird-45.8.0-39.1

MozillaThunderbird-devel-45.8.0-39.1

MozillaThunderbird-debuginfo-45.8.0-39.1

MozillaThunderbird-debugsource-45.8.0-39.1

MozillaThunderbird-translations-other-45.8.0-39.1

i586

MozillaThunderbird-translations-common-45.8.0-39.1

MozillaThunderbird-buildsymbols-45.8.0-39.1

MozillaThunderbird-45.8.0-39.1

MozillaThunderbird-devel-45.8.0-39.1

MozillaThunderbird-debuginfo-45.8.0-39.1

MozillaThunderbird-debugsource-45.8.0-39.1

MozillaThunderbird-translations-other-45.8.0-39.1

145841 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0483-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6702, CVE-2016-5300

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0483-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00071.html>

SuSE Linux 42.1

x86_64

libexpat-devel-2.1.0-20.1
expat-debuginfo-32bit-2.1.0-20.1
libexpat-devel-32bit-2.1.0-20.1
expat-debugsource-2.1.0-20.1
libexpat1-2.1.0-20.1
expat-debuginfo-2.1.0-20.1
libexpat1-debuginfo-32bit-2.1.0-20.1
expat-2.1.0-20.1
libexpat1-debuginfo-2.1.0-20.1
libexpat1-32bit-2.1.0-20.1

i586

libexpat-devel-2.1.0-20.1
expat-debugsource-2.1.0-20.1
libexpat1-2.1.0-20.1
expat-debuginfo-2.1.0-20.1
expat-2.1.0-20.1
libexpat1-debuginfo-2.1.0-20.1

SuSE Linux 42.2

x86_64

expat-2.1.0-19.1
libexpat1-2.1.0-19.1
expat-debuginfo-2.1.0-19.1
libexpat-devel-32bit-2.1.0-19.1
expat-debuginfo-32bit-2.1.0-19.1
libexpat-devel-2.1.0-19.1
libexpat1-debuginfo-2.1.0-19.1
expat-debugsource-2.1.0-19.1
libexpat1-debuginfo-32bit-2.1.0-19.1
libexpat1-32bit-2.1.0-19.1

i586

expat-2.1.0-19.1
libexpat1-2.1.0-19.1
expat-debuginfo-2.1.0-19.1
libexpat-devel-2.1.0-19.1
libexpat1-debuginfo-2.1.0-19.1
expat-debugsource-2.1.0-19.1

145845 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0933-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7551, CVE-2016-2339

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0933-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00019.html>

SuSE Linux 42.1

i586

ruby2.2-2.2.6-6.1

libruby2_2-2_2-debuginfo-2.2.6-6.1

ruby2.2-doc-2.2.6-6.1

ruby2.2-stdlib-debuginfo-2.2.6-6.1

ruby2.2-tk-debuginfo-2.2.6-6.1

ruby2.2-debugsource-2.2.6-6.1

ruby2.2-tk-2.2.6-6.1

ruby2.2-devel-2.2.6-6.1

ruby2.2-stdlib-2.2.6-6.1

ruby2.2-debuginfo-2.2.6-6.1

libruby2_2-2_2-2.2.6-6.1

ruby2.2-devel-extra-2.2.6-6.1

noarch

ruby2.2-doc-ri-2.2.6-6.1

x86_64

ruby2.2-2.2.6-6.1

libruby2_2-2_2-debuginfo-2.2.6-6.1

ruby2.2-doc-2.2.6-6.1

ruby2.2-stdlib-debuginfo-2.2.6-6.1

ruby2.2-tk-debuginfo-2.2.6-6.1

ruby2.2-debugsource-2.2.6-6.1

ruby2.2-tk-2.2.6-6.1

ruby2.2-devel-2.2.6-6.1

ruby2.2-stdlib-2.2.6-6.1

ruby2.2-debuginfo-2.2.6-6.1

libruby2_2-2_2-2.2.6-6.1

ruby2.2-devel-extra-2.2.6-6.1

SuSE Linux 42.2

i586

libruby2_2-2_2-2.2.6-6.3.1

ruby2.2-devel-2.2.6-6.3.1

ruby2.3-tk-debuginfo-2.3.3-2.3.1

ruby2.2-debugsource-2.2.6-6.3.1

ruby2.3-doc-2.3.3-2.3.1

ruby2.3-tk-2.3.3-2.3.1

ruby2.3-devel-extra-2.3.3-2.3.1

ruby2.3-2.3.3-2.3.1

ruby2.2-devel-extra-2.2.6-6.3.1

ruby2.3-debuginfo-2.3.3-2.3.1

ruby2.2-tk-2.2.6-6.3.1

libruby2_3-2_3-2.3.3-2.3.1

ruby2.2-tk-debuginfo-2.2.6-6.3.1

libruby2_3-2_3-debuginfo-2.3.3-2.3.1

ruby2.3-stdlib-debuginfo-2.3.3-2.3.1

ruby2.3-devel-2.3.3-2.3.1
ruby2.3-debugsource-2.3.3-2.3.1
ruby2.2-doc-2.2.6-6.3.1
ruby2.2-debuginfo-2.2.6-6.3.1
ruby2.2-stdlib-2.2.6-6.3.1
ruby2.3-stdlib-2.3.3-2.3.1
libruby2_2-2_2-debuginfo-2.2.6-6.3.1
ruby2.2-stdlib-debuginfo-2.2.6-6.3.1
ruby2.2-2.2.6-6.3.1

noarch
ruby2.2-doc-ri-2.2.6-6.3.1
ruby2.3-doc-ri-2.3.3-2.3.1

x86_64
libruby2_2-2_2-2.2.6-6.3.1
ruby2.2-devel-2.2.6-6.3.1
ruby2.3-tk-debuginfo-2.3.3-2.3.1
ruby2.2-debugsource-2.2.6-6.3.1
ruby2.3-doc-2.3.3-2.3.1
ruby2.3-tk-2.3.3-2.3.1
ruby2.3-devel-extra-2.3.3-2.3.1
ruby2.3-2.3.3-2.3.1
ruby2.2-devel-extra-2.2.6-6.3.1
ruby2.3-debuginfo-2.3.3-2.3.1
ruby2.2-tk-2.2.6-6.3.1
libruby2_3-2_3-2.3.3-2.3.1
ruby2.2-tk-debuginfo-2.2.6-6.3.1
libruby2_3-2_3-debuginfo-2.3.3-2.3.1
ruby2.3-stdlib-debuginfo-2.3.3-2.3.1
ruby2.3-devel-2.3.3-2.3.1
ruby2.3-debugsource-2.3.3-2.3.1
ruby2.2-doc-2.2.6-6.3.1
ruby2.2-debuginfo-2.2.6-6.3.1
ruby2.2-stdlib-2.2.6-6.3.1
ruby2.3-stdlib-2.3.3-2.3.1
libruby2_2-2_2-debuginfo-2.2.6-6.3.1
ruby2.2-stdlib-debuginfo-2.2.6-6.3.1
ruby2.2-2.2.6-6.3.1

145846 - SuSE Linux 42.2 openSUSE-SU-2017:1078-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6505, CVE-2017-7228

Description

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

openSUSE-SU-2017:1078-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00083.html>

SuSE Linux 42.2

x86_64

xen-4.7.2_02-11.3.1
xen-libs-debuginfo-32bit-4.7.2_02-11.3.1
xen-libs-4.7.2_02-11.3.1
xen-tools-domU-4.7.2_02-11.3.1
xen-libs-32bit-4.7.2_02-11.3.1
xen-libs-debuginfo-4.7.2_02-11.3.1
xen-doc-html-4.7.2_02-11.3.1
xen-tools-domU-debuginfo-4.7.2_02-11.3.1
xen-tools-debuginfo-4.7.2_02-11.3.1
xen-debugsource-4.7.2_02-11.3.1
xen-tools-4.7.2_02-11.3.1
xen-devel-4.7.2_02-11.3.1

i586

xen-libs-4.7.2_02-11.3.1
xen-tools-domU-4.7.2_02-11.3.1
xen-libs-debuginfo-4.7.2_02-11.3.1
xen-tools-domU-debuginfo-4.7.2_02-11.3.1
xen-debugsource-4.7.2_02-11.3.1
xen-devel-4.7.2_02-11.3.1

145847 - SuSE Linux 42.1 openSUSE-SU-2017:0077-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0077-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00050.html>

SuSE Linux 42.1

x86_64
libz1-debuginfo-32bit-1.2.8-8.1
zlib-devel-static-32bit-1.2.8-8.1
zlib-debugsource-1.2.8-8.1
zlib-devel-1.2.8-8.1
libz1-1.2.8-8.1
libz1-32bit-1.2.8-8.1
zlib-devel-32bit-1.2.8-8.1
libz1-debuginfo-1.2.8-8.1
zlib-devel-static-1.2.8-8.1

i586

libz1-debuginfo-1.2.8-8.1
libz1-1.2.8-8.1
zlib-devel-1.2.8-8.1
zlib-devel-static-1.2.8-8.1
zlib-debugsource-1.2.8-8.1

145848 - SuSE Linux 42.2 openSUSE-SU-2017:1610-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2624

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1610-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00070.html>

SuSE Linux 42.2

x86_64

xorg-x11-server-extra-debuginfo-7.6_1.18.3-12.15.2

xorg-x11-server-debugsource-7.6_1.18.3-12.15.2

xorg-x11-server-7.6_1.18.3-12.15.2

xorg-x11-server-debuginfo-7.6_1.18.3-12.15.2

xorg-x11-server-extra-7.6_1.18.3-12.15.2

xorg-x11-server-source-7.6_1.18.3-12.15.2

xorg-x11-server-sdk-7.6_1.18.3-12.15.2

i586

xorg-x11-server-extra-debuginfo-7.6_1.18.3-12.15.2

xorg-x11-server-debugsource-7.6_1.18.3-12.15.2

xorg-x11-server-7.6_1.18.3-12.15.2

xorg-x11-server-debuginfo-7.6_1.18.3-12.15.2

xorg-x11-server-extra-7.6_1.18.3-12.15.2

xorg-x11-server-source-7.6_1.18.3-12.15.2

xorg-x11-server-sdk-7.6_1.18.3-12.15.2

145850 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2344-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7436

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2344-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-September/003183.html>

SuSE SLED 12 SP3

x86_64

zypper-1.13.32-21.3.2

libzypp-debuginfo-16.15.6-2.8.1

libzypp-16.15.6-2.8.1

zypper-debugsource-1.13.32-21.3.2

libzypp-debugsource-16.15.6-2.8.1

zypper-debuginfo-1.13.32-21.3.2

noarch

zypper-log-1.13.32-21.3.2

SuSE SLES 12 SP3

noarch

zypper-log-1.13.32-21.3.2

x86_64

zypper-1.13.32-21.3.2

libzypp-debuginfo-16.15.6-2.8.1

libzypp-16.15.6-2.8.1

zypper-debugsource-1.13.32-21.3.2

libzypp-debugsource-16.15.6-2.8.1

zypper-debuginfo-1.13.32-21.3.2

145851 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0909-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Description

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

openSUSE-SU-2017:0909-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00003.html>

SuSE Linux 42.1

x86_64

chromium-57.0.2987.133-108.1

chromium-debugsource-57.0.2987.133-108.1

chromium-debuginfo-57.0.2987.133-108.1

chromedriver-debuginfo-57.0.2987.133-108.1

chromedriver-57.0.2987.133-108.1

SuSE Linux 42.2

x86_64

chromedriver-debuginfo-57.0.2987.133-104.6.1

chromium-57.0.2987.133-104.6.1

chromium-debugsource-57.0.2987.133-104.6.1

chromedriver-57.0.2987.133-104.6.1

chromium-debuginfo-57.0.2987.133-104.6.1

145852 - SuSE Linux 42.2 openSUSE-SU-2017:0973-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2640

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0973-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00038.html>

SuSE Linux 42.2
x86_64
pidgin-2.12.0-8.6.1
libpurple-plugin-sametime-debuginfo-2.12.0-8.6.1
libpurple-debuginfo-2.12.0-8.6.1
libpurple-2.12.0-8.6.1
pidgin-devel-2.12.0-8.6.1
pidgin-debuginfo-2.12.0-8.6.1
pidgin-debugsource-2.12.0-8.6.1
finch-2.12.0-8.6.1
libpurple-tcl-debuginfo-2.12.0-8.6.1
finch-debuginfo-2.12.0-8.6.1
libpurple-plugin-sametime-2.12.0-8.6.1
finch-devel-2.12.0-8.6.1
libpurple-devel-2.12.0-8.6.1
libpurple-tcl-2.12.0-8.6.1

noarch
libpurple-branding-upstream-2.12.0-8.6.1
libpurple-branding-openSUSE-42.2-3.3.2
libpurple-lang-2.12.0-8.6.1

145857 - SuSE Linux 42.1 openSUSE-SU-2017:1201-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5495

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1201-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00020.html>

SuSE Linux 42.1
x86_64
quagga-debugsource-0.99.24.1-17.1
quagga-devel-0.99.24.1-17.1
quagga-0.99.24.1-17.1
quagga-debuginfo-0.99.24.1-17.1

i586
quagga-debugsource-0.99.24.1-17.1
quagga-devel-0.99.24.1-17.1

quagga-0.99.24.1-17.1
quagga-debuginfo-0.99.24.1-17.1

145859 - SuSE Linux 42.2 openSUSE-SU-2017:1591-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1591-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00058.html>

SuSE Linux 42.2

x86_64

chromium-debuginfo-59.0.3071.104-104.18.2

chromium-debugsource-59.0.3071.104-104.18.2

chromedriver-debuginfo-59.0.3071.104-104.18.2

chromium-59.0.3071.104-104.18.2

chromedriver-59.0.3071.104-104.18.2

145861 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0955-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0955-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00028.html>

SuSE Linux 42.1

noarch

clamav-database-201704030005-240.1

SuSE Linux 42.2

noarch

clamav-database-201704030005-54.9.1

145862 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2205-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000100, CVE-2017-1000101

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2205-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00080.html>

SuSE Linux 42.2

x86_64

libcurl4-7.37.0-16.6.1

libcurl4-32bit-7.37.0-16.6.1

curl-7.37.0-16.6.1

libcurl-devel-32bit-7.37.0-16.6.1

curl-debuginfo-7.37.0-16.6.1

libcurl4-debuginfo-32bit-7.37.0-16.6.1

libcurl-devel-7.37.0-16.6.1

libcurl4-debuginfo-7.37.0-16.6.1

curl-debugsource-7.37.0-16.6.1

i586

libcurl4-7.37.0-16.6.1

curl-7.37.0-16.6.1

curl-debuginfo-7.37.0-16.6.1

libcurl-devel-7.37.0-16.6.1

libcurl4-debuginfo-7.37.0-16.6.1

curl-debugsource-7.37.0-16.6.1

SuSE Linux 42.3

x86_64

libcurl-devel-32bit-7.37.0-20.1

libcurl4-debuginfo-32bit-7.37.0-20.1

curl-debuginfo-7.37.0-20.1

libcurl4-debuginfo-7.37.0-20.1

libcurl4-7.37.0-20.1

libcurl4-32bit-7.37.0-20.1

libcurl-devel-7.37.0-20.1

curl-7.37.0-20.1

curl-debugsource-7.37.0-20.1

i586

curl-debuginfo-7.37.0-20.1

libcurl4-debuginfo-7.37.0-20.1

libcurl4-7.37.0-20.1

libcurl-devel-7.37.0-20.1

curl-7.37.0-20.1

curl-debugsource-7.37.0-20.1

145865 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0741-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6542

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0741-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00055.html>

SuSE Linux 42.1
x86_64
putty-debuginfo-0.68-12.1
putty-debugsource-0.68-12.1
putty-0.68-12.1

i586
putty-debuginfo-0.68-12.1
putty-debugsource-0.68-12.1
putty-0.68-12.1

SuSE Linux 42.2
x86_64
putty-debuginfo-0.68-12.1
putty-debugsource-0.68-12.1
putty-0.68-12.1

i586
putty-debuginfo-0.68-12.1
putty-debugsource-0.68-12.1
putty-0.68-12.1

145867 - SuSE Linux 42.2 openSUSE-SU-2017:1689-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2810

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1689-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00098.html>

SuSE Linux 42.2
noarch
python-tablib-0.10.0-6.3.1

145868 - SuSE SLES 11 SP4 SUSE-SU-2017:2302-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7782, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7798, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7804, CVE-2017-7807

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2302-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003171.html>

SuSE SLES 11 SP4

i586

MozillaFirefox-translations-52.3.0esr-72.9.1

MozillaFirefox-branding-SLED-52-24.5.1

MozillaFirefox-52.3.0esr-72.9.1

x86_64

MozillaFirefox-translations-52.3.0esr-72.9.1

MozillaFirefox-branding-SLED-52-24.5.1

MozillaFirefox-52.3.0esr-72.9.1

145869 - SuSE Linux 42.1 openSUSE-SU-2017:0935-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0935-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00021.html>

SuSE Linux 42.1

i586

libndr-standard-devel-4.2.4-27.1

libsmbconf0-debuginfo-4.2.4-27.1

libndr-nbt0-debuginfo-4.2.4-27.1

libtevent-util0-debuginfo-4.2.4-27.1

libsmbclient-devel-4.2.4-27.1

libdcerpc-binding0-debuginfo-4.2.4-27.1

ctdb-debuginfo-4.2.4-27.1

libdcerpc-atsvc-devel-4.2.4-27.1

libtevent-util-devel-4.2.4-27.1

libwbclient0-debuginfo-4.2.4-27.1

libdcerpc-samr0-4.2.4-27.1

samba-python-4.2.4-27.1

libnetapi-devel-4.2.4-27.1

libsamba-policy0-debuginfo-4.2.4-27.1

libndr-krb5pac0-4.2.4-27.1
ctdb-tests-debuginfo-4.2.4-27.1
samba-python-debuginfo-4.2.4-27.1
libsamba-credentials-devel-4.2.4-27.1
ctdb-4.2.4-27.1
libndr-krb5pac-devel-4.2.4-27.1
libsmbclient0-4.2.4-27.1
samba-test-devel-4.2.4-27.1
libdcerpc-atSvc0-4.2.4-27.1
libwbclient0-4.2.4-27.1
libdcerpc-atSvc0-debuginfo-4.2.4-27.1
libsamba-policy-devel-4.2.4-27.1
libdcerpc0-debuginfo-4.2.4-27.1
libsamba-passdb0-debuginfo-4.2.4-27.1
samba-client-debuginfo-4.2.4-27.1
libndr0-4.2.4-27.1
libsamba-credentials0-4.2.4-27.1
libnetapi0-debuginfo-4.2.4-27.1
libsamba-util0-debuginfo-4.2.4-27.1
libgensec-devel-4.2.4-27.1
samba-winbind-debuginfo-4.2.4-27.1
samba-4.2.4-27.1
libnetapi0-4.2.4-27.1
libndr-devel-4.2.4-27.1
libsamba-hostconfig0-4.2.4-27.1
libsamba-policy0-4.2.4-27.1
libndr-standard0-debuginfo-4.2.4-27.1
libsmbclient0-debuginfo-4.2.4-27.1
libsamba-hostconfig0-debuginfo-4.2.4-27.1
libsmbconf0-4.2.4-27.1
libgensec0-4.2.4-27.1
samba-libs-4.2.4-27.1
libndr-krb5pac0-debuginfo-4.2.4-27.1
libdcerpc-binding0-4.2.4-27.1
libregistry0-4.2.4-27.1
libsamdb0-debuginfo-4.2.4-27.1
libsmbconf-devel-4.2.4-27.1
libsmbclient-raw0-debuginfo-4.2.4-27.1
libsamba-passdb0-4.2.4-27.1
libsamdb-devel-4.2.4-27.1
samba-test-4.2.4-27.1
libgensec0-debuginfo-4.2.4-27.1
libdcerpc-samr-devel-4.2.4-27.1
libregistry-devel-4.2.4-27.1
samba-test-debuginfo-4.2.4-27.1
libsmbldap0-debuginfo-4.2.4-27.1
libwbclient-devel-4.2.4-27.1
libsmbclient-raw-devel-4.2.4-27.1
libsamba-hostconfig-devel-4.2.4-27.1
libsamdb0-4.2.4-27.1
samba-core-devel-4.2.4-27.1
libsmbldap0-4.2.4-27.1
libtevent-util0-4.2.4-27.1
libsamba-util0-4.2.4-27.1
ctdb-tests-4.2.4-27.1
libsmbclient-raw0-4.2.4-27.1
libsamba-util-devel-4.2.4-27.1
libndr-nbt-devel-4.2.4-27.1
libsamba-credentials0-debuginfo-4.2.4-27.1
libndr0-debuginfo-4.2.4-27.1

libdcerpc-samr0-debuginfo-4.2.4-27.1
libndr-standard0-4.2.4-27.1
libndr-nbt0-4.2.4-27.1
samba-winbind-4.2.4-27.1
samba-pidl-4.2.4-27.1
samba-client-4.2.4-27.1
samba-debugsource-4.2.4-27.1
libdcerpc-devel-4.2.4-27.1
libregistry0-debuginfo-4.2.4-27.1
libsamba-passdb-devel-4.2.4-27.1
libsmbldap-devel-4.2.4-27.1
samba-debuginfo-4.2.4-27.1
ctdb-devel-4.2.4-27.1
samba-libs-debuginfo-4.2.4-27.1
libdcerpc0-4.2.4-27.1

noarch
samba-doc-4.2.4-27.1

x86_64

libndr-nbt0-debuginfo-32bit-4.2.4-27.1
libndr-standard0-debuginfo-32bit-4.2.4-27.1
libdcerpc-devel-4.2.4-27.1
samba-debuginfo-4.2.4-27.1
libdcerpc-binding0-32bit-4.2.4-27.1
libsamba-util0-debuginfo-4.2.4-27.1
samba-libs-debuginfo-32bit-4.2.4-27.1
libwbclient-devel-4.2.4-27.1
samba-winbind-debuginfo-4.2.4-27.1
libdcerpc-atsvc0-debuginfo-32bit-4.2.4-27.1
samba-core-devel-4.2.4-27.1
libnetapi0-4.2.4-27.1
libnetapi0-32bit-4.2.4-27.1
libsamba-policy0-debuginfo-32bit-4.2.4-27.1
samba-python-4.2.4-27.1
libndr-krb5pac0-4.2.4-27.1
libwbclient0-4.2.4-27.1
ctdb-tests-debuginfo-4.2.4-27.1
samba-client-debuginfo-4.2.4-27.1
ctdb-devel-4.2.4-27.1
libndr-krb5pac0-debuginfo-4.2.4-27.1
ctdb-debuginfo-4.2.4-27.1
libsmbclient-raw0-32bit-4.2.4-27.1
samba-debuginfo-32bit-4.2.4-27.1
samba-python-debuginfo-4.2.4-27.1
libnetapi0-debuginfo-4.2.4-27.1
samba-test-4.2.4-27.1
libtevent-util0-debuginfo-32bit-4.2.4-27.1
libndr-standard0-4.2.4-27.1
libsamba-credentials0-debuginfo-32bit-4.2.4-27.1
libdcerpc-samr0-4.2.4-27.1
libsamba-policy0-32bit-4.2.4-27.1
libsmbconf0-32bit-4.2.4-27.1
libsamba-hostconfig0-debuginfo-32bit-4.2.4-27.1
samba-libs-4.2.4-27.1
samba-client-4.2.4-27.1
libsamba-hostconfig0-debuginfo-4.2.4-27.1
libsamba-passdb0-debuginfo-32bit-4.2.4-27.1
libndr-devel-4.2.4-27.1
libsamba-passdb0-4.2.4-27.1

libsamba-hostconfig-devel-4.2.4-27.1
libsamba-util0-32bit-4.2.4-27.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-27.1
samba-test-devel-4.2.4-27.1
libnetapi0-debuginfo-32bit-4.2.4-27.1
samba-test-debuginfo-4.2.4-27.1
libsamba-hostconfig0-32bit-4.2.4-27.1
libdcerpc-samr0-32bit-4.2.4-27.1
libndr-nbt0-4.2.4-27.1
libsamdb0-debuginfo-4.2.4-27.1
libsmbconf0-4.2.4-27.1
libndr-krb5pac0-debuginfo-32bit-4.2.4-27.1
libdcerpc-atsvc0-4.2.4-27.1
libregistry0-4.2.4-27.1
libsamba-credentials0-debuginfo-4.2.4-27.1
samba-pidl-4.2.4-27.1
libtevent-util-devel-4.2.4-27.1
libdcerpc0-32bit-4.2.4-27.1
libtevent-util0-4.2.4-27.1
libsmbclient0-debuginfo-32bit-4.2.4-27.1
libtevent-util0-32bit-4.2.4-27.1
samba-winbind-32bit-4.2.4-27.1
libwbclient0-debuginfo-4.2.4-27.1
libndr0-4.2.4-27.1
libsamba-util0-4.2.4-27.1
libsamdb0-32bit-4.2.4-27.1
libsmbldap0-32bit-4.2.4-27.1
libsamba-policy-devel-4.2.4-27.1
libsamdb-devel-4.2.4-27.1
libdcerpc0-4.2.4-27.1
libsmbconf-devel-4.2.4-27.1
libsmbconf0-debuginfo-32bit-4.2.4-27.1
libgensec0-debuginfo-4.2.4-27.1
libsmbldap0-debuginfo-32bit-4.2.4-27.1
libsamba-passdb-devel-4.2.4-27.1
libsamba-passdb0-debuginfo-4.2.4-27.1
libsamba-policy0-debuginfo-4.2.4-27.1
libndr-krb5pac0-32bit-4.2.4-27.1
libndr-nbt0-debuginfo-4.2.4-27.1
ctdb-tests-4.2.4-27.1
samba-client-32bit-4.2.4-27.1
libsmbclient0-32bit-4.2.4-27.1
libndr-nbt-devel-4.2.4-27.1
libsamdb0-debuginfo-32bit-4.2.4-27.1
libdcerpc-atsvc0-debuginfo-4.2.4-27.1
libtevent-util0-debuginfo-4.2.4-27.1
libdcerpc0-debuginfo-4.2.4-27.1
libdcerpc-samr0-debuginfo-4.2.4-27.1
samba-libs-debuginfo-4.2.4-27.1
libndr-standard0-32bit-4.2.4-27.1
samba-libs-32bit-4.2.4-27.1
libndr0-32bit-4.2.4-27.1
samba-4.2.4-27.1
libndr0-debuginfo-4.2.4-27.1
libsmbldap0-debuginfo-4.2.4-27.1
libdcerpc-samr-devel-4.2.4-27.1
libsamba-util-devel-4.2.4-27.1
libsamba-credentials-devel-4.2.4-27.1
libsamba-policy0-4.2.4-27.1
libdcerpc-atsvc0-32bit-4.2.4-27.1

libsamba-credentials0-4.2.4-27.1
libdcerpc-binding0-debuginfo-4.2.4-27.1
libsmbldap-devel-4.2.4-27.1
libdcerpc0-debuginfo-32bit-4.2.4-27.1
libsamba-util0-debuginfo-32bit-4.2.4-27.1
libndr-krb5pac-devel-4.2.4-27.1
libsamba-hostconfig0-4.2.4-27.1
samba-client-debuginfo-32bit-4.2.4-27.1
libsmbclient0-4.2.4-27.1
libndr0-debuginfo-32bit-4.2.4-27.1
libndr-nbt0-32bit-4.2.4-27.1
libsamdb0-4.2.4-27.1
libsmbclient-raw0-debuginfo-4.2.4-27.1
libwbclient0-32bit-4.2.4-27.1
libgensec0-debuginfo-32bit-4.2.4-27.1
libgensec0-32bit-4.2.4-27.1
ctdb-4.2.4-27.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-27.1
libsmbclient0-debuginfo-4.2.4-27.1
libdcerpc-atsvc-devel-4.2.4-27.1
samba-debugsource-4.2.4-27.1
libgensec0-4.2.4-27.1
libregistry0-debuginfo-4.2.4-27.1
libnetapi-devel-4.2.4-27.1
samba-winbind-4.2.4-27.1
libwbclient0-debuginfo-32bit-4.2.4-27.1
libsmbclient-raw-devel-4.2.4-27.1
libsamba-passsdb0-32bit-4.2.4-27.1

145870 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0548-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10166, CVE-2016-10167, CVE-2016-10168, CVE-2016-6906, CVE-2016-6912, CVE-2016-9317

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0548-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00101.html>

SuSE Linux 42.1

x86_64

gd-devel-2.1.0-19.1

gd-debugsource-2.1.0-19.1

gd-2.1.0-19.1

gd-debuginfo-32bit-2.1.0-19.1

gd-32bit-2.1.0-19.1

gd-debuginfo-2.1.0-19.1

i586

gd-devel-2.1.0-19.1

gd-debuginfo-2.1.0-19.1

gd-debugsource-2.1.0-19.1

gd-2.1.0-19.1

SuSE Linux 42.2

x86_64

gd-debuginfo-32bit-2.1.0-16.1

gd-32bit-2.1.0-16.1

gd-debugsource-2.1.0-16.1

gd-2.1.0-16.1

gd-debuginfo-2.1.0-16.1

gd-devel-2.1.0-16.1

i586

gd-devel-2.1.0-16.1

gd-debuginfo-2.1.0-16.1

gd-2.1.0-16.1

gd-debugsource-2.1.0-16.1

145872 - SuSE Linux 42.2 openSUSE-SU-2017:1629-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000366

Description

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

openSUSE-SU-2017:1629-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00075.html>

SuSE Linux 42.2

i586

glibc-obsolete-debuginfo-2.22-4.9.1

glibc-debuginfo-2.22-4.9.1

nscd-debuginfo-2.22-4.9.1

glibc-devel-2.22-4.9.1

glibc-devel-debuginfo-2.22-4.9.1

glibc-obsolete-2.22-4.9.1

nscd-2.22-4.9.1

glibc-debugsource-2.22-4.9.1

glibc-extra-debuginfo-2.22-4.9.1

glibc-devel-static-2.22-4.9.1

glibc-locale-debuginfo-2.22-4.9.1

glibc-locale-2.22-4.9.1

glibc-utils-debuginfo-2.22-4.9.1

glibc-extra-2.22-4.9.1

glibc-utils-debugsource-2.22-4.9.1

glibc-2.22-4.9.1

glibc-profile-2.22-4.9.1

glibc-utils-2.22-4.9.1

i686

glibc-2.22-4.9.1

glibc-profile-2.22-4.9.1

glibc-locale-2.22-4.9.1

glibc-debuginfo-2.22-4.9.1
glibc-devel-2.22-4.9.1
glibc-locale-debuginfo-2.22-4.9.1
glibc-devel-debuginfo-2.22-4.9.1
glibc-devel-static-2.22-4.9.1
glibc-debugsource-2.22-4.9.1

noarch
glibc-info-2.22-4.9.1
glibc-i18ndata-2.22-4.9.1
glibc-html-2.22-4.9.1

x86_64
glibc-devel-static-32bit-2.22-4.9.1
glibc-debuginfo-2.22-4.9.1
glibc-locale-32bit-2.22-4.9.1
nscd-debuginfo-2.22-4.9.1
glibc-devel-2.22-4.9.1
glibc-devel-debuginfo-2.22-4.9.1
glibc-locale-debuginfo-32bit-2.22-4.9.1
nscd-2.22-4.9.1
glibc-devel-debuginfo-32bit-2.22-4.9.1
glibc-debugsource-2.22-4.9.1
glibc-profile-32bit-2.22-4.9.1
glibc-extra-debuginfo-2.22-4.9.1
glibc-devel-32bit-2.22-4.9.1
glibc-devel-static-2.22-4.9.1
glibc-locale-debuginfo-2.22-4.9.1
glibc-locale-2.22-4.9.1
glibc-utils-32bit-2.22-4.9.1
glibc-utils-debuginfo-2.22-4.9.1
glibc-extra-2.22-4.9.1
glibc-debuginfo-32bit-2.22-4.9.1
glibc-utils-debugsource-2.22-4.9.1
glibc-2.22-4.9.1
glibc-utils-debuginfo-32bit-2.22-4.9.1
glibc-profile-2.22-4.9.1
glibc-32bit-2.22-4.9.1
glibc-utils-2.22-4.9.1

145878 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2183-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2005-4900, CVE-2017-9800

Description

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

openSUSE-SU-2017:2183-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00078.html>

SuSE Linux 42.2

x86_64

subversion-server-debuginfo-1.9.7-5.3.1
libsvn_auth_kwallet-1-0-1.9.7-5.3.1
subversion-python-debuginfo-1.9.7-5.3.1
subversion-devel-1.9.7-5.3.1
subversion-tools-debuginfo-1.9.7-5.3.1
subversion-debuginfo-1.9.7-5.3.1
libsvn_auth_gnome_keyring-1-0-debuginfo-1.9.7-5.3.1
subversion-debugsource-1.9.7-5.3.1
subversion-ruby-debuginfo-1.9.7-5.3.1
subversion-perl-1.9.7-5.3.1
subversion-tools-1.9.7-5.3.1
libsvn_auth_kwallet-1-0-debuginfo-1.9.7-5.3.1
subversion-1.9.7-5.3.1
subversion-python-1.9.7-5.3.1
subversion-ruby-1.9.7-5.3.1
subversion-server-1.9.7-5.3.1
libsvn_auth_gnome_keyring-1-0-1.9.7-5.3.1
subversion-perl-debuginfo-1.9.7-5.3.1
subversion-python-ctypes-1.9.7-5.3.1

noarch

subversion-bash-completion-1.9.7-5.3.1

SuSE Linux 42.3

i586

subversion-server-debuginfo-1.9.7-8.1
subversion-tools-1.9.7-8.1
libsvn_auth_gnome_keyring-1-0-1.9.7-8.1
subversion-debugsource-1.9.7-8.1
libsvn_auth_gnome_keyring-1-0-debuginfo-1.9.7-8.1
subversion-debuginfo-1.9.7-8.1
subversion-tools-debuginfo-1.9.7-8.1
subversion-python-ctypes-1.9.7-8.1
subversion-python-1.9.7-8.1
subversion-perl-debuginfo-1.9.7-8.1
subversion-devel-1.9.7-8.1
subversion-ruby-debuginfo-1.9.7-8.1
subversion-python-debuginfo-1.9.7-8.1
subversion-1.9.7-8.1
subversion-ruby-1.9.7-8.1
libsvn_auth_kwallet-1-0-debuginfo-1.9.7-8.1
subversion-server-1.9.7-8.1
libsvn_auth_kwallet-1-0-1.9.7-8.1
subversion-perl-1.9.7-8.1

noarch

subversion-bash-completion-1.9.7-8.1

x86_64

subversion-server-debuginfo-1.9.7-8.1
subversion-tools-1.9.7-8.1
libsvn_auth_gnome_keyring-1-0-1.9.7-8.1
subversion-debugsource-1.9.7-8.1
libsvn_auth_gnome_keyring-1-0-debuginfo-1.9.7-8.1
subversion-debuginfo-1.9.7-8.1
subversion-tools-debuginfo-1.9.7-8.1
subversion-python-ctypes-1.9.7-8.1
subversion-python-1.9.7-8.1
subversion-perl-debuginfo-1.9.7-8.1
subversion-devel-1.9.7-8.1

subversion-ruby-debuginfo-1.9.7-8.1
subversion-python-debuginfo-1.9.7-8.1
subversion-1.9.7-8.1
subversion-ruby-1.9.7-8.1
libsvn_auth_kwallet-1-0-debuginfo-1.9.7-8.1
subversion-server-1.9.7-8.1
libsvn_auth_kwallet-1-0-1.9.7-8.1
subversion-perl-1.9.7-8.1

145883 - SuSE Linux 42.2 openSUSE-SU-2017:1823-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10965, CVE-2017-10966

Description

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

openSUSE-SU-2017:1823-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00044.html>

SuSE Linux 42.2

x86_64

irssi-1.0.4-14.10.1

irssi-debugsource-1.0.4-14.10.1

irssi-devel-1.0.4-14.10.1

irssi-debuginfo-1.0.4-14.10.1

i586

irssi-1.0.4-14.10.1

irssi-debugsource-1.0.4-14.10.1

irssi-devel-1.0.4-14.10.1

irssi-debuginfo-1.0.4-14.10.1

145884 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0290-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

openSUSE-SU-2017:0290-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00146.html>

SuSE Linux 42.1

x86_64

xorg-x11-Xvnc-debuginfo-1.5.0-27.1
tigervnc-1.5.0-27.1
xorg-x11-Xvnc-1.5.0-27.1
tigervnc-debuginfo-1.5.0-27.1
tigervnc-debugsource-1.5.0-27.1

i586
xorg-x11-Xvnc-debuginfo-1.5.0-27.1
tigervnc-1.5.0-27.1
xorg-x11-Xvnc-1.5.0-27.1
tigervnc-debuginfo-1.5.0-27.1
tigervnc-debugsource-1.5.0-27.1

SuSE Linux 42.2
x86_64
tigervnc-debuginfo-1.6.0-6.1
libXvnc-devel-1.6.0-6.1
tigervnc-debugsource-1.6.0-6.1
xorg-x11-Xvnc-debuginfo-1.6.0-6.1
libXvnc1-debuginfo-1.6.0-6.1
tigervnc-1.6.0-6.1
libXvnc1-1.6.0-6.1
xorg-x11-Xvnc-1.6.0-6.1

i586
tigervnc-debuginfo-1.6.0-6.1
libXvnc-devel-1.6.0-6.1
tigervnc-debugsource-1.6.0-6.1
xorg-x11-Xvnc-debuginfo-1.6.0-6.1
libXvnc1-debuginfo-1.6.0-6.1
tigervnc-1.6.0-6.1
libXvnc1-1.6.0-6.1
xorg-x11-Xvnc-1.6.0-6.1

145886 - SuSE Linux 42.3 openSUSE-SU-2017:2182-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2182-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00064.html>

SuSE Linux 42.3
i586
git-daemon-debuginfo-2.13.5-3.1
git-gui-2.13.5-3.1
git-credential-gnome-keyring-2.13.5-3.1
git-web-2.13.5-3.1
git-credential-gnome-keyring-debuginfo-2.13.5-3.1
git-core-debuginfo-2.13.5-3.1

git-core-2.13.5-3.1
git-debugsource-2.13.5-3.1
git-arch-2.13.5-3.1
git-svn-debuginfo-2.13.5-3.1
git-svn-2.13.5-3.1
git-cvs-2.13.5-3.1
git-2.13.5-3.1
git-daemon-2.13.5-3.1
gitk-2.13.5-3.1
git-email-2.13.5-3.1

noarch
git-doc-2.13.5-3.1

x86_64
git-daemon-debuginfo-2.13.5-3.1
git-gui-2.13.5-3.1
git-credential-gnome-keyring-2.13.5-3.1
git-web-2.13.5-3.1
git-credential-gnome-keyring-debuginfo-2.13.5-3.1
git-core-debuginfo-2.13.5-3.1
git-core-2.13.5-3.1
git-debugsource-2.13.5-3.1
git-arch-2.13.5-3.1
git-svn-debuginfo-2.13.5-3.1
git-svn-2.13.5-3.1
git-cvs-2.13.5-3.1
git-2.13.5-3.1
git-daemon-2.13.5-3.1
gitk-2.13.5-3.1
git-email-2.13.5-3.1

145887 - SuSE Linux 42.2 openSUSE-SU-2017:1433-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10190, CVE-2016-10191, CVE-2016-10192, CVE-2016-9561, CVE-2017-7863, CVE-2017-7865, CVE-2017-7866

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1433-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00100.html>

SuSE Linux 42.2

x86_64
libavcodec56-debuginfo-32bit-2.8.11-25.3.1
libavcodec56-2.8.11-25.3.1
libavfilter5-debuginfo-32bit-2.8.11-25.3.1
libavformat56-debuginfo-32bit-2.8.11-25.3.1
libavdevice56-debuginfo-32bit-2.8.11-25.3.1
libswscale3-debuginfo-2.8.11-25.3.1
libswresample1-32bit-2.8.11-25.3.1
libavutil54-debuginfo-2.8.11-25.3.1

libswresample1-debuginfo-32bit-2.8.11-25.3.1
ffmpeg2-debugsource-2.8.11-25.3.1
libavfilter5-32bit-2.8.11-25.3.1
libavdevice56-2.8.11-25.3.1
libavdevice56-32bit-2.8.11-25.3.1
libswresample1-2.8.11-25.3.1
libavresample2-debuginfo-32bit-2.8.11-25.3.1
ffmpeg2-devel-2.8.11-25.3.1
libavformat56-2.8.11-25.3.1
libswscale3-2.8.11-25.3.1
libpostproc53-32bit-2.8.11-25.3.1
libavfilter5-debuginfo-2.8.11-25.3.1
libavcodec56-debuginfo-2.8.11-25.3.1
libavdevice56-debuginfo-2.8.11-25.3.1
libavresample2-2.8.11-25.3.1
libavutil54-debuginfo-32bit-2.8.11-25.3.1
libavresample2-debuginfo-2.8.11-25.3.1
libswscale3-32bit-2.8.11-25.3.1
libavformat56-32bit-2.8.11-25.3.1
libpostproc53-2.8.11-25.3.1
libpostproc53-debuginfo-32bit-2.8.11-25.3.1
libavcodec56-32bit-2.8.11-25.3.1
libswresample1-debuginfo-2.8.11-25.3.1
libavformat56-debuginfo-2.8.11-25.3.1
libavfilter5-2.8.11-25.3.1
libavutil54-2.8.11-25.3.1
libavutil54-32bit-2.8.11-25.3.1
libavresample2-32bit-2.8.11-25.3.1
libswscale3-debuginfo-32bit-2.8.11-25.3.1
libpostproc53-debuginfo-2.8.11-25.3.1

i586

libavfilter5-debuginfo-2.8.11-25.3.1
libavdevice56-2.8.11-25.3.1
libavresample2-debuginfo-2.8.11-25.3.1
ffmpeg2-debugsource-2.8.11-25.3.1
ffmpeg2-devel-2.8.11-25.3.1
libswscale3-debuginfo-2.8.11-25.3.1
libavdevice56-debuginfo-2.8.11-25.3.1
libavcodec56-2.8.11-25.3.1
libavresample2-2.8.11-25.3.1
libavutil54-debuginfo-2.8.11-25.3.1
libavutil54-2.8.11-25.3.1
libavcodec56-debuginfo-2.8.11-25.3.1
libavformat56-2.8.11-25.3.1
libpostproc53-2.8.11-25.3.1
libswresample1-debuginfo-2.8.11-25.3.1
libavformat56-debuginfo-2.8.11-25.3.1
libswscale3-2.8.11-25.3.1
libpostproc53-debuginfo-2.8.11-25.3.1
libavfilter5-2.8.11-25.3.1
libswresample1-2.8.11-25.3.1

145890 - SuSE Linux 42.2 openSUSE-SU-2017:0664-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6467, CVE-2017-6468, CVE-2017-6469, CVE-2017-6470, CVE-2017-6471, CVE-2017-6472, CVE-2017-6473, CVE-2017-6474

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0664-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00024.html>

SuSE Linux 42.2
x86_64
wireshark-2.2.5-12.1
wireshark-debuginfo-2.2.5-12.1
wireshark-devel-2.2.5-12.1
wireshark-ui-qt-debuginfo-2.2.5-12.1
wireshark-ui-gtk-2.2.5-12.1
wireshark-ui-gtk-debuginfo-2.2.5-12.1
wireshark-ui-qt-2.2.5-12.1
wireshark-debugsource-2.2.5-12.1

145891 - SuSE Linux 42.2 openSUSE-SU-2017:0270-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5501, CVE-2016-5538, CVE-2016-5605, CVE-2016-5608, CVE-2016-5610, CVE-2016-5611, CVE-2016-561313

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0270-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00136.html>

SuSE Linux 42.2
x86_64
virtualbox-guest-x11-5.1.12-6.1
virtualbox-5.1.12-6.1
virtualbox-guest-tools-5.1.12-6.1
virtualbox-websrv-debuginfo-5.1.12-6.1
virtualbox-guest-kmp-default-debuginfo-5.1.12_k4.4.36_8-6.1
virtualbox-qt-5.1.12-6.1
virtualbox-guest-kmp-default-5.1.12_k4.4.36_8-6.1
virtualbox-debuginfo-5.1.12-6.1
virtualbox-qt-debuginfo-5.1.12-6.1
virtualbox-devel-5.1.12-6.1
python-virtualbox-5.1.12-6.1
virtualbox-debugsource-5.1.12-6.1
virtualbox-websrv-5.1.12-6.1
virtualbox-guest-x11-debuginfo-5.1.12-6.1
virtualbox-guest-tools-debuginfo-5.1.12-6.1
virtualbox-host-kmp-default-debuginfo-5.1.12_k4.4.36_8-6.1
python-virtualbox-debuginfo-5.1.12-6.1
virtualbox-host-kmp-default-5.1.12_k4.4.36_8-6.1

noarch
virtualbox-host-source-5.1.12-6.1
virtualbox-guest-desktop-icons-5.1.12-6.1

145892 - SuSE Linux 42.2 openSUSE-SU-2017:1121-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10190, CVE-2016-10191, CVE-2016-10192, CVE-2017-7859, CVE-2017-7862, CVE-2017-7863, CVE-2017-7865, CVE-2017-7866

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1121-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00106.html>

SuSE Linux 42.2

x86_64

libavutil55-debuginfo-32bit-3.3-6.6.1
libavresample3-debuginfo-3.3-6.6.1
libavformat57-debuginfo-3.3-6.6.1
libswresample2-debuginfo-3.3-6.6.1
libavresample3-32bit-3.3-6.6.1
libavutil55-debuginfo-3.3-6.6.1
libavdevice57-32bit-3.3-6.6.1
libpostproc54-32bit-3.3-6.6.1
libavcodec57-debuginfo-32bit-3.3-6.6.1
libswscale4-3.3-6.6.1
libavresample-devel-3.3-6.6.1
libavfilter6-debuginfo-32bit-3.3-6.6.1
libswscale4-32bit-3.3-6.6.1
libavdevice-devel-3.3-6.6.1
libavcodec-devel-3.3-6.6.1
libswresample2-3.3-6.6.1
libavdevice57-debuginfo-3.3-6.6.1
libavformat57-debuginfo-32bit-3.3-6.6.1
libavcodec57-3.3-6.6.1
libswresample-devel-3.3-6.6.1
libavutil55-32bit-3.3-6.6.1
libavresample3-debuginfo-32bit-3.3-6.6.1
libavfilter6-debuginfo-3.3-6.6.1
libavdevice57-debuginfo-32bit-3.3-6.6.1
libavdevice57-3.3-6.6.1
libswresample2-debuginfo-32bit-3.3-6.6.1
libpostproc54-3.3-6.6.1
libswresample2-32bit-3.3-6.6.1
libavformat57-32bit-3.3-6.6.1
libavfilter-devel-3.3-6.6.1
libpostproc54-debuginfo-3.3-6.6.1
libavcodec57-debuginfo-3.3-6.6.1
libavcodec57-32bit-3.3-6.6.1
libavformat57-3.3-6.6.1

libavformat-devel-3.3-6.6.1
libswscale4-debuginfo-3.3-6.6.1
ffmpeg-debuginfo-3.3-6.6.1
libavutil55-3.3-6.6.1
libavfilter6-32bit-3.3-6.6.1
libswscale4-debuginfo-32bit-3.3-6.6.1
ffmpeg-3.3-6.6.1
ffmpeg-debugsource-3.3-6.6.1
libpostproc-devel-3.3-6.6.1
libswscale-devel-3.3-6.6.1
libavfilter6-3.3-6.6.1
libpostproc54-debuginfo-32bit-3.3-6.6.1
libavresample3-3.3-6.6.1
libavutil-devel-3.3-6.6.1

i586

libavresample3-debuginfo-3.3-6.6.1
libavformat57-debuginfo-3.3-6.6.1
libswresample2-debuginfo-3.3-6.6.1
libavutil55-debuginfo-3.3-6.6.1
libswscale4-3.3-6.6.1
libavresample-devel-3.3-6.6.1
libavdevice-devel-3.3-6.6.1
libavcodec-devel-3.3-6.6.1
libswresample2-3.3-6.6.1
libavdevice57-debuginfo-3.3-6.6.1
libavcodec57-3.3-6.6.1
libswresample-devel-3.3-6.6.1
libavfilter6-debuginfo-3.3-6.6.1
libavdevice57-3.3-6.6.1
libpostproc54-3.3-6.6.1
libavfilter-devel-3.3-6.6.1
libpostproc54-debuginfo-3.3-6.6.1
libavcodec57-debuginfo-3.3-6.6.1
libavformat57-3.3-6.6.1
libavformat-devel-3.3-6.6.1
libswscale4-debuginfo-3.3-6.6.1
ffmpeg-debuginfo-3.3-6.6.1
libavutil55-3.3-6.6.1
ffmpeg-3.3-6.6.1
ffmpeg-debugsource-3.3-6.6.1
libpostproc-devel-3.3-6.6.1
libswscale-devel-3.3-6.6.1
libavfilter6-3.3-6.6.1
libavresample3-3.3-6.6.1
libavutil-devel-3.3-6.6.1

145893 - SuSE Linux 42.1 openSUSE-SU-2017:0511-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5953

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0511-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00090.html>

SuSE Linux 42.1
i586
vim-7.4.326-11.1
gvim-7.4.326-11.1
vim-debugsource-7.4.326-11.1
vim-debuginfo-7.4.326-11.1
gvim-debuginfo-7.4.326-11.1

noarch
vim-data-7.4.326-11.1

x86_64
vim-7.4.326-11.1
gvim-7.4.326-11.1
vim-debugsource-7.4.326-11.1
vim-debuginfo-7.4.326-11.1
gvim-debuginfo-7.4.326-11.1

145894 - SuSE Linux 42.2 openSUSE-SU-2017:1140-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4997, CVE-2016-4998, CVE-2017-2671, CVE-2017-7187, CVE-2017-7261, CVE-2017-7294, CVE-2017-7308, CVE-2017-7374, CVE-2017-7616, CVE-2017-7618

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1140-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00001.html>

SuSE Linux 42.2
x86_64
kernel-default-devel-4.4.62-18.6.1
kernel-obs-build-4.4.62-18.6.1
kernel-debug-base-debuginfo-4.4.62-18.6.1
kernel-default-4.4.62-18.6.1
kernel-syms-4.4.62-18.6.1
kernel-default-base-4.4.62-18.6.1
kernel-debug-devel-debuginfo-4.4.62-18.6.1
kernel-default-debuginfo-4.4.62-18.6.1
kernel-debug-debuginfo-4.4.62-18.6.1
kernel-vanilla-debugsource-4.4.62-18.6.1
kernel-debug-devel-4.4.62-18.6.1
kernel-vanilla-4.4.62-18.6.1
kernel-debug-base-4.4.62-18.6.1
kernel-obs-qa-4.4.62-18.6.1
kernel-default-base-debuginfo-4.4.62-18.6.1
kernel-vanilla-devel-4.4.62-18.6.1

kernel-obs-build-debugsource-4.4.62-18.6.1
kernel-debug-debugsource-4.4.62-18.6.1
kernel-vanilla-debuginfo-4.4.62-18.6.1
kernel-debug-4.4.62-18.6.1
kernel-vanilla-base-4.4.62-18.6.1
kernel-vanilla-base-debuginfo-4.4.62-18.6.1
kernel-default-debugsource-4.4.62-18.6.1

noarch
kernel-docs-4.4.62-18.6.2
kernel-docs-html-4.4.62-18.6.2
kernel-source-vanilla-4.4.62-18.6.1
kernel-source-4.4.62-18.6.1
kernel-devel-4.4.62-18.6.1
kernel-docs-pdf-4.4.62-18.6.2
kernel-macros-4.4.62-18.6.1

145896 - SuSE Linux 42.1 openSUSE-SU-2017:1205-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0860

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1205-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00030.html>

SuSE Linux 42.1

i586
update-alternatives-debugsource-1.16.10-14.1
dpkg-debuginfo-1.16.10-14.1
dpkg-debugsource-1.16.10-14.1
update-alternatives-debuginfo-1.16.10-14.1
dpkg-devel-1.16.10-14.1
dpkg-1.16.10-14.1
update-alternatives-1.16.10-14.1

noarch
dpkg-lang-1.16.10-14.1

x86_64
update-alternatives-debugsource-1.16.10-14.1
dpkg-debuginfo-1.16.10-14.1
dpkg-debugsource-1.16.10-14.1
update-alternatives-debuginfo-1.16.10-14.1
dpkg-devel-1.16.10-14.1
dpkg-1.16.10-14.1
update-alternatives-1.16.10-14.1

145897 - SuSE Linux 42.2 openSUSE-SU-2017:1811-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5953, CVE-2017-6349, CVE-2017-6350

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1811-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00039.html>

SuSE Linux 42.2

i586

gvim-7.4.326-10.3.1

vim-debugsource-7.4.326-10.3.1

gvim-debuginfo-7.4.326-10.3.1

vim-debuginfo-7.4.326-10.3.1

vim-7.4.326-10.3.1

noarch

vim-data-7.4.326-10.3.1

x86_64

gvim-7.4.326-10.3.1

vim-debugsource-7.4.326-10.3.1

gvim-debuginfo-7.4.326-10.3.1

vim-debuginfo-7.4.326-10.3.1

vim-7.4.326-10.3.1

160292 - CentOS 6 CESA-2017-2534 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2534

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-August/022528.html>

CentOS 6

x86_64

thunderbird-52.3.0-1.el6.centos

i686

thunderbird-52.3.0-1.el6.centos

170853 - Amazon Linux AMI ALAS-2017-876 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0553

Description

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

ALAS-2017-876

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2017-876.html>

Amazon Linux AMI

x86_64

libnl3-debuginfo-3.2.28-4.6.amzn1

libnl3-3.2.28-4.6.amzn1

libnl3-cli-3.2.28-4.6.amzn1

libnl3-devel-3.2.28-4.6.amzn1

libnl3-doc-3.2.28-4.6.amzn1

i686

libnl3-debuginfo-3.2.28-4.6.amzn1

libnl3-doc-3.2.28-4.6.amzn1

libnl3-cli-3.2.28-4.6.amzn1

libnl3-devel-3.2.28-4.6.amzn1

libnl3-3.2.28-4.6.amzn1

170854 - Amazon Linux AMI ALAS-2017-877 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779

Description

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

ALAS-2017-877

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2017-877.html>

Amazon Linux AMI

x86_64

glibc-utils-2.17-196.172.amzn1

glibc-headers-2.17-196.172.amzn1

glibc-static-2.17-196.172.amzn1

glibc-debuginfo-common-2.17-196.172.amzn1

glibc-common-2.17-196.172.amzn1

glibc-2.17-196.172.amzn1

nscd-2.17-196.172.amzn1

glibc-devel-2.17-196.172.amzn1

glibc-debuginfo-2.17-196.172.amzn1

i686
glibc-utils-2.17-196.172.amzn1
glibc-devel-2.17-196.172.amzn1
glibc-debuginfo-common-2.17-196.172.amzn1
nscd-2.17-196.172.amzn1
glibc-common-2.17-196.172.amzn1
glibc-2.17-196.172.amzn1
glibc-headers-2.17-196.172.amzn1
glibc-static-2.17-196.172.amzn1
glibc-debuginfo-2.17-196.172.amzn1

170859 - Amazon Linux AMI ALAS-2017-882 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000117

Description

The scan detected that the host is missing the following update:
ALAS-2017-882

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-882.html>

Amazon Linux AMI

i686
git-2.13.5-1.53.amzn1
git-daemon-2.13.5-1.53.amzn1
git-svn-2.13.5-1.53.amzn1
git-debuginfo-2.13.5-1.53.amzn1

noarch
git-all-2.13.5-1.53.amzn1
git-cvs-2.13.5-1.53.amzn1
emacs-git-2.13.5-1.53.amzn1
git-p4-2.13.5-1.53.amzn1
emacs-git-el-2.13.5-1.53.amzn1
git-hg-2.13.5-1.53.amzn1
git-email-2.13.5-1.53.amzn1
gitweb-2.13.5-1.53.amzn1
git-bzr-2.13.5-1.53.amzn1
perl-Git-SVN-2.13.5-1.53.amzn1
perl-Git-2.13.5-1.53.amzn1

x86_64
git-2.13.5-1.53.amzn1
git-daemon-2.13.5-1.53.amzn1
git-svn-2.13.5-1.53.amzn1
git-debuginfo-2.13.5-1.53.amzn1

170860 - Amazon Linux AMI ALAS-2017-883 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9800

Description

The scan detected that the host is missing the following update:
ALAS-2017-883

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-883.html>

Amazon Linux AMI

x86_64

subversion-python27-1.9.7-1.58.amzn1
subversion-1.9.7-1.58.amzn1
subversion-libs-1.9.7-1.58.amzn1
subversion-perl-1.9.7-1.58.amzn1
subversion-debuginfo-1.9.7-1.58.amzn1
subversion-tools-1.9.7-1.58.amzn1
subversion-python26-1.9.7-1.58.amzn1
mod_dav_svn-1.9.7-1.54.amzn1
mod24_dav_svn-1.9.7-1.58.amzn1
subversion-javahl-1.9.7-1.58.amzn1
mod_dav_svn-debuginfo-1.9.7-1.54.amzn1
subversion-devel-1.9.7-1.58.amzn1
subversion-ruby-1.9.7-1.58.amzn1

i686

subversion-python27-1.9.7-1.58.amzn1
subversion-perl-1.9.7-1.58.amzn1
subversion-libs-1.9.7-1.58.amzn1
subversion-tools-1.9.7-1.58.amzn1
subversion-debuginfo-1.9.7-1.58.amzn1
subversion-python26-1.9.7-1.58.amzn1
subversion-javahl-1.9.7-1.58.amzn1
mod_dav_svn-1.9.7-1.54.amzn1
subversion-devel-1.9.7-1.58.amzn1
mod24_dav_svn-1.9.7-1.58.amzn1
subversion-1.9.7-1.58.amzn1
mod_dav_svn-debuginfo-1.9.7-1.54.amzn1
subversion-ruby-1.9.7-1.58.amzn1

170861 - Amazon Linux AMI ALAS-2017-884 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547

Description

The scan detected that the host is missing the following update:
ALAS-2017-884

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-884.html>

Amazon Linux AMI

x86_64

postgresql92-libs-9.2.22-1.61.amzn1
postgresql93-9.3.18-1.64.amzn1
postgresql93-plpython26-9.3.18-1.64.amzn1
postgresql93-plpython27-9.3.18-1.64.amzn1
postgresql93-docs-9.3.18-1.64.amzn1
postgresql92-pltcl-9.2.22-1.61.amzn1
postgresql93-libs-9.3.18-1.64.amzn1
postgresql93-server-9.3.18-1.64.amzn1
postgresql92-contrib-9.2.22-1.61.amzn1
postgresql92-test-9.2.22-1.61.amzn1
postgresql92-server-compat-9.2.22-1.61.amzn1
postgresql92-plpython27-9.2.22-1.61.amzn1
postgresql93-debuginfo-9.3.18-1.64.amzn1
postgresql93-contrib-9.3.18-1.64.amzn1
postgresql93-plperl-9.3.18-1.64.amzn1
postgresql92-plperl-9.2.22-1.61.amzn1
postgresql92-9.2.22-1.61.amzn1
postgresql93-pltcl-9.3.18-1.64.amzn1
postgresql92-devel-9.2.22-1.61.amzn1
postgresql92-server-9.2.22-1.61.amzn1
postgresql92-debuginfo-9.2.22-1.61.amzn1
postgresql92-plpython26-9.2.22-1.61.amzn1
postgresql92-docs-9.2.22-1.61.amzn1
postgresql93-test-9.3.18-1.64.amzn1
postgresql93-devel-9.3.18-1.64.amzn1

i686

postgresql92-docs-9.2.22-1.61.amzn1
postgresql93-9.3.18-1.64.amzn1
postgresql93-plpython26-9.3.18-1.64.amzn1
postgresql93-plpython27-9.3.18-1.64.amzn1
postgresql93-docs-9.3.18-1.64.amzn1
postgresql92-pltcl-9.2.22-1.61.amzn1
postgresql92-test-9.2.22-1.61.amzn1
postgresql92-libs-9.2.22-1.61.amzn1
postgresql93-libs-9.3.18-1.64.amzn1
postgresql93-server-9.3.18-1.64.amzn1
postgresql92-contrib-9.2.22-1.61.amzn1
postgresql92-devel-9.2.22-1.61.amzn1
postgresql92-server-compat-9.2.22-1.61.amzn1
postgresql92-plpython27-9.2.22-1.61.amzn1
postgresql93-pltcl-9.3.18-1.64.amzn1
postgresql93-contrib-9.3.18-1.64.amzn1
postgresql93-plperl-9.3.18-1.64.amzn1
postgresql92-plperl-9.2.22-1.61.amzn1
postgresql92-9.2.22-1.61.amzn1
postgresql92-server-9.2.22-1.61.amzn1
postgresql92-debuginfo-9.2.22-1.61.amzn1
postgresql92-plpython26-9.2.22-1.61.amzn1
postgresql93-debuginfo-9.3.18-1.64.amzn1
postgresql93-test-9.3.18-1.64.amzn1
postgresql93-devel-9.3.18-1.64.amzn1

170862 - Amazon Linux AMI ALAS-2017-885 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

Description

The scan detected that the host is missing the following update:
ALAS-2017-885

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-885.html>

Amazon Linux AMI

x86_64

postgresql94-plpython27-9.4.13-1.69.amzn1
postgresql95-libs-9.5.8-1.73.amzn1
postgresql95-static-9.5.8-1.73.amzn1
postgresql95-devel-9.5.8-1.73.amzn1
postgresql94-docs-9.4.13-1.69.amzn1
postgresql95-9.5.8-1.73.amzn1
postgresql95-contrib-9.5.8-1.73.amzn1
postgresql95-plpython27-9.5.8-1.73.amzn1
postgresql95-test-9.5.8-1.73.amzn1
postgresql94-plpython26-9.4.13-1.69.amzn1
postgresql94-server-9.4.13-1.69.amzn1
postgresql94-test-9.4.13-1.69.amzn1
postgresql95-server-9.5.8-1.73.amzn1
postgresql95-plperl-9.5.8-1.73.amzn1
postgresql94-contrib-9.4.13-1.69.amzn1
postgresql94-devel-9.4.13-1.69.amzn1
postgresql95-debuginfo-9.5.8-1.73.amzn1
postgresql95-docs-9.5.8-1.73.amzn1
postgresql94-debuginfo-9.4.13-1.69.amzn1
postgresql94-9.4.13-1.69.amzn1
postgresql94-libs-9.4.13-1.69.amzn1
postgresql94-plperl-9.4.13-1.69.amzn1
postgresql95-plpython26-9.5.8-1.73.amzn1

i686

postgresql94-plpython27-9.4.13-1.69.amzn1
postgresql95-libs-9.5.8-1.73.amzn1
postgresql95-static-9.5.8-1.73.amzn1
postgresql95-devel-9.5.8-1.73.amzn1
postgresql94-docs-9.4.13-1.69.amzn1
postgresql95-9.5.8-1.73.amzn1
postgresql95-contrib-9.5.8-1.73.amzn1
postgresql94-test-9.4.13-1.69.amzn1
postgresql95-plpython27-9.5.8-1.73.amzn1
postgresql95-test-9.5.8-1.73.amzn1
postgresql94-plpython26-9.4.13-1.69.amzn1
postgresql94-server-9.4.13-1.69.amzn1
postgresql95-debuginfo-9.5.8-1.73.amzn1
postgresql95-server-9.5.8-1.73.amzn1
postgresql95-plperl-9.5.8-1.73.amzn1
postgresql94-contrib-9.4.13-1.69.amzn1
postgresql94-devel-9.4.13-1.69.amzn1
postgresql95-docs-9.5.8-1.73.amzn1
postgresql94-debuginfo-9.4.13-1.69.amzn1

postgresql94-9.4.13-1.69.amzn1
postgresql94-libs-9.4.13-1.69.amzn1
postgresql94-plperl-9.4.13-1.69.amzn1
postgresql95-plpython26-9.5.8-1.73.amzn1

170863 - Amazon Linux AMI ALAS-2017-886 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
ALAS-2017-886

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-886.html>

Amazon Linux AMI
noarch
aws-cfn-bootstrap-1.4-21.13.amzn1

170865 - Amazon Linux AMI ALAS-2017-878 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0634, CVE-2016-7543, CVE-2016-9401

Description

The scan detected that the host is missing the following update:
ALAS-2017-878

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-878.html>

Amazon Linux AMI
x86_64
bash-debuginfo-4.2.46-28.37.amzn1
bash-4.2.46-28.37.amzn1
bash-doc-4.2.46-28.37.amzn1

i686
bash-debuginfo-4.2.46-28.37.amzn1
bash-4.2.46-28.37.amzn1
bash-doc-4.2.46-28.37.amzn1

178489 - Gentoo Linux GLSA-201709-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2292

Description

The scan detected that the host is missing the following update:
GLSA-201709-01

Observation

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

<https://security.gentoo.org/glsa/201709-01>

Affected packages:

app-admin/mcollective < 2.11.0

192586 - Fedora Linux 26 FEDORA-2017-9899aba20e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3253

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9899aba20e

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

groovy18-1.8.9-30.fc26

192592 - Fedora Linux 26 FEDORA-2017-5617ab3b38 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12858

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5617ab3b38

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

mingw-libzip-1.2.0-3.fc26

192593 - Fedora Linux 26 FEDORA-2017-2d4ead8da9 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2d4ead8da9

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 26

libidn2-2.0.4-1.fc26

192595 - Fedora Linux 25 FEDORA-2017-fa6784d0bd Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12562

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fa6784d0bd

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 25

libsndfile-1.0.28-6.fc25

192598 - Fedora Linux 25 FEDORA-2017-57722ccd30 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-57722ccd30

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 25

libidn2-2.0.4-1.fc25

192602 - Fedora Linux 25 FEDORA-2017-6a0389a6a7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3253

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6a0389a6a7

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=2>

Fedora Core 25

groovy18-1.8.9-30.fc25

192604 - Fedora Linux 27 FEDORA-2017-09b1c3f099 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-09b1c3f099

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 27

libidn2-2.0.4-1.fc27

22326 - (SB10207) Threat Intelligence Exchange Server Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-1000364, CVE-2017-3907

Description

Multiple vulnerabilities are present in some versions of McAfee Threat Intelligence Exchange Server.

Observation

McAfee Threat Intelligence Exchange Server is a real-time threat detection and response software.

Multiple vulnerabilities are present in some versions of McAfee Threat Intelligence Exchange Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute remote arbitrary code or to obtain elevated privileges in the system.

22327 - Westermo MRD Wireless Routers Multiple Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: Medium

CVE: CVE-2016-5816, CVE-2017-12703, CVE-2017-12709

Description

Multiple vulnerabilities are present in some versions of Westermo MRD Wireless routers.

Observation

Westermo MRD Wireless routers are robust industrial data communications routers.

Multiple vulnerabilities are present in some versions of Westermo MRD Wireless routers. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code or disclose private information.

132395 - Oracle VM OVMSA-2017-0147 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-3702, CVE-2010-3703, CVE-2010-3704, CVE-2017-9776

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0147

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000776.html>

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000779.html>

OVM3.3

x86_64

poppler-0.12.4-12.el6_9

poppler-utils-0.12.4-12.el6_9

OVM3.4

x86_64

poppler-0.12.4-12.el6_9

poppler-utils-0.12.4-12.el6_9

141698 - Red Hat Enterprise Linux RHSA-2017-2550 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9776

Description

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

RHSA-2017-2550

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-August/msg00084.html>

RHEL6D

x86_64

poppler-qt-devel-0.12.4-12.el6_9
poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-debuginfo-0.12.4-12.el6_9

i386

poppler-qt-devel-0.12.4-12.el6_9
poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-debuginfo-0.12.4-12.el6_9

RHEL6S

i386

poppler-qt-devel-0.12.4-12.el6_9
poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-debuginfo-0.12.4-12.el6_9

x86_64

poppler-qt-devel-0.12.4-12.el6_9
poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9

poppler-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-debuginfo-0.12.4-12.el6_9

RHEL6WS

x86_64
poppler-qt4-0.12.4-12.el6_9
poppler-debuginfo-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9

i386

poppler-qt4-0.12.4-12.el6_9
poppler-debuginfo-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9

141702 - Red Hat Enterprise Linux RHSA-2017-2551 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9775, CVE-2017-9776

Description

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

RHSA-2017-2551

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-August/msg00083.html>

RHEL7D

x86_64
poppler-debuginfo-0.26.5-17.el7_4
poppler-cpp-devel-0.26.5-17.el7_4
poppler-qt-0.26.5-17.el7_4
poppler-demos-0.26.5-17.el7_4
poppler-glib-0.26.5-17.el7_4
poppler-devel-0.26.5-17.el7_4
poppler-utils-0.26.5-17.el7_4
poppler-qt-devel-0.26.5-17.el7_4
poppler-0.26.5-17.el7_4
poppler-cpp-0.26.5-17.el7_4
poppler-glib-devel-0.26.5-17.el7_4

RHEL7S

x86_64
poppler-debuginfo-0.26.5-17.el7_4
poppler-cpp-devel-0.26.5-17.el7_4
poppler-qt-0.26.5-17.el7_4
poppler-demos-0.26.5-17.el7_4
poppler-glib-0.26.5-17.el7_4
poppler-devel-0.26.5-17.el7_4

poppler-utils-0.26.5-17.el7_4
poppler-qt-devel-0.26.5-17.el7_4
poppler-0.26.5-17.el7_4
poppler-cpp-0.26.5-17.el7_4
poppler-glib-devel-0.26.5-17.el7_4

RHEL7WS

x86_64
poppler-debuginfo-0.26.5-17.el7_4
poppler-cpp-devel-0.26.5-17.el7_4
poppler-qt-0.26.5-17.el7_4
poppler-demos-0.26.5-17.el7_4
poppler-glib-0.26.5-17.el7_4
poppler-devel-0.26.5-17.el7_4
poppler-utils-0.26.5-17.el7_4
poppler-qt-devel-0.26.5-17.el7_4
poppler-0.26.5-17.el7_4
poppler-cpp-0.26.5-17.el7_4
poppler-glib-devel-0.26.5-17.el7_4

145507 - SuSE Linux 42.2 openSUSE-SU-2017:1885-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10971, CVE-2017-10972

Description

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

openSUSE-SU-2017:1885-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00074.html>

SuSE Linux 42.2

x86_64
xorg-x11-server-sdk-7.6_1.18.3-12.20.1
xorg-x11-server-debuginfo-7.6_1.18.3-12.20.1
xorg-x11-server-7.6_1.18.3-12.20.1
xorg-x11-server-debugsource-7.6_1.18.3-12.20.1
xorg-x11-server-extra-7.6_1.18.3-12.20.1
xorg-x11-server-extra-debuginfo-7.6_1.18.3-12.20.1
xorg-x11-server-source-7.6_1.18.3-12.20.1

i586

xorg-x11-server-sdk-7.6_1.18.3-12.20.1
xorg-x11-server-debuginfo-7.6_1.18.3-12.20.1
xorg-x11-server-7.6_1.18.3-12.20.1
xorg-x11-server-debugsource-7.6_1.18.3-12.20.1
xorg-x11-server-extra-7.6_1.18.3-12.20.1
xorg-x11-server-extra-debuginfo-7.6_1.18.3-12.20.1
xorg-x11-server-source-7.6_1.18.3-12.20.1

145509 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2273-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2017-8288

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2273-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00101.html>

SuSE Linux 42.2
x86_64
gnome-shell-3.20.4-10.3.1
gnome-shell-browser-plugin-3.20.4-10.3.1
gnome-shell-browser-plugin-debuginfo-3.20.4-10.3.1
gnome-shell-calendar-debuginfo-3.20.4-10.3.1
gnome-shell-debuginfo-3.20.4-10.3.1
gnome-shell-debugsource-3.20.4-10.3.1
gnome-shell-calendar-3.20.4-10.3.1
gnome-shell-devel-3.20.4-10.3.1

noarch
gnome-shell-lang-3.20.4-10.3.1

SuSE Linux 42.3
x86_64
gnome-shell-calendar-3.20.4-13.1
gnome-shell-calendar-debuginfo-3.20.4-13.1
gnome-shell-debuginfo-3.20.4-13.1
gnome-shell-debugsource-3.20.4-13.1
gnome-shell-3.20.4-13.1
gnome-shell-browser-plugin-debuginfo-3.20.4-13.1
gnome-shell-browser-plugin-3.20.4-13.1
gnome-shell-devel-3.20.4-13.1

noarch
gnome-shell-lang-3.20.4-13.1

145512 - SuSE Linux 42.2 openSUSE-SU-2017:1685-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2017-1000364

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1685-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00099.html>

SuSE Linux 42.2

x86_64

kernel-debug-debugsource-4.4.73-18.17.1
kernel-debug-base-debuginfo-4.4.73-18.17.1
kernel-debug-4.4.73-18.17.1
kernel-debug-devel-debuginfo-4.4.73-18.17.1
kernel-vanilla-debuginfo-4.4.73-18.17.1
kernel-vanilla-base-4.4.73-18.17.1
kernel-default-base-4.4.73-18.17.1
kernel-vanilla-devel-4.4.73-18.17.1
kernel-default-base-debuginfo-4.4.73-18.17.1
kernel-obs-qa-4.4.73-18.17.1
kernel-syms-4.4.73-18.17.1
kernel-obs-build-4.4.73-18.17.1
kernel-obs-build-debugsource-4.4.73-18.17.1
kernel-vanilla-debugsource-4.4.73-18.17.1
kernel-default-debugsource-4.4.73-18.17.1
kernel-debug-devel-4.4.73-18.17.1
kernel-vanilla-4.4.73-18.17.1
kernel-vanilla-base-debuginfo-4.4.73-18.17.1
kernel-debug-base-4.4.73-18.17.1
kernel-default-4.4.73-18.17.1
kernel-debug-debuginfo-4.4.73-18.17.1
kernel-default-devel-4.4.73-18.17.1
kernel-default-debuginfo-4.4.73-18.17.1

noarch

kernel-source-vanilla-4.4.73-18.17.1
kernel-docs-4.4.73-18.17.2
kernel-macros-4.4.73-18.17.1
kernel-source-4.4.73-18.17.1
kernel-devel-4.4.73-18.17.1
kernel-docs-pdf-4.4.73-18.17.2
kernel-docs-html-4.4.73-18.17.2

145516 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0513-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3259, CVE-2017-3260, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0513-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00092.html>

SuSE Linux 42.1

i586

java-1_7_0-openjdk-src-1.7.0.131-40.1
java-1_7_0-openjdk-1.7.0.131-40.1
java-1_7_0-openjdk-demo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.131-40.1

java-1_7_0-openjdk-bootstrap-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.131-40.1
java-1_7_0-openjdk-debugsource-1.7.0.131-40.1
java-1_7_0-openjdk-devel-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.131-40.1
java-1_7_0-openjdk-accessibility-1.7.0.131-40.1
java-1_7_0-openjdk-headless-1.7.0.131-40.1
java-1_7_0-openjdk-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.131-40.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.131-40.1

noarch

java-1_7_0-openjdk-javadoc-1.7.0.131-40.1

x86_64

java-1_7_0-openjdk-src-1.7.0.131-40.1
java-1_7_0-openjdk-1.7.0.131-40.1
java-1_7_0-openjdk-demo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.131-40.1
java-1_7_0-openjdk-debugsource-1.7.0.131-40.1
java-1_7_0-openjdk-devel-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.131-40.1
java-1_7_0-openjdk-accessibility-1.7.0.131-40.1
java-1_7_0-openjdk-headless-1.7.0.131-40.1
java-1_7_0-openjdk-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.131-40.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.131-40.1

SuSE Linux 42.2

i586

java-1_7_0-openjdk-src-1.7.0.131-40.1
java-1_7_0-openjdk-1.7.0.131-40.1
java-1_7_0-openjdk-demo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.131-40.1
java-1_7_0-openjdk-debugsource-1.7.0.131-40.1
java-1_7_0-openjdk-devel-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.131-40.1
java-1_7_0-openjdk-accessibility-1.7.0.131-40.1
java-1_7_0-openjdk-headless-1.7.0.131-40.1
java-1_7_0-openjdk-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.131-40.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.131-40.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.131-40.1

noarch

java-1_7_0-openjdk-javadoc-1.7.0.131-40.1

x86_64

java-1_7_0-openjdk-src-1.7.0.131-40.1

java-1_7_0-openjdk-1.7.0.131-40.1

java-1_7_0-openjdk-demo-1.7.0.131-40.1

java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.131-40.1

java-1_7_0-openjdk-bootstrap-1.7.0.131-40.1

java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.131-40.1

java-1_7_0-openjdk-bootstrap-headless-1.7.0.131-40.1

java-1_7_0-openjdk-debugsource-1.7.0.131-40.1

java-1_7_0-openjdk-devel-1.7.0.131-40.1

java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.131-40.1

java-1_7_0-openjdk-accessibility-1.7.0.131-40.1

java-1_7_0-openjdk-headless-1.7.0.131-40.1

java-1_7_0-openjdk-debuginfo-1.7.0.131-40.1

java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.131-40.1

java-1_7_0-openjdk-bootstrap-devel-1.7.0.131-40.1

java-1_7_0-openjdk-devel-debuginfo-1.7.0.131-40.1

java-1_7_0-openjdk-demo-debuginfo-1.7.0.131-40.1

java-1_7_0-openjdk-headless-debuginfo-1.7.0.131-40.1

145518 - SuSE Linux 42.3 openSUSE-SU-2017:1959-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11110

Description

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

openSUSE-SU-2017:1959-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00091.html>

SuSE Linux 42.3

x86_64

catdoc-0.95-10.1

catdoc-debuginfo-0.95-10.1

catdoc-debugsource-0.95-10.1

i586

catdoc-0.95-10.1

catdoc-debuginfo-0.95-10.1

catdoc-debugsource-0.95-10.1

145520 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2271-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11403, CVE-2017-9439, CVE-2017-9440, CVE-2017-9501

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2271-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00102.html>

SuSE Linux 42.2

i586

perl-PerlMagick-6.8.8.1-30.6.1
libMagick++-devel-6.8.8.1-30.6.1
libMagickCore-6_Q16-1-6.8.8.1-30.6.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.6.1
libMagick++-6_Q16-3-6.8.8.1-30.6.1
ImageMagick-devel-6.8.8.1-30.6.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.6.1
libMagickWand-6_Q16-1-6.8.8.1-30.6.1
perl-PerlMagick-debuginfo-6.8.8.1-30.6.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.6.1
ImageMagick-extra-debuginfo-6.8.8.1-30.6.1
ImageMagick-6.8.8.1-30.6.1
ImageMagick-extra-6.8.8.1-30.6.1
ImageMagick-debugsource-6.8.8.1-30.6.1
ImageMagick-debuginfo-6.8.8.1-30.6.1

noarch

ImageMagick-doc-6.8.8.1-30.6.1

x86_64

perl-PerlMagick-6.8.8.1-30.6.1
libMagick++-devel-32bit-6.8.8.1-30.6.1
libMagick++-devel-6.8.8.1-30.6.1
libMagickCore-6_Q16-1-6.8.8.1-30.6.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-30.6.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-30.6.1
libMagick++-6_Q16-3-6.8.8.1-30.6.1
libMagick++-6_Q16-3-32bit-6.8.8.1-30.6.1
ImageMagick-devel-6.8.8.1-30.6.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-30.6.1
libMagickWand-6_Q16-1-6.8.8.1-30.6.1
perl-PerlMagick-debuginfo-6.8.8.1-30.6.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-30.6.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-30.6.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-30.6.1
ImageMagick-extra-debuginfo-6.8.8.1-30.6.1
ImageMagick-devel-32bit-6.8.8.1-30.6.1
ImageMagick-6.8.8.1-30.6.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-30.6.1
ImageMagick-extra-6.8.8.1-30.6.1
ImageMagick-debugsource-6.8.8.1-30.6.1
ImageMagick-debuginfo-6.8.8.1-30.6.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-30.6.1

SuSE Linux 42.3

i586

perl-PerlMagick-debuginfo-6.8.8.1-34.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-34.1
libMagickCore-6_Q16-1-6.8.8.1-34.1

ImageMagick-debugsource-6.8.8.1-34.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-34.1
ImageMagick-extra-debuginfo-6.8.8.1-34.1
ImageMagick-6.8.8.1-34.1
libMagick++-devel-6.8.8.1-34.1
ImageMagick-devel-6.8.8.1-34.1
perl-PerlMagick-6.8.8.1-34.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-34.1
ImageMagick-extra-6.8.8.1-34.1
ImageMagick-debuginfo-6.8.8.1-34.1
libMagickWand-6_Q16-1-6.8.8.1-34.1
libMagick++-6_Q16-3-6.8.8.1-34.1

noarch
ImageMagick-doc-6.8.8.1-34.1

x86_64
libMagickWand-6_Q16-1-32bit-6.8.8.1-34.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-34.1
perl-PerlMagick-debuginfo-6.8.8.1-34.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-34.1
libMagickCore-6_Q16-1-6.8.8.1-34.1
ImageMagick-debugsource-6.8.8.1-34.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-34.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-34.1
ImageMagick-extra-debuginfo-6.8.8.1-34.1
ImageMagick-6.8.8.1-34.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-34.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-34.1
libMagick++-devel-32bit-6.8.8.1-34.1
libMagick++-devel-6.8.8.1-34.1
ImageMagick-devel-32bit-6.8.8.1-34.1
ImageMagick-devel-6.8.8.1-34.1
perl-PerlMagick-6.8.8.1-34.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-34.1
libMagick++-6_Q16-3-32bit-6.8.8.1-34.1
ImageMagick-extra-6.8.8.1-34.1
ImageMagick-debuginfo-6.8.8.1-34.1
libMagickWand-6_Q16-1-6.8.8.1-34.1
libMagick++-6_Q16-3-6.8.8.1-34.1

145530 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2149-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11464

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2149-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00042.html>

SuSE Linux 42.2

i586
gdk-pixbuf-loader-rsvg-2.40.18-9.3.1
rsvg-view-2.40.18-9.3.1
rsvg-view-debuginfo-2.40.18-9.3.1
librsvg-2-2-debuginfo-2.40.18-9.3.1
typelib-1_0-Rsvg-2_0-2.40.18-9.3.1
librsvg-debugsource-2.40.18-9.3.1
gdk-pixbuf-loader-rsvg-debuginfo-2.40.18-9.3.1
librsvg-2-2-2.40.18-9.3.1
librsvg-devel-2.40.18-9.3.1

noarch
rsvg-thumbnailer-2.40.18-9.3.1

x86_64
gdk-pixbuf-loader-rsvg-32bit-2.40.18-9.3.1
gdk-pixbuf-loader-rsvg-debuginfo-32bit-2.40.18-9.3.1
librsvg-devel-2.40.18-9.3.1
rsvg-view-debuginfo-2.40.18-9.3.1
librsvg-2-2-debuginfo-32bit-2.40.18-9.3.1
librsvg-2-2-debuginfo-2.40.18-9.3.1
rsvg-view-2.40.18-9.3.1
librsvg-2-2-2.40.18-9.3.1
typelib-1_0-Rsvg-2_0-2.40.18-9.3.1
librsvg-debugsource-2.40.18-9.3.1
gdk-pixbuf-loader-rsvg-2.40.18-9.3.1
gdk-pixbuf-loader-rsvg-debuginfo-2.40.18-9.3.1
librsvg-2-2-32bit-2.40.18-9.3.1

SuSE Linux 42.3

i586
rsvg-view-debuginfo-2.40.18-12.1
librsvg-devel-2.40.18-12.1
librsvg-2-2-debuginfo-2.40.18-12.1
librsvg-2-2-2.40.18-12.1
rsvg-view-2.40.18-12.1
typelib-1_0-Rsvg-2_0-2.40.18-12.1
gdk-pixbuf-loader-rsvg-debuginfo-2.40.18-12.1
librsvg-debugsource-2.40.18-12.1
gdk-pixbuf-loader-rsvg-2.40.18-12.1

noarch
rsvg-thumbnailer-2.40.18-12.1

x86_64
typelib-1_0-Rsvg-2_0-2.40.18-12.1
gdk-pixbuf-loader-rsvg-2.40.18-12.1
librsvg-debugsource-2.40.18-12.1
rsvg-view-debuginfo-2.40.18-12.1
librsvg-2-2-debuginfo-2.40.18-12.1
gdk-pixbuf-loader-rsvg-32bit-2.40.18-12.1
gdk-pixbuf-loader-rsvg-debuginfo-32bit-2.40.18-12.1
librsvg-2-2-2.40.18-12.1
librsvg-devel-2.40.18-12.1
rsvg-view-2.40.18-12.1
gdk-pixbuf-loader-rsvg-debuginfo-2.40.18-12.1
librsvg-2-2-32bit-2.40.18-12.1
librsvg-2-2-debuginfo-32bit-2.40.18-12.1

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

Risk Level: Medium

CVE: CVE-2017-5209, CVE-2017-5545

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0428-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00046.html>

SuSE Linux 42.1

x86_64

libplist-devel-1.12-4.1

python-plist-debuginfo-1.12-4.1

libplist++3-debuginfo-32bit-1.12-4.1

libplist3-1.12-4.1

libplist++3-debuginfo-1.12-4.1

plistutil-debuginfo-1.12-4.1

libplist3-32bit-1.12-4.1

python-plist-1.12-4.1

libplist-debugsource-1.12-4.1

libplist3-debuginfo-1.12-4.1

libplist++3-32bit-1.12-4.1

libplist3-debuginfo-32bit-1.12-4.1

libplist++3-1.12-4.1

plistutil-1.12-4.1

libplist++-devel-1.12-4.1

i586

libplist++3-1.12-4.1

libplist3-debuginfo-1.12-4.1

python-plist-debuginfo-1.12-4.1

libplist++-devel-1.12-4.1

plistutil-debuginfo-1.12-4.1

libplist-devel-1.12-4.1

plistutil-1.12-4.1

libplist3-1.12-4.1

python-plist-1.12-4.1

libplist-debugsource-1.12-4.1

libplist++3-debuginfo-1.12-4.1

SuSE Linux 42.2

x86_64

libplist++-devel-1.12-5.1

libplist3-32bit-1.12-5.1

plistutil-1.12-5.1

libplist3-1.12-5.1

python-plist-debuginfo-1.12-5.1

libplist-devel-1.12-5.1

libplist++3-debuginfo-32bit-1.12-5.1

libplist++3-debuginfo-1.12-5.1

python-plist-1.12-5.1

libplist-debugsource-1.12-5.1

libplist++3-1.12-5.1

plistutil-debuginfo-1.12-5.1
libplist++3-32bit-1.12-5.1
libplist3-debuginfo-1.12-5.1
libplist3-debuginfo-32bit-1.12-5.1

i586
libplist3-debuginfo-1.12-5.1
python-plist-debuginfo-1.12-5.1
libplist++3-1.12-5.1
libplist3-1.12-5.1
plistutil-1.12-5.1
python-plist-1.12-5.1
libplist-devel-1.12-5.1
libplist++3-debuginfo-1.12-5.1
libplist-debugsource-1.12-5.1
libplist+-devel-1.12-5.1
plistutil-debuginfo-1.12-5.1

145535 - SuSE Linux 42.2 openSUSE-SU-2017:1676-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7038, CVE-2013-7039

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1676-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00089.html>

SuSE Linux 42.2

x86_64

libmicrohttpd10-0.9.30-5.3.1
libmicrospdy-devel-0.9.30-5.3.1
libmicrohttpd-devel-0.9.30-5.3.1
microspdy2http-0.9.30-5.3.1
libmicrohttpd10-debuginfo-0.9.30-5.3.1
libmicrohttpd-debugsource-0.9.30-5.3.1
microspdy2http-debuginfo-0.9.30-5.3.1
libmicrospdy0-debuginfo-0.9.30-5.3.1
libmicrospdy0-0.9.30-5.3.1

i586

libmicrohttpd10-0.9.30-5.3.1
libmicrospdy-devel-0.9.30-5.3.1
libmicrohttpd-devel-0.9.30-5.3.1
microspdy2http-0.9.30-5.3.1
libmicrohttpd10-debuginfo-0.9.30-5.3.1
libmicrohttpd-debugsource-0.9.30-5.3.1
microspdy2http-debuginfo-0.9.30-5.3.1
libmicrospdy0-debuginfo-0.9.30-5.3.1
libmicrospdy0-0.9.30-5.3.1

145562 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1263-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8114

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1263-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00039.html>

SuSE Linux 42.1

noarch
roundcubemail-1.1.9-21.1

SuSE Linux 42.2

noarch
roundcubemail-1.1.9-17.6.1

145568 - SuSE Linux 42.1 openSUSE-SU-2017:0207-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7445, CVE-2016-8332, CVE-2016-9112, CVE-2016-9113, CVE-2016-9114, CVE-2016-9115, CVE-2016-9116, CVE-2016-9117, CVE-2016-9118, CVE-2016-9572, CVE-2016-9573, CVE-2016-9580, CVE-2016-9581

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0207-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00113.html>

SuSE Linux 42.1

x86_64
openjpeg2-devel-2.1.0-9.1
openjpeg2-2.1.0-9.1
openjpeg2-debuginfo-2.1.0-9.1
libopenjp2-7-32bit-2.1.0-9.1
libopenjp2-7-debuginfo-2.1.0-9.1
libopenjp2-7-2.1.0-9.1
openjpeg2-debugsource-2.1.0-9.1
libopenjp2-7-debuginfo-32bit-2.1.0-9.1

i586

openjpeg2-devel-2.1.0-9.1
openjpeg2-2.1.0-9.1
openjpeg2-debuginfo-2.1.0-9.1

libopenjp2-7-debuginfo-2.1.0-9.1
libopenjp2-7-2.1.0-9.1
openjpeg2-debugsource-2.1.0-9.1

145581 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0499-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5006, CVE-2017-5007, CVE-2017-5008, CVE-2017-5009, CVE-2017-5010, CVE-2017-5011, CVE-2017-5012, CVE-2017-5013, CVE-2017-5014, CVE-2017-5015, CVE-2017-5016, CVE-2017-5017, CVE-2017-5018, CVE-2017-5019, CVE-2017-5020, CVE-2017-5021, CVE-2017-5022, CVE-2017-5023, CVE-2017-5024, CVE-2017-5025, CVE-2017-5026

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0499-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00080.html>

SuSE Linux 42.1

x86_64

libavcodec57-debuginfo-32bit-3.2.2-2.1
chromium-56.0.2924.87-102.1
libavdevice57-32bit-3.2.2-2.1
libavcodec-devel-3.2.2-2.1
libavutil55-debuginfo-32bit-3.2.2-2.1
libswscale-devel-3.2.2-2.1
libswresample2-debuginfo-3.2.2-2.1
libswresample2-3.2.2-2.1
libavdevice57-debuginfo-3.2.2-2.1
libavfilter6-debuginfo-3.2.2-2.1
libswresample2-32bit-3.2.2-2.1
libswresample2-debuginfo-32bit-3.2.2-2.1
libavformat57-3.2.2-2.1
libpostproc-devel-3.2.2-2.1
chromium-debuginfo-56.0.2924.87-102.1
libavcodec57-3.2.2-2.1
libavutil-devel-3.2.2-2.1
libavformat57-32bit-3.2.2-2.1
libavresample-devel-3.2.2-2.1
chromedriver-debuginfo-56.0.2924.87-102.1
libavdevice57-debuginfo-32bit-3.2.2-2.1
libavresample3-debuginfo-32bit-3.2.2-2.1
libswscale4-debuginfo-32bit-3.2.2-2.1
libavfilter6-3.2.2-2.1
libavutil55-debuginfo-3.2.2-2.1
ffmpeg3-debugsource-3.2.2-2.1
libavdevice57-3.2.2-2.1
libpostproc54-debuginfo-32bit-3.2.2-2.1
libpostproc54-debuginfo-3.2.2-2.1
libpostproc54-32bit-3.2.2-2.1
libpostproc54-3.2.2-2.1
libavcodec57-32bit-3.2.2-2.1
chromium-debugsource-56.0.2924.87-102.1
chromedriver-56.0.2924.87-102.1

libavfilter-devel-3.2.2-2.1
libavformat57-debuginfo-32bit-3.2.2-2.1
libswresample-devel-3.2.2-2.1
libavresample3-debuginfo-3.2.2-2.1
libavfilter6-debuginfo-32bit-3.2.2-2.1
libavformat57-debuginfo-3.2.2-2.1
libavutil55-3.2.2-2.1
libavcodec57-debuginfo-3.2.2-2.1
libswscale4-3.2.2-2.1
libswscale4-debuginfo-3.2.2-2.1
ffmpeg3-3.2.2-2.1
libavformat-devel-3.2.2-2.1
libavfilter6-32bit-3.2.2-2.1
libavresample3-32bit-3.2.2-2.1
ffmpeg3-debuginfo-3.2.2-2.1
libavdevice-devel-3.2.2-2.1
libavresample3-3.2.2-2.1
libswscale4-32bit-3.2.2-2.1
libavutil55-32bit-3.2.2-2.1

i586

libavcodec-devel-3.2.2-2.1
libswscale-devel-3.2.2-2.1
libswresample2-debuginfo-3.2.2-2.1
libswresample2-3.2.2-2.1
libavdevice57-debuginfo-3.2.2-2.1
libavfilter6-debuginfo-3.2.2-2.1
libavformat57-3.2.2-2.1
libpostproc-devel-3.2.2-2.1
libavcodec57-3.2.2-2.1
libavutil-devel-3.2.2-2.1
libavresample-devel-3.2.2-2.1
libavfilter6-3.2.2-2.1
libavutil55-debuginfo-3.2.2-2.1
ffmpeg3-debugsource-3.2.2-2.1
libavdevice57-3.2.2-2.1
libpostproc54-debuginfo-3.2.2-2.1
libpostproc54-3.2.2-2.1
libavfilter-devel-3.2.2-2.1
libswresample-devel-3.2.2-2.1
libavresample3-debuginfo-3.2.2-2.1
libavformat57-debuginfo-3.2.2-2.1
libavutil55-3.2.2-2.1
libavcodec57-debuginfo-3.2.2-2.1
libswscale4-3.2.2-2.1
libswscale4-debuginfo-3.2.2-2.1
ffmpeg3-3.2.2-2.1
libavformat-devel-3.2.2-2.1
ffmpeg3-debuginfo-3.2.2-2.1
libavdevice-devel-3.2.2-2.1
libavresample3-3.2.2-2.1

SuSE Linux 42.2

x86_64

harfbuzz-tools-debuginfo-1.4.2-3.1
libharfbuzz-icu0-1.4.2-3.1
chromium-56.0.2924.87-102.1
libharfbuzz0-32bit-1.4.2-3.1
harfbuzz-tools-1.4.2-3.1
harfbuzz-debugsource-1.4.2-3.1

libharfbuzz0-debuginfo-32bit-1.4.2-3.1
chromedriver-56.0.2924.87-102.1
chromedriver-debuginfo-56.0.2924.87-102.1
libharfbuzz-icu0-debuginfo-1.4.2-3.1
harfbuzz-devel-1.4.2-3.1
libharfbuzz0-1.4.2-3.1
chromium-debugsource-56.0.2924.87-102.1
libharfbuzz0-debuginfo-1.4.2-3.1
libharfbuzz-icu0-debuginfo-32bit-1.4.2-3.1
chromium-debuginfo-56.0.2924.87-102.1
libharfbuzz-icu0-32bit-1.4.2-3.1

i586

harfbuzz-devel-1.4.2-3.1
libharfbuzz-icu0-debuginfo-1.4.2-3.1
libharfbuzz0-debuginfo-1.4.2-3.1
libharfbuzz-icu0-1.4.2-3.1
harfbuzz-debugsource-1.4.2-3.1
harfbuzz-tools-debuginfo-1.4.2-3.1
harfbuzz-tools-1.4.2-3.1
libharfbuzz0-1.4.2-3.1

145591 - SuSE Linux 42.3 openSUSE-SU-2017:2311-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11103

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2311-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00112.html>

SuSE Linux 42.3

i586

samba-libs-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libwbclient-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsmbclient0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
samba-client-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libndr-standard0-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-passdb-devel-4.6.7+git.38.90b2cdb4f22-3.1
ctdb-tests-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libndr-krb5pac0-4.6.7+git.38.90b2cdb4f22-3.1
samba-test-4.6.7+git.38.90b2cdb4f22-3.1
libsmbldap-devel-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-devel-4.6.7+git.38.90b2cdb4f22-3.1
libndr-standard-devel-4.6.7+git.38.90b2cdb4f22-3.1
samba-python-4.6.7+git.38.90b2cdb4f22-3.1
libndr-krb5pac-devel-4.6.7+git.38.90b2cdb4f22-3.1
samba-pidl-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-samr0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-hostconfig-devel-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-binding0-4.6.7+git.38.90b2cdb4f22-3.1

libsamba-policy-devel-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-samr-devel-4.6.7+git.38.90b2cdb4f22-3.1
samba-4.6.7+git.38.90b2cdb4f22-3.1
libsamdb0-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-passdb0-4.6.7+git.38.90b2cdb4f22-3.1
libnetapi-devel-4.6.7+git.38.90b2cdb4f22-3.1
libtevent-util0-4.6.7+git.38.90b2cdb4f22-3.1
ctdb-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-binding0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libwbclient0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsmbconf0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
ctdb-4.6.7+git.38.90b2cdb4f22-3.1
ldirectord-4.0.1+git.1495055229.643177f1-3.1
libndr-nbt-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-hostconfig0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-util-devel-4.6.7+git.38.90b2cdb4f22-3.1
libwbclient0-4.6.7+git.38.90b2cdb4f22-3.1
libtevent-util0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
samba-core-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsmbclient-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsamdb0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
samba-test-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
resource-agents-debuginfo-4.0.1+git.1495055229.643177f1-3.1
samba-python-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
resource-agents-4.0.1+git.1495055229.643177f1-3.1
libsamba-policy0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsamdb-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-credentials0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libndr-standard0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-util0-4.6.7+git.38.90b2cdb4f22-3.1
samba-debugsource-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-credentials-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-util0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsmbconf0-4.6.7+git.38.90b2cdb4f22-3.1
libnetapi0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-policy0-4.6.7+git.38.90b2cdb4f22-3.1
samba-winbind-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc0-4.6.7+git.38.90b2cdb4f22-3.1
libndr-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-hostconfig0-4.6.7+git.38.90b2cdb4f22-3.1
samba-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
ctdb-tests-4.6.7+git.38.90b2cdb4f22-3.1
libndr-nbt0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libndr0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
samba-libs-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-errors0-4.6.7+git.38.90b2cdb4f22-3.1
libsmbconf-devel-4.6.7+git.38.90b2cdb4f22-3.1
resource-agents-debugsource-4.0.1+git.1495055229.643177f1-3.1
libndr-krb5pac0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsmbldap0-4.6.7+git.38.90b2cdb4f22-3.1
libsmbldap0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-passdb0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-samr0-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-errors-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsmbclient0-4.6.7+git.38.90b2cdb4f22-3.1
samba-client-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-errors0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libndr-nbt0-4.6.7+git.38.90b2cdb4f22-3.1
libndr0-4.6.7+git.38.90b2cdb4f22-3.1
libtevent-util-devel-4.6.7+git.38.90b2cdb4f22-3.1

libdcerpc0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
samba-winbind-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libnetapi0-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-credentials0-4.6.7+git.38.90b2cdb4f22-3.1

noarch

samba-doc-4.6.7+git.38.90b2cdb4f22-3.1
monitoring-plugins-metadata-4.0.1+git.1495055229.643177f1-3.1

x86_64

samba-libs-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-errors0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libwbclient-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsmbclient0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
samba-client-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libndr-standard0-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-passsdb-devel-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-samr0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
ctdb-tests-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-credentials0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libndr-krb5pac0-4.6.7+git.38.90b2cdb4f22-3.1
libsamdb0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libsmbldap0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
samba-test-4.6.7+git.38.90b2cdb4f22-3.1
libsmbldap-devel-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-devel-4.6.7+git.38.90b2cdb4f22-3.1
libndr0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libndr-standard-devel-4.6.7+git.38.90b2cdb4f22-3.1
samba-python-4.6.7+git.38.90b2cdb4f22-3.1
libsamdb0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libndr-standard0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-util0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libndr-krb5pac-devel-4.6.7+git.38.90b2cdb4f22-3.1
samba-pidl-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-samr0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
samba-ceph-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-hostconfig0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-binding0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libsmbclient0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-hostconfig-devel-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-binding0-4.6.7+git.38.90b2cdb4f22-3.1
samba-winbind-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-policy-devel-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-samr-devel-4.6.7+git.38.90b2cdb4f22-3.1
libsmbconf0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
samba-4.6.7+git.38.90b2cdb4f22-3.1
samba-libs-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libsamdb0-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-passsdb0-4.6.7+git.38.90b2cdb4f22-3.1
libwbclient0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libtevent-util0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libnetapi-devel-4.6.7+git.38.90b2cdb4f22-3.1
libtevent-util0-4.6.7+git.38.90b2cdb4f22-3.1
libndr-krb5pac0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libsmbconf0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libwbclient0-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libsamba-hostconfig0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
ctdb-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libdcerpc-binding0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1

libwbclient0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
libsmbconf0-debuginfo-4.6.7+git.38.90b2cdb4f22-3.1
ctdb-4.6.7+git.38.90b2cdb4f22-3.1
ldirectord-4.0.1+git.1495055229.643177f1-3.1
libsamba-policy0-debuginfo-32bit-4.6.7+git.38.90b2cdb4f22-3.1
libndr-nbt-devel-4.6.7+git.38.90b2cdb4f22-3.1

145599 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0015-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7098

Description

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

openSUSE-SU-2017:0015-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00007.html>

SuSE Linux 42.1

x86_64

wget-debugsource-1.14-8.1

wget-1.14-8.1

wget-debuginfo-1.14-8.1

i586

wget-debugsource-1.14-8.1

wget-1.14-8.1

wget-debuginfo-1.14-8.1

SuSE Linux 42.2

x86_64

wget-1.14-6.1

wget-debuginfo-1.14-6.1

wget-debugsource-1.14-6.1

i586

wget-1.14-6.1

wget-debuginfo-1.14-6.1

wget-debugsource-1.14-6.1

145603 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1292-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8745, CVE-2017-5647, CVE-2017-5648

Description

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

openSUSE-SU-2017:1292-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00057.html>

SuSE Linux 42.1

noarch
tomcat-lib-8.0.43-17.1
tomcat-embed-8.0.43-17.1
tomcat-admin-webapps-8.0.43-17.1
tomcat-jsp-2_3-api-8.0.43-17.1
tomcat-el-3_0-api-8.0.43-17.1
tomcat-javadoc-8.0.43-17.1
tomcat-jsvc-8.0.43-17.1
tomcat-webapps-8.0.43-17.1
tomcat-docs-webapp-8.0.43-17.1
tomcat-servlet-3_1-api-8.0.43-17.1
tomcat-8.0.43-17.1

SuSE Linux 42.2

noarch
tomcat-javadoc-8.0.43-6.7.1
tomcat-jsvc-8.0.43-6.7.1
tomcat-lib-8.0.43-6.7.1
tomcat-servlet-3_1-api-8.0.43-6.7.1
tomcat-docs-webapp-8.0.43-6.7.1
tomcat-admin-webapps-8.0.43-6.7.1
tomcat-webapps-8.0.43-6.7.1
tomcat-8.0.43-6.7.1
tomcat-el-3_0-api-8.0.43-6.7.1
tomcat-jsp-2_3-api-8.0.43-6.7.1
tomcat-embed-8.0.43-6.7.1

145609 - SuSE Linux 42.2 openSUSE-SU-2017:1746-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0663, CVE-2017-5969

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1746-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00000.html>

SuSE Linux 42.2

i586
python-libxml2-debugsource-2.9.4-5.9.1
libxml2-2-2.9.4-5.9.1
libxml2-tools-debuginfo-2.9.4-5.9.1
libxml2-devel-2.9.4-5.9.1
libxml2-debugsource-2.9.4-5.9.1
libxml2-tools-2.9.4-5.9.1
python-libxml2-debuginfo-2.9.4-5.9.1

python-libxml2-2.9.4-5.9.1
libxml2-2-debuginfo-2.9.4-5.9.1

noarch
libxml2-doc-2.9.4-5.9.1

x86_64
python-libxml2-debugsource-2.9.4-5.9.1
libxml2-2-2.9.4-5.9.1
libxml2-tools-debuginfo-2.9.4-5.9.1
libxml2-2-32bit-2.9.4-5.9.1
libxml2-devel-2.9.4-5.9.1
libxml2-debugsource-2.9.4-5.9.1
libxml2-tools-2.9.4-5.9.1
libxml2-2-debuginfo-32bit-2.9.4-5.9.1
python-libxml2-debuginfo-2.9.4-5.9.1
python-libxml2-2.9.4-5.9.1
libxml2-2-debuginfo-2.9.4-5.9.1
libxml2-devel-32bit-2.9.4-5.9.1

145611 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1034-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10251, CVE-2016-9583, CVE-2016-9600, CVE-2017-5498, CVE-2017-6850

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1034-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00061.html>

SuSE Linux 42.1

x86_64
jasper-1.900.14-176.1
jasper-debuginfo-1.900.14-176.1
libjasper-devel-1.900.14-176.1
libjasper1-1.900.14-176.1
jasper-debugsource-1.900.14-176.1
libjasper1-debuginfo-32bit-1.900.14-176.1
libjasper1-32bit-1.900.14-176.1
libjasper1-debuginfo-1.900.14-176.1

i586

jasper-1.900.14-176.1
jasper-debuginfo-1.900.14-176.1
libjasper-devel-1.900.14-176.1
libjasper1-1.900.14-176.1
jasper-debugsource-1.900.14-176.1
libjasper1-debuginfo-1.900.14-176.1

SuSE Linux 42.2

x86_64
libjasper1-1.900.14-175.3.1

libjasper-devel-1.900.14-175.3.1
libjasper1-debuginfo-32bit-1.900.14-175.3.1
jasper-debuginfo-1.900.14-175.3.1
libjasper1-debuginfo-1.900.14-175.3.1
libjasper1-32bit-1.900.14-175.3.1
jasper-debugsource-1.900.14-175.3.1
jasper-1.900.14-175.3.1

i586

libjasper1-1.900.14-175.3.1
libjasper-devel-1.900.14-175.3.1
jasper-debuginfo-1.900.14-175.3.1
libjasper1-debuginfo-1.900.14-175.3.1
jasper-debugsource-1.900.14-175.3.1
jasper-1.900.14-175.3.1

145614 - SuSE Linux 42.2 openSUSE-SU-2017:0382-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5545, CVE-2017-3290, CVE-2017-3316, CVE-2017-3332

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0382-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00019.html>

SuSE Linux 42.2

x86_64
virtualbox-guest-kmp-default-5.1.14_k4.4.36_8-9.2
virtualbox-websrv-5.1.14-9.2
python-virtualbox-debuginfo-5.1.14-9.2
virtualbox-guest-x11-debuginfo-5.1.14-9.2
virtualbox-host-kmp-default-debuginfo-5.1.14_k4.4.36_8-9.2
virtualbox-guest-x11-5.1.14-9.2
virtualbox-guest-kmp-default-debuginfo-5.1.14_k4.4.36_8-9.2
virtualbox-debugsource-5.1.14-9.2
virtualbox-websrv-debuginfo-5.1.14-9.2
virtualbox-debuginfo-5.1.14-9.2
virtualbox-guest-tools-5.1.14-9.2
virtualbox-qt-debuginfo-5.1.14-9.2
python-virtualbox-5.1.14-9.2
virtualbox-qt-5.1.14-9.2
virtualbox-devel-5.1.14-9.2
virtualbox-guest-tools-debuginfo-5.1.14-9.2
virtualbox-5.1.14-9.2
virtualbox-host-kmp-default-5.1.14_k4.4.36_8-9.2

noarch

virtualbox-guest-desktop-icons-5.1.14-9.2
virtualbox-host-source-5.1.14-9.2

145616 - SuSE Linux 42.2 openSUSE-SU-2017:1455-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000367

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1455-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00106.html>

SuSE Linux 42.2

x86_64

sudo-1.8.10p3-9.3.1

sudo-debuginfo-1.8.10p3-9.3.1

sudo-test-1.8.10p3-9.3.1

sudo-devel-1.8.10p3-9.3.1

sudo-debugsource-1.8.10p3-9.3.1

i586

sudo-1.8.10p3-9.3.1

sudo-debuginfo-1.8.10p3-9.3.1

sudo-test-1.8.10p3-9.3.1

sudo-devel-1.8.10p3-9.3.1

sudo-debugsource-1.8.10p3-9.3.1

145617 - SuSE Linux 42.2 openSUSE-SU-2017:0167-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5331, CVE-2017-5332, CVE-2017-5333

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0167-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00097.html>

SuSE Linux 42.2

x86_64

icoutils-0.31.1-8.1

icoutils-debugsource-0.31.1-8.1

icoutils-debuginfo-0.31.1-8.1

i586

icoutils-0.31.1-8.1

icoutils-debugsource-0.31.1-8.1

145618 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1230-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8400, CVE-2017-8401

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1230-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00034.html>

SuSE Linux 42.1

x86_64

swftools-debuginfo-0.9.2-8.1

swftools-0.9.2-8.1

swftools-debugsource-0.9.2-8.1

i586

swftools-debuginfo-0.9.2-8.1

swftools-0.9.2-8.1

swftools-debugsource-0.9.2-8.1

SuSE Linux 42.2

x86_64

swftools-0.9.2-8.3.1

swftools-debugsource-0.9.2-8.3.1

swftools-debuginfo-0.9.2-8.3.1

i586

swftools-0.9.2-8.3.1

swftools-debugsource-0.9.2-8.3.1

swftools-debuginfo-0.9.2-8.3.1

145625 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1038-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6827, CVE-2017-6828, CVE-2017-6829, CVE-2017-6830, CVE-2017-6831, CVE-2017-6832, CVE-2017-6833, CVE-2017-6834, CVE-2017-6835, CVE-2017-6836, CVE-2017-6837, CVE-2017-6838, CVE-2017-6839

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1038-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00064.html>

SuSE Linux 42.1
x86_64
audiofile-0.3.6-12.1
libaudiofile1-debuginfo-32bit-0.3.6-12.1
audiofile-devel-0.3.6-12.1
libaudiofile1-32bit-0.3.6-12.1
audiofile-devel-32bit-0.3.6-12.1
libaudiofile1-debuginfo-0.3.6-12.1
audiofile-debuginfo-0.3.6-12.1
libaudiofile1-0.3.6-12.1
audiofile-debugsource-0.3.6-12.1
audiofile-doc-0.3.6-12.1

i586
audiofile-0.3.6-12.1
audiofile-devel-0.3.6-12.1
libaudiofile1-debuginfo-0.3.6-12.1
audiofile-debuginfo-0.3.6-12.1
libaudiofile1-0.3.6-12.1
audiofile-debugsource-0.3.6-12.1
audiofile-doc-0.3.6-12.1

SuSE Linux 42.2
x86_64
audiofile-debugsource-0.3.6-10.3.1
audiofile-0.3.6-10.3.1
audiofile-doc-0.3.6-10.3.1
libaudiofile1-32bit-0.3.6-10.3.1
audiofile-devel-32bit-0.3.6-10.3.1
audiofile-debuginfo-0.3.6-10.3.1
libaudiofile1-debuginfo-32bit-0.3.6-10.3.1
libaudiofile1-debuginfo-0.3.6-10.3.1
libaudiofile1-0.3.6-10.3.1
audiofile-devel-0.3.6-10.3.1

i586
audiofile-debugsource-0.3.6-10.3.1
audiofile-0.3.6-10.3.1
audiofile-doc-0.3.6-10.3.1
audiofile-debuginfo-0.3.6-10.3.1
libaudiofile1-debuginfo-0.3.6-10.3.1
libaudiofile1-0.3.6-10.3.1
audiofile-devel-0.3.6-10.3.1

145627 - SuSE Linux 42.1 openSUSE-SU-2017:0166-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5331, CVE-2017-5332, CVE-2017-5333

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0166-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00096.html>

SuSE Linux 42.1

x86_64

icoutils-debugsource-0.31.1-7.1

icoutils-debuginfo-0.31.1-7.1

icoutils-0.31.1-7.1

i586

icoutils-debugsource-0.31.1-7.1

icoutils-debuginfo-0.31.1-7.1

icoutils-0.31.1-7.1

145632 - SuSE Linux 42.2 openSUSE-SU-2017:1510-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1839, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050

Description

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

openSUSE-SU-2017:1510-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00022.html>

SuSE Linux 42.2

i586

python-libxml2-debugsource-2.9.4-5.3.1

libxml2-devel-2.9.4-5.3.1

python-libxml2-debuginfo-2.9.4-5.3.1

libxml2-tools-debuginfo-2.9.4-5.3.1

python-libxml2-2.9.4-5.3.1

libxml2-2-2.9.4-5.3.1

libxml2-debugsource-2.9.4-5.3.1

libxml2-tools-2.9.4-5.3.1

libxml2-2-debuginfo-2.9.4-5.3.1

noarch

libxml2-doc-2.9.4-5.3.1

x86_64

libxml2-2-32bit-2.9.4-5.3.1

python-libxml2-debugsource-2.9.4-5.3.1

libxml2-2-debuginfo-32bit-2.9.4-5.3.1

libxml2-devel-2.9.4-5.3.1

python-libxml2-debuginfo-2.9.4-5.3.1

libxml2-tools-debuginfo-2.9.4-5.3.1

python-libxml2-2.9.4-5.3.1

libxml2-2-2.9.4-5.3.1

libxml2-debugsource-2.9.4-5.3.1

libxml2-tools-2.9.4-5.3.1

libxml2-devel-32bit-2.9.4-5.3.1

libxml2-2-debuginfo-2.9.4-5.3.1

145637 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0252-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1246, CVE-2016-1249, CVE-2016-1251

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0252-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00127.html>

SuSE Linux 42.1

x86_64

perl-DBD-mysql-debugsource-4.021-13.1

perl-DBD-mysql-debuginfo-4.021-13.1

perl-DBD-mysql-4.021-13.1

i586

perl-DBD-mysql-debugsource-4.021-13.1

perl-DBD-mysql-debuginfo-4.021-13.1

perl-DBD-mysql-4.021-13.1

SuSE Linux 42.2

x86_64

perl-DBD-mysql-debugsource-4.021-14.1

perl-DBD-mysql-debuginfo-4.021-14.1

perl-DBD-mysql-4.021-14.1

145643 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0850-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8994

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0850-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00107.html>

SuSE Linux 42.1

i586

php5-xmlreader-debuginfo-5.5.14-78.1

php5-soap-debuginfo-5.5.14-78.1

php5-mssql-5.5.14-78.1

php5-mcrypt-debuginfo-5.5.14-78.1

php5-xmlreader-5.5.14-78.1

php5-json-5.5.14-78.1
apache2-mod_php5-5.5.14-78.1
php5-intl-5.5.14-78.1
php5-xmlrpc-debuginfo-5.5.14-78.1
php5-mssql-debuginfo-5.5.14-78.1
php5-dom-5.5.14-78.1
php5-zip-debuginfo-5.5.14-78.1
php5-odbc-5.5.14-78.1
php5-xsl-debuginfo-5.5.14-78.1
php5-gd-debuginfo-5.5.14-78.1
php5-pspell-debuginfo-5.5.14-78.1
php5-debuginfo-5.5.14-78.1
php5-pgsql-debuginfo-5.5.14-78.1
php5-sysvshm-debuginfo-5.5.14-78.1
php5-openssl-debuginfo-5.5.14-78.1
php5-mbstring-debuginfo-5.5.14-78.1
php5-fpm-5.5.14-78.1
php5-suhosin-debuginfo-5.5.14-78.1
php5-gettext-debuginfo-5.5.14-78.1
php5-opcache-5.5.14-78.1
php5-xmlwriter-5.5.14-78.1
php5-ctype-5.5.14-78.1
php5-devel-5.5.14-78.1
php5-sysvmsg-5.5.14-78.1
php5-bcmath-debuginfo-5.5.14-78.1
php5-dba-5.5.14-78.1
php5-tokenizer-5.5.14-78.1
php5-bz2-debuginfo-5.5.14-78.1
php5-mysql-debuginfo-5.5.14-78.1
php5-readline-5.5.14-78.1
php5-calendar-5.5.14-78.1
php5-phar-5.5.14-78.1
php5-gmp-debuginfo-5.5.14-78.1
php5-enchanted-debuginfo-5.5.14-78.1
php5-imap-debuginfo-5.5.14-78.1
php5-imap-5.5.14-78.1
php5-enchanted-5.5.14-78.1
php5-posix-debuginfo-5.5.14-78.1
php5-fileinfo-5.5.14-78.1
php5-mbstring-5.5.14-78.1
php5-pcntl-debuginfo-5.5.14-78.1
php5-snmp-debuginfo-5.5.14-78.1
php5-zlib-debuginfo-5.5.14-78.1
php5-ftp-debuginfo-5.5.14-78.1
php5-pdo-5.5.14-78.1
php5-calendar-debuginfo-5.5.14-78.1
php5-firebird-5.5.14-78.1
php5-opcache-debuginfo-5.5.14-78.1
php5-pdo-debuginfo-5.5.14-78.1
php5-tokenizer-debuginfo-5.5.14-78.1
php5-iconv-5.5.14-78.1
php5-snmp-5.5.14-78.1
php5-5.5.14-78.1
php5-zlib-5.5.14-78.1
php5-wddx-5.5.14-78.1
php5-zip-5.5.14-78.1
php5-debugsource-5.5.14-78.1
php5-xsl-5.5.14-78.1
php5-firebird-debuginfo-5.5.14-78.1
php5-sockets-debuginfo-5.5.14-78.1

php5-curl-debuginfo-5.5.14-78.1
php5-exif-5.5.14-78.1
php5-wddx-debuginfo-5.5.14-78.1
php5-ctype-debuginfo-5.5.14-78.1
apache2-mod_php5-debuginfo-5.5.14-78.1
php5-gd-5.5.14-78.1
php5-sysvmsg-debuginfo-5.5.14-78.1
php5-pcntl-5.5.14-78.1
php5-sysvsem-5.5.14-78.1
php5-sysvshm-5.5.14-78.1
php5-dba-debuginfo-5.5.14-78.1
php5-sqlite-debuginfo-5.5.14-78.1
php5-bcmath-5.5.14-78.1
php5-sysvsem-debuginfo-5.5.14-78.1
php5-dom-debuginfo-5.5.14-78.1
php5-ispell-5.5.14-78.1
php5-posix-5.5.14-78.1
php5-fpm-debuginfo-5.5.14-78.1
php5-soap-5.5.14-78.1
php5-mysql-5.5.14-78.1
php5-shmop-debuginfo-5.5.14-78.1
php5-sockets-5.5.14-78.1
php5-fileinfo-debuginfo-5.5.14-78.1
php5-ldap-5.5.14-78.1
php5-mcrypt-5.5.14-78.1
php5-fastcgi-debuginfo-5.5.14-78.1
php5-shmop-5.5.14-78.1
php5-suhosin-5.5.14-78.1
php5-ftp-5.5.14-78.1
php5-json-debuginfo-5.5.14-78.1
php5-ldap-debuginfo-5.5.14-78.1
php5-intl-debuginfo-5.5.14-78.1
php5-phar-debuginfo-5.5.14-78.1
php5-readline-debuginfo-5.5.14-78.1
php5-fastcgi-5.5.14-78.1
php5-curl-5.5.14-78.1
php5-bz2-5.5.14-78.1
php5-gmp-5.5.14-78.1
php5-iconv-debuginfo-5.5.14-78.1
php5-pgsql-5.5.14-78.1
php5-gettext-5.5.14-78.1
php5-exif-debuginfo-5.5.14-78.1
php5-tidy-debuginfo-5.5.14-78.1
php5-xmlrpc-5.5.14-78.1
php5-openssl-5.5.14-78.1
php5-sqlite-5.5.14-78.1
php5-odbc-debuginfo-5.5.14-78.1
php5-tidy-5.5.14-78.1
php5-xmlwriter-debuginfo-5.5.14-78.1

noarch

php5-pear-5.5.14-78.1

x86_64

php5-xmlreader-debuginfo-5.5.14-78.1
php5-soap-debuginfo-5.5.14-78.1
php5-mssql-5.5.14-78.1
php5-mcrypt-debuginfo-5.5.14-78.1
php5-xmlreader-5.5.14-78.1
php5-json-5.5.14-78.1

apache2-mod_php5-5.5.14-78.1
php5-intl-5.5.14-78.1
php5-xmlrpc-debuginfo-5.5.14-78.1
php5-mssql-debuginfo-5.5.14-78.1
php5-dom-5.5.14-78.1
php5-zip-debuginfo-5.5.14-78.1
php5-odbc-5.5.14-78.1
php5-xsl-debuginfo-5.5.14-78.1
php5-gd-debuginfo-5.5.14-78.1
php5-pspell-debuginfo-5.5.14-78.1
php5-debuginfo-5.5.14-78.1
php5-pgsql-debuginfo-5.5.14-78.1
php5-sysvshm-debuginfo-5.5.14-78.1
php5-openssl-debuginfo-5.5.14-78.1
php5-mbstring-debuginfo-5.5.14-78.1
php5-fpm-5.5.14-78.1
php5-suhosin-debuginfo-5.5.14-78.1
php5-gettext-debuginfo-5.5.14-78.1
php5-opcache-5.5.14-78.1
php5-xmlwriter-5.5.14-78.1
php5-ctype-5.5.14-78.1
php5-devel-5.5.14-78.1
php5-sysvmsg-5.5.14-78.1
php5-bcmath-debuginfo-5.5.14-78.1
php5-dba-5.5.14-78.1
php5-tokenizer-5.5.14-78.1
php5-bz2-debuginfo-5.5.14-78.1
php5-mysql-debuginfo-5.5.14-78.1
php5-readline-5.5.14-78.1
php5-calendar-5.5.14-78.1
php5-phar-5.5.14-78.1
php5-gmp-debuginfo-5.5.14-78.1
php5-enchanted-debuginfo-5.5.14-78.1
php5-imap-debuginfo-5.5.14-78.1
php5-imap-5.5.14-78.1
php5-enchanted-5.5.14-78.1
php5-posix-debuginfo-5.5.14-78.1
php5-fileinfo-5.5.14-78.1
php5-mbstring-5.5.14-78.1
php5-pcntl-debuginfo-5.5.14-78.1
php5-snmp-debuginfo-5.5.14-78.1
php5-zlib-debuginfo-5.5.14-78.1
php5-ftp-debuginfo-5.5.14-78.1
php5-pdo-5.5.14-78.1
php5-calendar-debuginfo-5.5.14-78.1
php5-firebird-5.5.14-78.1
php5-opcache-debuginfo-5.5.14-78.1
php5-pdo-debuginfo-5.5.14-78.1
php5-tokenizer-debuginfo-5.5.14-78.1
php5-iconv-5.5.14-78.1
php5-snmp-5.5.14-78.1
php5-5.5.14-78.1
php5-zlib-5.5.14-78.1
php5-wddx-5.5.14-78.1
php5-zip-5.5.14-78.1
php5-debugsource-5.5.14-78.1
php5-xsl-5.5.14-78.1
php5-firebird-debuginfo-5.5.14-78.1
php5-sockets-debuginfo-5.5.14-78.1
php5-curl-debuginfo-5.5.14-78.1

php5-exif-5.5.14-78.1
php5-wddx-debuginfo-5.5.14-78.1
php5-ctype-debuginfo-5.5.14-78.1
apache2-mod_php5-debuginfo-5.5.14-78.1
php5-gd-5.5.14-78.1
php5-sysvmsg-debuginfo-5.5.14-78.1
php5-pcntl-5.5.14-78.1
php5-sysvsem-5.5.14-78.1
php5-sysvshm-5.5.14-78.1
php5-dba-debuginfo-5.5.14-78.1
php5-sqlite-debuginfo-5.5.14-78.1
php5-bcmath-5.5.14-78.1
php5-sysvsem-debuginfo-5.5.14-78.1
php5-dom-debuginfo-5.5.14-78.1
php5-ispell-5.5.14-78.1
php5-posix-5.5.14-78.1
php5-fpm-debuginfo-5.5.14-78.1
php5-soap-5.5.14-78.1
php5-mysql-5.5.14-78.1
php5-shmop-debuginfo-5.5.14-78.1
php5-sockets-5.5.14-78.1
php5-fileinfo-debuginfo-5.5.14-78.1
php5-ldap-5.5.14-78.1
php5-mcrypt-5.5.14-78.1
php5-fastcgi-debuginfo-5.5.14-78.1
php5-shmop-5.5.14-78.1
php5-suhosin-5.5.14-78.1
php5-ftp-5.5.14-78.1
php5-json-debuginfo-5.5.14-78.1
php5-ldap-debuginfo-5.5.14-78.1
php5-intl-debuginfo-5.5.14-78.1
php5-phar-debuginfo-5.5.14-78.1
php5-readline-debuginfo-5.5.14-78.1
php5-fastcgi-5.5.14-78.1
php5-curl-5.5.14-78.1
php5-bz2-5.5.14-78.1
php5-gmp-5.5.14-78.1
php5-iconv-debuginfo-5.5.14-78.1
php5-pgsql-5.5.14-78.1
php5-gettext-5.5.14-78.1
php5-exif-debuginfo-5.5.14-78.1
php5-tidy-debuginfo-5.5.14-78.1
php5-xmlrpc-5.5.14-78.1
php5-openssl-5.5.14-78.1
php5-sqlite-5.5.14-78.1
php5-odbc-debuginfo-5.5.14-78.1
php5-tidy-5.5.14-78.1
php5-xmlwriter-debuginfo-5.5.14-78.1

SuSE Linux 42.2

i586

php5-posix-debuginfo-5.5.14-77.3.1
php5-tokenizer-5.5.14-77.3.1
php5-suhosin-5.5.14-77.3.1
php5-iconv-5.5.14-77.3.1
php5-fastcgi-5.5.14-77.3.1
php5-ldap-debuginfo-5.5.14-77.3.1
php5-xmlwriter-debuginfo-5.5.14-77.3.1
php5-fpm-5.5.14-77.3.1

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

Risk Level: Medium

CVE: CVE-2017-2295

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1948-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00086.html>

SuSE Linux 42.2

i586

ruby2.1-rubygem-puppet-testsuite-3.8.7-17.3.1
rubygem-puppet-3.8.7-17.3.1
ruby2.1-rubygem-puppet-doc-3.8.7-17.3.1
ruby2.1-rubygem-puppet-3.8.7-17.3.1
rubygem-puppet-master-3.8.7-17.3.1

noarch

rubygem-puppet-emacs-3.8.7-17.3.1
rubygem-puppet-master-unicorn-3.8.7-17.3.1
rubygem-puppet-vim-3.8.7-17.3.1

x86_64

ruby2.1-rubygem-puppet-testsuite-3.8.7-17.3.1
rubygem-puppet-3.8.7-17.3.1
ruby2.1-rubygem-puppet-doc-3.8.7-17.3.1
ruby2.1-rubygem-puppet-3.8.7-17.3.1
rubygem-puppet-master-3.8.7-17.3.1

SuSE Linux 42.3

i586

rubygem-puppet-master-3.8.7-20.1
ruby2.3-rubygem-puppet-3.8.7-20.1
ruby2.4-rubygem-puppet-3.8.7-20.1
ruby2.4-rubygem-puppet-testsuite-3.8.7-20.1
ruby2.3-rubygem-puppet-testsuite-3.8.7-20.1
ruby2.2-rubygem-puppet-testsuite-3.8.7-20.1
ruby2.1-rubygem-puppet-3.8.7-20.1
ruby2.1-rubygem-puppet-doc-3.8.7-20.1
ruby2.1-rubygem-puppet-testsuite-3.8.7-20.1
ruby2.3-rubygem-puppet-doc-3.8.7-20.1
ruby2.2-rubygem-puppet-3.8.7-20.1
ruby2.2-rubygem-puppet-doc-3.8.7-20.1
rubygem-puppet-3.8.7-20.1
ruby2.4-rubygem-puppet-doc-3.8.7-20.1

noarch

rubygem-puppet-emacs-3.8.7-20.1
rubygem-puppet-master-unicorn-3.8.7-20.1
rubygem-puppet-vim-3.8.7-20.1

x86_64

rubygem-puppet-master-3.8.7-20.1
ruby2.3-rubygem-puppet-3.8.7-20.1
ruby2.4-rubygem-puppet-3.8.7-20.1
ruby2.4-rubygem-puppet-testsuite-3.8.7-20.1
ruby2.3-rubygem-puppet-testsuite-3.8.7-20.1
ruby2.2-rubygem-puppet-testsuite-3.8.7-20.1
ruby2.1-rubygem-puppet-3.8.7-20.1
ruby2.1-rubygem-puppet-doc-3.8.7-20.1
ruby2.1-rubygem-puppet-testsuite-3.8.7-20.1
ruby2.3-rubygem-puppet-doc-3.8.7-20.1
ruby2.2-rubygem-puppet-3.8.7-20.1
ruby2.2-rubygem-puppet-doc-3.8.7-20.1
rubygem-puppet-3.8.7-20.1
ruby2.4-rubygem-puppet-doc-3.8.7-20.1

145660 - SuSE Linux 42.1 openSUSE-SU-2017:0152-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

openSUSE-SU-2017:0152-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00084.html>

SuSE Linux 42.1

i586

libgstcodecparsers-1_0-0-1.4.5-11.1
libgstwayland-1_0-0-debuginfo-1.4.5-11.1
libgstcodecparsers-1_0-0-debuginfo-1.4.5-11.1
libgstbadbase-1_0-0-debuginfo-1.4.5-11.1
gstreamer-plugins-bad-devel-1.4.5-11.1
libgstmpegts-1_0-0-1.4.5-11.1
gstreamer-plugins-bad-doc-1.4.5-11.1
libgsturidownloader-1_0-0-debuginfo-1.4.5-11.1
gstreamer-plugins-bad-1.4.5-11.1
libgstwayland-1_0-0-1.4.5-11.1
libgstbasecamerabinsrc-1_0-0-debuginfo-1.4.5-11.1
libgstinsertbin-1_0-0-1.4.5-11.1
libgsturidownloader-1_0-0-1.4.5-11.1
libgstbadbase-1_0-0-1.4.5-11.1
libgstbadvideo-1_0-0-1.4.5-11.1
libgstbasecamerabinsrc-1_0-0-1.4.5-11.1
libgstinsertbin-1_0-0-debuginfo-1.4.5-11.1
libgstgl-1_0-0-debuginfo-1.4.5-11.1
gstreamer-plugins-bad-debuginfo-1.4.5-11.1
libgstmpegts-1_0-0-debuginfo-1.4.5-11.1
libgstphotography-1_0-0-debuginfo-1.4.5-11.1
gstreamer-plugins-bad-debugsource-1.4.5-11.1
libgstbadvideo-1_0-0-debuginfo-1.4.5-11.1
libgstphotography-1_0-0-1.4.5-11.1
libgstgl-1_0-0-1.4.5-11.1

noarch

gstreamer-plugins-bad-lang-1.4.5-11.1

x86_64

gstreamer-plugins-bad-debuginfo-32bit-1.4.5-11.1

gstreamer-plugins-bad-debugsource-1.4.5-11.1

libgstbadbase-1_0-0-32bit-1.4.5-11.1

libgstwayland-1_0-0-1.4.5-11.1

libgstmpegts-1_0-0-1.4.5-11.1

gstreamer-plugins-bad-1.4.5-11.1

libgstwayland-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstinsertbin-1_0-0-1.4.5-11.1

libgstbadvideo-1_0-0-debuginfo-1.4.5-11.1

libgstcodecparsers-1_0-0-1.4.5-11.1

libgstinsertbin-1_0-0-32bit-1.4.5-11.1

libgstgl-1_0-0-debuginfo-1.4.5-11.1

libgsturidownloader-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstbadbase-1_0-0-debuginfo-1.4.5-11.1

libgstbasecamerabinsrc-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstbasecamerabinsrc-1_0-0-1.4.5-11.1

libgstbadvideo-1_0-0-debuginfo-32bit-1.4.5-11.1

gstreamer-plugins-bad-doc-1.4.5-11.1

libgstgl-1_0-0-1.4.5-11.1

libgstbasecamerabinsrc-1_0-0-32bit-1.4.5-11.1

libgsturidownloader-1_0-0-1.4.5-11.1

libgstwayland-1_0-0-32bit-1.4.5-11.1

gstreamer-plugins-bad-devel-1.4.5-11.1

libgstinsertbin-1_0-0-debuginfo-1.4.5-11.1

libgsturidownloader-1_0-0-32bit-1.4.5-11.1

libgstbadvideo-1_0-0-32bit-1.4.5-11.1

libgstphotography-1_0-0-32bit-1.4.5-11.1

libgstphotography-1_0-0-1.4.5-11.1

libgstcodecparsers-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstgl-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstinsertbin-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstwayland-1_0-0-debuginfo-1.4.5-11.1

libgstbasecamerabinsrc-1_0-0-debuginfo-1.4.5-11.1

libgstbadbase-1_0-0-1.4.5-11.1

libgstgl-1_0-0-32bit-1.4.5-11.1

libgstcodecparsers-1_0-0-32bit-1.4.5-11.1

gstreamer-plugins-bad-32bit-1.4.5-11.1

libgstcodecparsers-1_0-0-debuginfo-1.4.5-11.1

libgstphotography-1_0-0-debuginfo-1.4.5-11.1

libgstmpegts-1_0-0-debuginfo-1.4.5-11.1

libgsturidownloader-1_0-0-debuginfo-1.4.5-11.1

gstreamer-plugins-bad-debuginfo-1.4.5-11.1

libgstbadvideo-1_0-0-1.4.5-11.1

libgstphotography-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstmpegts-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstbadbase-1_0-0-debuginfo-32bit-1.4.5-11.1

libgstmpegts-1_0-0-32bit-1.4.5-11.1

145664 - SuSE Linux 42.2 openSUSE-SU-2017:0155-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7445, CVE-2016-8332, CVE-2016-9112, CVE-2016-9113, CVE-2016-9114, CVE-2016-9115, CVE-2016-9116, CVE-2016-9117, CVE-2016-9118, CVE-2016-9572, CVE-2016-9573, CVE-2016-9580, CVE-2016-9581

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0155-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00087.html>

SuSE Linux 42.2

x86_64

libopenjp2-7-2.1.0-11.1

libopenjp2-7-debuginfo-2.1.0-11.1

openjpeg2-2.1.0-11.1

openjpeg2-debugsource-2.1.0-11.1

openjpeg2-devel-2.1.0-11.1

libopenjp2-7-32bit-2.1.0-11.1

libopenjp2-7-debuginfo-32bit-2.1.0-11.1

openjpeg2-debuginfo-2.1.0-11.1

i586

libopenjp2-7-2.1.0-11.1

libopenjp2-7-debuginfo-2.1.0-11.1

openjpeg2-2.1.0-11.1

openjpeg2-debugsource-2.1.0-11.1

openjpeg2-devel-2.1.0-11.1

openjpeg2-debuginfo-2.1.0-11.1

145666 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1021-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1021-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00054.html>

SuSE Linux 42.1

i586

postgresql93-plpython-9.3.14-8.1

postgresql93-server-debuginfo-9.3.14-8.1

postgresql93-pltcl-debuginfo-9.3.14-8.1

postgresql93-contrib-debuginfo-9.3.14-8.1

postgresql93-pltcl-9.3.14-8.1

postgresql93-plpython-debuginfo-9.3.14-8.1

postgresql93-9.3.14-8.1

postgresql93-server-9.3.14-8.1

postgresql93-libs-debugsource-9.3.14-8.1

postgresql93-devel-9.3.14-8.1

postgresql93-debugsource-9.3.14-8.1
postgresql93-contrib-9.3.14-8.1
postgresql93-plperl-9.3.14-8.1
postgresql93-test-9.3.14-8.1
postgresql93-debuginfo-9.3.14-8.1
postgresql93-devel-debuginfo-9.3.14-8.1
postgresql93-plperl-debuginfo-9.3.14-8.1

noarch
postgresql93-docs-9.3.14-8.1

x86_64
postgresql93-plpython-9.3.14-8.1
postgresql93-server-debuginfo-9.3.14-8.1
postgresql93-pltcl-debuginfo-9.3.14-8.1
postgresql93-contrib-debuginfo-9.3.14-8.1
postgresql93-pltcl-9.3.14-8.1
postgresql93-plpython-debuginfo-9.3.14-8.1
postgresql93-9.3.14-8.1
postgresql93-server-9.3.14-8.1
postgresql93-libs-debugsource-9.3.14-8.1
postgresql93-devel-9.3.14-8.1
postgresql93-debugsource-9.3.14-8.1
postgresql93-contrib-9.3.14-8.1
postgresql93-plperl-9.3.14-8.1
postgresql93-test-9.3.14-8.1
postgresql93-debuginfo-9.3.14-8.1
postgresql93-devel-debuginfo-9.3.14-8.1
postgresql93-plperl-debuginfo-9.3.14-8.1

SuSE Linux 42.2
i586
postgresql93-libs-debugsource-9.3.14-5.5.1
postgresql93-devel-debuginfo-9.3.14-5.5.1
postgresql93-devel-9.3.14-5.5.1

noarch
postgresql93-docs-9.3.14-5.5.1

x86_64
postgresql93-plpython-debuginfo-9.3.14-5.5.1
postgresql93-plperl-9.3.14-5.5.1
postgresql93-test-9.3.14-5.5.1
postgresql93-contrib-debuginfo-9.3.14-5.5.1
postgresql93-server-9.3.14-5.5.1
postgresql93-contrib-9.3.14-5.5.1
postgresql93-debuginfo-9.3.14-5.5.1
postgresql93-server-debuginfo-9.3.14-5.5.1
postgresql93-9.3.14-5.5.1
postgresql93-plpython-9.3.14-5.5.1
postgresql93-pltcl-9.3.14-5.5.1
postgresql93-devel-9.3.14-5.5.1
postgresql93-debugsource-9.3.14-5.5.1
postgresql93-plperl-debuginfo-9.3.14-5.5.1
postgresql93-devel-debuginfo-9.3.14-5.5.1
postgresql93-libs-debugsource-9.3.14-5.5.1
postgresql93-pltcl-debuginfo-9.3.14-5.5.1

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

Risk Level: Medium

CVE: CVE-2016-9102, CVE-2016-9103, CVE-2016-9381, CVE-2016-9776, CVE-2016-9845, CVE-2016-9846, CVE-2016-9907, CVE-2016-9908, CVE-2016-9911, CVE-2016-9912, CVE-2016-9913, CVE-2016-9921, CVE-2016-9922

Description

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

openSUSE-SU-2017:0194-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00109.html>

SuSE Linux 42.2

i586

qemu-ppc-debuginfo-2.6.2-26.1

qemu-tools-2.6.2-26.1

qemu-x86-2.6.2-26.1

qemu-block-ssh-debuginfo-2.6.2-26.1

qemu-linux-user-debugsource-2.6.2-26.1

qemu-ppc-2.6.2-26.1

qemu-block-ssh-2.6.2-26.1

qemu-block-dmg-2.6.2-26.1

qemu-kvm-2.6.2-26.1

qemu-arm-2.6.2-26.1

qemu-block-curl-2.6.2-26.1

qemu-debugsource-2.6.2-26.1

qemu-arm-debuginfo-2.6.2-26.1

qemu-block-iscsi-debuginfo-2.6.2-26.1

qemu-guest-agent-debuginfo-2.6.2-26.1

qemu-linux-user-debuginfo-2.6.2-26.1

qemu-block-dmg-debuginfo-2.6.2-26.1

qemu-lang-2.6.2-26.1

qemu-block-iscsi-2.6.2-26.1

qemu-testsuite-2.6.2-26.1

qemu-guest-agent-2.6.2-26.1

qemu-extra-debuginfo-2.6.2-26.1

qemu-block-curl-debuginfo-2.6.2-26.1

qemu-s390-2.6.2-26.1

qemu-extra-2.6.2-26.1

qemu-x86-debuginfo-2.6.2-26.1

qemu-s390-debuginfo-2.6.2-26.1

qemu-linux-user-2.6.2-26.1

qemu-2.6.2-26.1

qemu-tools-debuginfo-2.6.2-26.1

noarch

qemu-ipxe-1.0.0-26.1

qemu-vgabios-1.9.1-26.1

qemu-seabios-1.9.1-26.1

qemu-sgabios-8-26.1

x86_64

qemu-ppc-debuginfo-2.6.2-26.1

qemu-tools-2.6.2-26.1

qemu-x86-2.6.2-26.1

qemu-block-ssh-debuginfo-2.6.2-26.1

qemu-linux-user-debugsource-2.6.2-26.1
qemu-ppc-2.6.2-26.1
qemu-block-ssh-2.6.2-26.1
qemu-block-dmg-2.6.2-26.1
qemu-kvm-2.6.2-26.1
qemu-block-rbd-debuginfo-2.6.2-26.1
qemu-arm-2.6.2-26.1
qemu-block-curl-2.6.2-26.1
qemu-debugsource-2.6.2-26.1
qemu-arm-debuginfo-2.6.2-26.1
qemu-block-iscsi-debuginfo-2.6.2-26.1
qemu-guest-agent-debuginfo-2.6.2-26.1
qemu-linux-user-debuginfo-2.6.2-26.1
qemu-block-dmg-debuginfo-2.6.2-26.1
qemu-lang-2.6.2-26.1
qemu-block-iscsi-2.6.2-26.1
qemu-block-rbd-2.6.2-26.1
qemu-testsuite-2.6.2-26.1
qemu-guest-agent-2.6.2-26.1
qemu-extra-debuginfo-2.6.2-26.1
qemu-block-curl-debuginfo-2.6.2-26.1
qemu-s390-2.6.2-26.1
qemu-extra-2.6.2-26.1
qemu-x86-debuginfo-2.6.2-26.1
qemu-s390-debuginfo-2.6.2-26.1
qemu-linux-user-2.6.2-26.1
qemu-2.6.2-26.1
qemu-tools-debuginfo-2.6.2-26.1

145675 - SuSE Linux 42.2 openSUSE-SU-2017:0388-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9809

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0388-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00025.html>

SuSE Linux 42.2

i586

libgstsignalprocessor-0_10-23-0.10.23-27.1
libgstbasecamerabinsrc-0_10-23-debuginfo-0.10.23-27.1
libgstphotography-0_10-23-0.10.23-27.1
libgstsignalprocessor-0_10-23-debuginfo-0.10.23-27.1
gstreamer-0_10-plugins-bad-debuginfo-0.10.23-27.1
libgstbasevideo-0_10-23-0.10.23-27.1
gstreamer-0_10-plugins-bad-0.10.23-27.1
gstreamer-0_10-plugins-bad-devel-0.10.23-27.1
libgstvdp-0_10-23-0.10.23-27.1
gstreamer-0_10-plugins-bad-debugsource-0.10.23-27.1
libgstcodecparsers-0_10-23-debuginfo-0.10.23-27.1

gststreamer-0_10-plugins-bad-doc-0.10.23-27.1
libgstbasevideo-0_10-23-debuginfo-0.10.23-27.1
libgstphotography-0_10-23-debuginfo-0.10.23-27.1
libgstvdvp-0_10-23-debuginfo-0.10.23-27.1
libgstcodecparsers-0_10-23-0.10.23-27.1
libgstbasecamerabinsrc-0_10-23-0.10.23-27.1

noarch
gststreamer-0_10-plugins-bad-lang-0.10.23-27.1

x86_64
libgstphotography-0_10-23-debuginfo-0.10.23-27.1
libgstcodecparsers-0_10-23-debuginfo-0.10.23-27.1
gststreamer-0_10-plugins-bad-32bit-0.10.23-27.1
libgstbasevideo-0_10-23-debuginfo-32bit-0.10.23-27.1
libgstvdvp-0_10-23-debuginfo-0.10.23-27.1
gststreamer-0_10-plugins-bad-doc-0.10.23-27.1
libgstphotography-0_10-23-32bit-0.10.23-27.1
gststreamer-0_10-plugins-bad-debugsource-0.10.23-27.1
libgstbasecamerabinsrc-0_10-23-32bit-0.10.23-27.1
libgstphotography-0_10-23-0.10.23-27.1
libgstbasecamerabinsrc-0_10-23-debuginfo-0.10.23-27.1
libgstbasevideo-0_10-23-32bit-0.10.23-27.1
libgstcodecparsers-0_10-23-32bit-0.10.23-27.1
libgstbasevideo-0_10-23-0.10.23-27.1
libgstvdvp-0_10-23-debuginfo-32bit-0.10.23-27.1
libgstbasecamerabinsrc-0_10-23-0.10.23-27.1
libgstcodecparsers-0_10-23-0.10.23-27.1
libgstsignalprocessor-0_10-23-debuginfo-32bit-0.10.23-27.1
gststreamer-0_10-plugins-bad-debuginfo-32bit-0.10.23-27.1
libgstvdvp-0_10-23-0.10.23-27.1
libgstphotography-0_10-23-debuginfo-32bit-0.10.23-27.1
libgstsignalprocessor-0_10-23-debuginfo-0.10.23-27.1
libgstvdvp-0_10-23-32bit-0.10.23-27.1
gststreamer-0_10-plugins-bad-devel-0.10.23-27.1
gststreamer-0_10-plugins-bad-debuginfo-0.10.23-27.1
libgstbasecamerabinsrc-0_10-23-debuginfo-32bit-0.10.23-27.1
libgstcodecparsers-0_10-23-debuginfo-32bit-0.10.23-27.1
libgstbasevideo-0_10-23-debuginfo-0.10.23-27.1
libgstsignalprocessor-0_10-23-0.10.23-27.1
gststreamer-0_10-plugins-bad-0.10.23-27.1
libgstsignalprocessor-0_10-23-32bit-0.10.23-27.1

145676 - SuSE Linux 42.2 openSUSE-SU-2017:1633-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000364, CVE-2017-1000380, CVE-2017-7346, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1633-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00076.html>

SuSE Linux 42.2
x86_64
kernel-vanilla-base-debuginfo-4.4.72-18.12.2
kernel-obs-build-debugsource-4.4.72-18.12.2
kernel-debug-base-4.4.72-18.12.2
kernel-vanilla-base-4.4.72-18.12.2
kernel-default-devel-4.4.72-18.12.2
kernel-vanilla-debugsource-4.4.72-18.12.2
kernel-debug-debuginfo-4.4.72-18.12.2
kernel-default-4.4.72-18.12.2
kernel-debug-devel-4.4.72-18.12.2
kernel-obs-qa-4.4.72-18.12.1
kernel-default-debugsource-4.4.72-18.12.2
kernel-default-base-debuginfo-4.4.72-18.12.2
kernel-vanilla-debuginfo-4.4.72-18.12.2
kernel-debug-debugsource-4.4.72-18.12.2
kernel-default-debuginfo-4.4.72-18.12.2
kernel-default-base-4.4.72-18.12.2
kernel-debug-devel-debuginfo-4.4.72-18.12.2
kernel-vanilla-4.4.72-18.12.2
kernel-debug-base-debuginfo-4.4.72-18.12.2
kernel-vanilla-devel-4.4.72-18.12.2
kernel-syms-4.4.72-18.12.1
kernel-obs-build-4.4.72-18.12.2
kernel-debug-4.4.72-18.12.2

noarch
kernel-docs-4.4.72-18.12.3
kernel-docs-html-4.4.72-18.12.3
kernel-source-vanilla-4.4.72-18.12.1
kernel-devel-4.4.72-18.12.1
kernel-macros-4.4.72-18.12.1
kernel-docs-pdf-4.4.72-18.12.3
kernel-source-4.4.72-18.12.1

145678 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2366-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10397, CVE-2016-5766, CVE-2017-11143, CVE-2017-11144, CVE-2017-11145, CVE-2017-11146, CVE-2017-11147, CVE-2017-11628, CVE-2017-7890

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2366-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00016.html>

SuSE Linux 42.2
i586
php5-fastcgi-5.5.14-77.9.1
php5-fpm-5.5.14-77.9.1
php5-tidy-debuginfo-5.5.14-77.9.1
php5-gettext-5.5.14-77.9.1

php5-exif-debuginfo-5.5.14-77.9.1
php5-pdo-5.5.14-77.9.1
php5-debuginfo-5.5.14-77.9.1
php5-iconv-5.5.14-77.9.1
php5-ctype-debuginfo-5.5.14-77.9.1
php5-dba-debuginfo-5.5.14-77.9.1
php5-mysql-5.5.14-77.9.1
php5-dba-5.5.14-77.9.1
php5-sysvsem-debuginfo-5.5.14-77.9.1
php5-calendar-5.5.14-77.9.1
php5-firebird-debuginfo-5.5.14-77.9.1
php5-firebird-5.5.14-77.9.1
php5-shmop-5.5.14-77.9.1
php5-sysvmsg-debuginfo-5.5.14-77.9.1
php5-zlib-debuginfo-5.5.14-77.9.1
php5-ftp-5.5.14-77.9.1
php5-sockets-5.5.14-77.9.1
php5-fileinfo-debuginfo-5.5.14-77.9.1
php5-exif-5.5.14-77.9.1
php5-posix-debuginfo-5.5.14-77.9.1
php5-dom-debuginfo-5.5.14-77.9.1
php5-ldap-debuginfo-5.5.14-77.9.1
php5-xmlwriter-debuginfo-5.5.14-77.9.1
php5-bcmath-5.5.14-77.9.1
php5-fileinfo-5.5.14-77.9.1
php5-suhosin-debuginfo-5.5.14-77.9.1
php5-bz2-debuginfo-5.5.14-77.9.1
php5-fastcgi-debuginfo-5.5.14-77.9.1
php5-enchanted-5.5.14-77.9.1
php5-bz2-5.5.14-77.9.1
php5-zlib-5.5.14-77.9.1
php5-ctype-5.5.14-77.9.1
php5-zip-5.5.14-77.9.1
php5-dom-5.5.14-77.9.1
php5-phar-5.5.14-77.9.1
php5-wddx-debuginfo-5.5.14-77.9.1
php5-shmop-debuginfo-5.5.14-77.9.1
php5-odbc-debuginfo-5.5.14-77.9.1
php5-curl-5.5.14-77.9.1
php5-xmlwriter-5.5.14-77.9.1
php5-calendar-debuginfo-5.5.14-77.9.1
php5-openssl-5.5.14-77.9.1
php5-gettext-debuginfo-5.5.14-77.9.1
php5-zip-debuginfo-5.5.14-77.9.1
php5-gd-debuginfo-5.5.14-77.9.1
php5-pcntl-5.5.14-77.9.1
php5-sqlite-debuginfo-5.5.14-77.9.1
php5-sysvsem-5.5.14-77.9.1
php5-sysvshm-debuginfo-5.5.14-77.9.1
php5-ldap-debuginfo-5.5.14-77.9.1
php5-bcmath-debuginfo-5.5.14-77.9.1
php5-opcache-debuginfo-5.5.14-77.9.1
php5-tokenizer-debuginfo-5.5.14-77.9.1
php5-iconv-debuginfo-5.5.14-77.9.1
php5-pspell-5.5.14-77.9.1
php5-wddx-5.5.14-77.9.1
php5-pdo-debuginfo-5.5.14-77.9.1
php5-phar-debuginfo-5.5.14-77.9.1
php5-opcache-5.5.14-77.9.1
php5-readline-5.5.14-77.9.1

php5-gmp-debuginfo-5.5.14-77.9.1
php5-tokenizer-5.5.14-77.9.1
php5-pcntl-debuginfo-5.5.14-77.9.1
php5-gmp-5.5.14-77.9.1
php5-json-debuginfo-5.5.14-77.9.1
php5-pgsql-debuginfo-5.5.14-77.9.1
php5-mbstring-debuginfo-5.5.14-77.9.1
php5-mssql-debuginfo-5.5.14-77.9.1
php5-sysvmsg-5.5.14-77.9.1
php5-xmlreader-5.5.14-77.9.1
php5-intl-5.5.14-77.9.1
php5-soap-debuginfo-5.5.14-77.9.1
php5-pspell-debuginfo-5.5.14-77.9.1
php5-sockets-debuginfo-5.5.14-77.9.1
php5-sqlite-5.5.14-77.9.1
php5-openssl-debuginfo-5.5.14-77.9.1
php5-snmp-5.5.14-77.9.1
php5-odbc-5.5.14-77.9.1
php5-sysvshm-5.5.14-77.9.1
php5-ftp-debuginfo-5.5.14-77.9.1
php5-xsl-5.5.14-77.9.1
php5-imap-5.5.14-77.9.1
php5-xsl-debuginfo-5.5.14-77.9.1
php5-mbstring-5.5.14-77.9.1
apache2-mod_php5-5.5.14-77.9.1
php5-debugsource-5.5.14-77.9.1
php5-curl-debuginfo-5.5.14-77.9.1
php5-intl-debuginfo-5.5.14-77.9.1
php5-pgsql-5.5.14-77.9.1
php5-readline-debuginfo-5.5.14-77.9.1
apache2-mod_php5-debuginfo-5.5.14-77.9.1
php5-ldap-5.5.14-77.9.1
php5-mcrypt-5.5.14-77.9.1
php5-suhosin-5.5.14-77.9.1
php5-xmlrpc-debuginfo-5.5.14-77.9.1
php5-enchanted-debuginfo-5.5.14-77.9.1
php5-tidy-5.5.14-77.9.1
php5-posix-5.5.14-77.9.1
php5-mcrypt-debuginfo-5.5.14-77.9.1
php5-5.5.14-77.9.1
php5-json-5.5.14-77.9.1
php5-xmlreader-debuginfo-5.5.14-77.9.1
php5-mssql-5.5.14-77.9.1
php5-devel-5.5.14-77.9.1
php5-fpm-debuginfo-5.5.14-77.9.1
php5-mysql-debuginfo-5.5.14-77.9.1
php5-gd-5.5.14-77.9.1
php5-snmp-debuginfo-5.5.14-77.9.1
php5-xmlrpc-5.5.14-77.9.1
php5-soap-5.5.14-77.9.1

noarch

php5-pear-5.5.14-77.9.1

x86_64

php5-fastcgi-5.5.14-77.9.1

php5-fpm-5.5.14-77.9.1

php5-tidy-debuginfo-5.5.14-77.9.1

php5-gettext-5.5.14-77.9.1

php5-exif-debuginfo-5.5.14-77.9.1

php5-pdo-5.5.14-77.9.1
php5-debuginfo-5.5.14-77.9.1
php5-iconv-5.5.14-77.9.1
php5-ctype-debuginfo-5.5.14-77.9.1
php5-dba-debuginfo-5.5.14-77.9.1
php5-mysql-5.5.14-77.9.1
php5-dba-5.5.14-77.9.1
php5-sysvsem-debuginfo-5.5.14-77.9.1
php5-calendar-5.5.14-77.9.1
php5-firebird-debuginfo-5.5.14-77.9.1
php5-firebird-5.5.14-77.9.1
php5-shmop-5.5.14-77.9.1
php5-sysvmsg-debuginfo-5.5.14-77.9.1
php5-zlib-debuginfo-5.5.14-77.9.1
php5-ftp-5.5.14-77.9.1
php5-sockets-5.5.14-77.9.1
php5-fileinfo-debuginfo-5.5.14-77.9.1
php5-exif-5.5.14-77.9.1
php5-posix-debuginfo-5.5.14-77.9.1
php5-dom-debuginfo-5.5.14-77.9.1
php5-ldap-debuginfo-5.5.14-77.9.1
php5-xmlwriter-debuginfo-5.5.14-77.9.1
php5-bcmath-5.5.14-77.9.1
php5-fileinfo-5.5.14-77.9.1
php5-suhosin-debuginfo-5.5.14-77.9.1
php5-bz2-debuginfo-5.5.14-77.9.1
php5-fastcgi-debuginfo-5.5.14-77.9.1
php5-enchanted-5.5.14-77.9.1
php5-bz2-5.5.14-77.9.1
php5-zlib-5.5.14-77.9.1
php5-ctype-5.5.14-77.9.1
php5-zip-5.5.14-77.9.1
php5-dom-5.5.14-77.9.1
php5-phar-5.5.14-77.9.1
php5-wddx-debuginfo-5.5.14-77.9.1
php5-shmop-debuginfo-5.5.14-77.9.1
php5-odbc-debuginfo-5.5.14-77.9.1
php5-curl-5.5.14-77.9.1
php5-xmlwriter-5.5.14-77.9.1
php5-calendar-debuginfo-5.5.14-77.9.1
php5-openssl-5.5.14-77.9.1
php5-gettext-debuginfo-5.5.14-77.9.1
php5-zip-debuginfo-5.5.14-77.9.1
php5-gd-debuginfo-5.5.14-77.9.1
php5-pcntl-5.5.14-77.9.1
php5-sqlite-debuginfo-5.5.14-77.9.1
php5-sysvsem-5.5.14-77.9.1
php5-sysvshm-debuginfo-5.5.14-77.9.1
php5-ldap-debuginfo-5.5.14-77.9.1
php5-bcmath-debuginfo-5.5.14-77.9.1
php5-opcache-debuginfo-5.5.14-77.9.1
php5-tokenizer-debuginfo-5.5.14-77.9.1
php5-iconv-debuginfo-5.5.14-77.9.1
php5-ispell-5.5.14-77.9.1
php5-wddx-5.5.14-77.9.1
php5-pdo-debuginfo-5.5.14-77.9.1
php5-phar-debuginfo-5.5.14-77.9.1
php5-opcache-5.5.14-77.9.1
php5-readline-5.5.14-77.9.1
php5-gmp-debuginfo-5.5.14-77.9.1

php5-tokenizer-5.5.14-77.9.1
php5-pcntl-debuginfo-5.5.14-77.9.1
php5-gmp-5.5.14-77.9.1
php5-json-debuginfo-5.5.14-77.9.1
php5-pgsql-debuginfo-5.5.14-77.9.1
php5-mbstring-debuginfo-5.5.14-77.9.1
php5-mssql-debuginfo-5.5.14-77.9.1
php5-sysvmsg-5.5.14-77.9.1
php5-xmlreader-5.5.14-77.9.1
php5-intl-5.5.14-77.9.1
php5-soap-debuginfo-5.5.14-77.9.1
php5-pspell-debuginfo-5.5.14-77.9.1
php5-sockets-debuginfo-5.5.14-77.9.1
php5-sqlite-5.5.14-77.9.1
php5-openssl-debuginfo-5.5.14-77.9.1
php5-snmp-5.5.14-77.9.1
php5-odbc-5.5.14-77.9.1
php5-sysvshm-5.5.14-77.9.1
php5-ftp-debuginfo-5.5.14-77.9.1
php5-xsl-5.5.14-77.9.1
php5-imap-5.5.14-77.9.1
php5-xsl-debuginfo-5.5.14-77.9.1
php5-mbstring-5.5.14-77.9.1
apache2-mod_php5-5.5.14-77.9.1
php5-debugsource-5.5.14-77.9.1
php5-curl-debuginfo-5.5.14-77.9.1
php5-intl-debuginfo-5.5.14-77.9.1
php5-pgsql-5.5.14-77.9.1
php5-readline-debuginfo-5.5.14-77.9.1
apache2-mod_php5-debuginfo-5.5.14-77.9.1
php5-ldap-5.5.14-77.9.1
php5-mcrypt-5.5.14-77.9.1
php5-suhosin-5.5.14-77.9.1
php5-xmlrpc-debuginfo-5.5.14-77.9.1
php5-enchanted-debuginfo-5.5.14-77.9.1
php5-tidy-5.5.14-77.9.1
php5-posix-5.5.14-77.9.1
php5-mcrypt-debuginfo-5.5.14-77.9.1
php5-5.5.14-77.9.1
php5-json-5.5.14-77.9.1
php5-xmlreader-debuginfo-5.5.14-77.9.1
php5-mssql-5.5.14-77.9.1
php5-devel-5.5.14-77.9.1

SuSE Linux 42.3

i586

php5-mysql-5.5.14-82.1

145684 - SuSE Linux 42.1 openSUSE-SU-2017:0332-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5545, CVE-2017-3290, CVE-2017-3316, CVE-2017-3332

Description

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

openSUSE-SU-2017:0332-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00173.html>

SuSE Linux 42.1

x86_64

virtualbox-qt-debuginfo-5.0.32-34.1

virtualbox-guest-kmp-default-debuginfo-5.0.32_k4.1.36_44-34.1

virtualbox-guest-tools-5.0.32-34.1

virtualbox-debugsource-5.0.32-34.1

virtualbox-websrv-5.0.32-34.1

virtualbox-guest-x11-debuginfo-5.0.32-34.1

virtualbox-devel-5.0.32-34.1

virtualbox-qt-5.0.32-34.1

virtualbox-guest-tools-debuginfo-5.0.32-34.1

virtualbox-host-kmp-default-5.0.32_k4.1.36_44-34.1

virtualbox-debuginfo-5.0.32-34.1

virtualbox-websrv-debuginfo-5.0.32-34.1

virtualbox-host-kmp-default-debuginfo-5.0.32_k4.1.36_44-34.1

virtualbox-guest-x11-5.0.32-34.1

virtualbox-guest-kmp-default-5.0.32_k4.1.36_44-34.1

python-virtualbox-5.0.32-34.1

virtualbox-5.0.32-34.1

python-virtualbox-debuginfo-5.0.32-34.1

noarch

virtualbox-guest-desktop-icons-5.0.32-34.1

virtualbox-host-source-5.0.32-34.1

145687 - SuSE Linux 42.2 openSUSE-SU-2017:1899-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11110

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1899-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00076.html>

SuSE Linux 42.2

x86_64

catdoc-debuginfo-0.95-7.6.1

catdoc-0.95-7.6.1

catdoc-debugsource-0.95-7.6.1

i586

catdoc-debuginfo-0.95-7.6.1

catdoc-0.95-7.6.1

catdoc-debugsource-0.95-7.6.1

145689 - SuSE Linux 42.2 openSUSE-SU-2017:1142-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3513, CVE-2017-3538, CVE-2017-3558, CVE-2017-3559, CVE-2017-3561, CVE-2017-3563, CVE-2017-3575, CVE-2017-3576, CVE-2017-3587

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1142-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00003.html>

SuSE Linux 42.2

x86_64

virtualbox-guest-tools-debuginfo-5.1.22-19.10.1

virtualbox-qt-5.1.22-19.10.1

virtualbox-devel-5.1.22-19.10.1

python-virtualbox-debuginfo-5.1.22-19.10.1

virtualbox-guest-x11-debuginfo-5.1.22-19.10.1

virtualbox-guest-kmp-default-debuginfo-5.1.22_k4.4.57_18.3-19.10.1

virtualbox-5.1.22-19.10.1

virtualbox-guest-kmp-default-5.1.22_k4.4.57_18.3-19.10.1

virtualbox-guest-tools-5.1.22-19.10.1

python-virtualbox-5.1.22-19.10.1

virtualbox-debugsource-5.1.22-19.10.1

virtualbox-host-kmp-default-debuginfo-5.1.22_k4.4.57_18.3-19.10.1

virtualbox-websrv-5.1.22-19.10.1

virtualbox-websrv-debuginfo-5.1.22-19.10.1

virtualbox-qt-debuginfo-5.1.22-19.10.1

virtualbox-debuginfo-5.1.22-19.10.1

virtualbox-host-kmp-default-5.1.22_k4.4.57_18.3-19.10.1

virtualbox-guest-x11-5.1.22-19.10.1

noarch

virtualbox-host-source-5.1.22-19.10.1

virtualbox-guest-desktop-icons-5.1.22-19.10.1

145698 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1108-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10266, CVE-2016-10267, CVE-2016-10268, CVE-2016-10269, CVE-2016-10270, CVE-2016-10271, CVE-2016-10272

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1108-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00097.html>

SuSE Linux 42.1

x86_64
tiff-debuginfo-4.0.7-18.1
libtiff-devel-4.0.7-18.1
libtiff5-debuginfo-4.0.7-18.1
libtiff5-4.0.7-18.1
tiff-debugsource-4.0.7-18.1
libtiff5-debuginfo-32bit-4.0.7-18.1
tiff-4.0.7-18.1
libtiff5-32bit-4.0.7-18.1
libtiff-devel-32bit-4.0.7-18.1

i586

tiff-debuginfo-4.0.7-18.1
libtiff-devel-4.0.7-18.1
libtiff5-debuginfo-4.0.7-18.1
libtiff5-4.0.7-18.1
tiff-debugsource-4.0.7-18.1
tiff-4.0.7-18.1

SuSE Linux 42.2

x86_64
libtiff5-debuginfo-32bit-4.0.7-17.3.1
libtiff5-debuginfo-4.0.7-17.3.1
tiff-4.0.7-17.3.1
libtiff5-4.0.7-17.3.1
tiff-debuginfo-4.0.7-17.3.1
libtiff5-32bit-4.0.7-17.3.1
libtiff-devel-32bit-4.0.7-17.3.1
libtiff-devel-4.0.7-17.3.1
tiff-debugsource-4.0.7-17.3.1

i586

libtiff5-debuginfo-4.0.7-17.3.1
tiff-4.0.7-17.3.1
libtiff5-4.0.7-17.3.1
tiff-debuginfo-4.0.7-17.3.1
libtiff-devel-4.0.7-17.3.1
tiff-debugsource-4.0.7-17.3.1

145699 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:1985-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11403

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1985-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00101.html>

SuSE Linux 42.2

x86_64

libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.15.1
GraphicsMagick-debuginfo-1.3.25-11.15.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.15.1
GraphicsMagick-devel-1.3.25-11.15.1
GraphicsMagick-debugsource-1.3.25-11.15.1
libGraphicsMagick++-Q16-12-1.3.25-11.15.1
perl-GraphicsMagick-debuginfo-1.3.25-11.15.1
GraphicsMagick-1.3.25-11.15.1
libGraphicsMagick++-devel-1.3.25-11.15.1
libGraphicsMagick-Q16-3-1.3.25-11.15.1
perl-GraphicsMagick-1.3.25-11.15.1
libGraphicsMagick3-config-1.3.25-11.15.1
libGraphicsMagickWand-Q16-2-1.3.25-11.15.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.15.1

i586

libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.15.1
GraphicsMagick-debuginfo-1.3.25-11.15.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.15.1
GraphicsMagick-devel-1.3.25-11.15.1
GraphicsMagick-debugsource-1.3.25-11.15.1
libGraphicsMagick++-Q16-12-1.3.25-11.15.1
perl-GraphicsMagick-debuginfo-1.3.25-11.15.1
GraphicsMagick-1.3.25-11.15.1
libGraphicsMagick++-devel-1.3.25-11.15.1
libGraphicsMagick-Q16-3-1.3.25-11.15.1
perl-GraphicsMagick-1.3.25-11.15.1
libGraphicsMagick3-config-1.3.25-11.15.1
libGraphicsMagickWand-Q16-2-1.3.25-11.15.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.15.1

SuSE Linux 42.3

x86_64

libGraphicsMagick-Q16-3-1.3.25-17.1
GraphicsMagick-1.3.25-17.1
perl-GraphicsMagick-1.3.25-17.1
GraphicsMagick-debugsource-1.3.25-17.1
libGraphicsMagickWand-Q16-2-1.3.25-17.1
GraphicsMagick-debuginfo-1.3.25-17.1
libGraphicsMagick3-config-1.3.25-17.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-17.1
libGraphicsMagick++-devel-1.3.25-17.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-17.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-17.1
libGraphicsMagick++-Q16-12-1.3.25-17.1
GraphicsMagick-devel-1.3.25-17.1
perl-GraphicsMagick-debuginfo-1.3.25-17.1

i586

libGraphicsMagick-Q16-3-1.3.25-17.1
GraphicsMagick-1.3.25-17.1
perl-GraphicsMagick-1.3.25-17.1
GraphicsMagick-debugsource-1.3.25-17.1
libGraphicsMagickWand-Q16-2-1.3.25-17.1
GraphicsMagick-debuginfo-1.3.25-17.1
libGraphicsMagick3-config-1.3.25-17.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-17.1
libGraphicsMagick++-devel-1.3.25-17.1

libGraphicsMagick++-Q16-12-debuginfo-1.3.25-17.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-17.1
libGraphicsMagick++-Q16-12-1.3.25-17.1
GraphicsMagick-devel-1.3.25-17.1
perl-GraphicsMagick-debuginfo-1.3.25-17.1

145705 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0101-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8654, CVE-2016-9395, CVE-2016-9398, CVE-2016-9560, CVE-2016-9591

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0101-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00061.html>

SuSE Linux 42.1

x86_64
libjasper1-debuginfo-32bit-1.900.14-170.1
libjasper1-1.900.14-170.1
jasper-debuginfo-1.900.14-170.1
jasper-debugsource-1.900.14-170.1
libjasper-devel-1.900.14-170.1
libjasper1-debuginfo-1.900.14-170.1
libjasper1-32bit-1.900.14-170.1
jasper-1.900.14-170.1

i586

libjasper1-1.900.14-170.1
jasper-debuginfo-1.900.14-170.1
jasper-debugsource-1.900.14-170.1
libjasper-devel-1.900.14-170.1
libjasper1-debuginfo-1.900.14-170.1
jasper-1.900.14-170.1

SuSE Linux 42.2

x86_64
libjasper1-debuginfo-32bit-1.900.14-170.1
libjasper1-1.900.14-170.1
jasper-debuginfo-1.900.14-170.1
jasper-debugsource-1.900.14-170.1
libjasper-devel-1.900.14-170.1
libjasper1-debuginfo-1.900.14-170.1
libjasper1-32bit-1.900.14-170.1
jasper-1.900.14-170.1

i586

libjasper1-1.900.14-170.1
jasper-debuginfo-1.900.14-170.1
jasper-debugsource-1.900.14-170.1
libjasper-devel-1.900.14-170.1
libjasper1-debuginfo-1.900.14-170.1

145706 - SuSE Linux 42.2 openSUSE-SU-2017:1571-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9324

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1571-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00048.html>

SuSE Linux 42.2

noarch

otrs-3.3.17-5.3.1

otrs-doc-3.3.17-5.3.1

otrs-itsm-3.3.14-5.3.1

145711 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0648-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8685, CVE-2016-8686

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0648-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00015.html>

SuSE Linux 42.1

x86_64

ptrace-debuginfo-1.14-8.1

ptrace-1.14-8.1

libptrace0-debuginfo-1.14-8.1

ptrace-devel-1.14-8.1

libptrace0-1.14-8.1

ptrace-debugsource-1.14-8.1

i586

ptrace-debuginfo-1.14-8.1

ptrace-1.14-8.1

libptrace0-debuginfo-1.14-8.1

ptrace-devel-1.14-8.1

libptrace0-1.14-8.1

ptrace-debugsource-1.14-8.1

SuSE Linux 42.2
x86_64
potrace-debuginfo-1.14-8.1
potrace-1.14-8.1
libpotrace0-debuginfo-1.14-8.1
potrace-devel-1.14-8.1
libpotrace0-1.14-8.1
potrace-debugsource-1.14-8.1

i586
potrace-debuginfo-1.14-8.1
potrace-1.14-8.1
libpotrace0-debuginfo-1.14-8.1
potrace-devel-1.14-8.1
libpotrace0-1.14-8.1
potrace-debugsource-1.14-8.1

145713 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2309-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12976

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2309-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00115.html>

SuSE Linux 42.2
x86_64
git-annex-bash-completion-6.20170818-2.6.1
git-annex-6.20170818-2.6.1

SuSE Linux 42.3
x86_64
git-annex-6.20170818-3.1
git-annex-bash-completion-6.20170818-3.1

145722 - SuSE Linux 42.1 openSUSE-SU-2017:0528-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5209, CVE-2017-5834, CVE-2017-5835, CVE-2017-5836

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0528-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00096.html>

SuSE Linux 42.1

x86_64

libplist3-debuginfo-1.12-7.1

libplist++3-debuginfo-1.12-7.1

libplist3-32bit-1.12-7.1

libplist++3-debuginfo-32bit-1.12-7.1

plistutil-debuginfo-1.12-7.1

python-plist-debuginfo-1.12-7.1

libplist++3-1.12-7.1

plistutil-1.12-7.1

libplist3-debuginfo-32bit-1.12-7.1

libplist-devel-1.12-7.1

libplist3-1.12-7.1

python-plist-1.12-7.1

libplist-debugsource-1.12-7.1

libplist++-devel-1.12-7.1

libplist++3-32bit-1.12-7.1

i586

libplist3-debuginfo-1.12-7.1

plistutil-1.12-7.1

libplist++3-1.12-7.1

plistutil-debuginfo-1.12-7.1

libplist3-1.12-7.1

python-plist-debuginfo-1.12-7.1

libplist++3-debuginfo-1.12-7.1

libplist++-devel-1.12-7.1

libplist-devel-1.12-7.1

python-plist-1.12-7.1

libplist-debugsource-1.12-7.1

145723 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0374-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3260, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

Description

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

openSUSE-SU-2017:0374-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00017.html>

SuSE Linux 42.1

i586

java-1_8_0-openjdk-debugsource-1.8.0.121-21.4

java-1_8_0-openjdk-devel-1.8.0.121-21.4

java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-21.4

java-1_8_0-openjdk-accessibility-1.8.0.121-21.4

java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-21.4
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-21.4
java-1_8_0-openjdk-debuginfo-1.8.0.121-21.4
java-1_8_0-openjdk-headless-1.8.0.121-21.4
java-1_8_0-openjdk-src-1.8.0.121-21.4
java-1_8_0-openjdk-demo-1.8.0.121-21.4
java-1_8_0-openjdk-1.8.0.121-21.4

noarch
java-1_8_0-openjdk-javadoc-1.8.0.121-21.4

x86_64
java-1_8_0-openjdk-debugsource-1.8.0.121-21.4
java-1_8_0-openjdk-devel-1.8.0.121-21.4
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-21.4
java-1_8_0-openjdk-accessibility-1.8.0.121-21.4
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-21.4
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-21.4
java-1_8_0-openjdk-debuginfo-1.8.0.121-21.4
java-1_8_0-openjdk-headless-1.8.0.121-21.4
java-1_8_0-openjdk-src-1.8.0.121-21.4
java-1_8_0-openjdk-demo-1.8.0.121-21.4
java-1_8_0-openjdk-1.8.0.121-21.4

SuSE Linux 42.2

i586
java-1_8_0-openjdk-1.8.0.121-6.4
java-1_8_0-openjdk-accessibility-1.8.0.121-6.4
java-1_8_0-openjdk-demo-1.8.0.121-6.4
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-6.4
java-1_8_0-openjdk-debuginfo-1.8.0.121-6.4
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-6.4
java-1_8_0-openjdk-devel-1.8.0.121-6.4
java-1_8_0-openjdk-debugsource-1.8.0.121-6.4
java-1_8_0-openjdk-headless-1.8.0.121-6.4
java-1_8_0-openjdk-src-1.8.0.121-6.4
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-6.4

noarch
java-1_8_0-openjdk-javadoc-1.8.0.121-6.4

x86_64
java-1_8_0-openjdk-1.8.0.121-6.4
java-1_8_0-openjdk-accessibility-1.8.0.121-6.4
java-1_8_0-openjdk-demo-1.8.0.121-6.4
java-1_8_0-openjdk-devel-debuginfo-1.8.0.121-6.4
java-1_8_0-openjdk-debuginfo-1.8.0.121-6.4
java-1_8_0-openjdk-headless-debuginfo-1.8.0.121-6.4
java-1_8_0-openjdk-devel-1.8.0.121-6.4
java-1_8_0-openjdk-debugsource-1.8.0.121-6.4
java-1_8_0-openjdk-headless-1.8.0.121-6.4
java-1_8_0-openjdk-src-1.8.0.121-6.4
java-1_8_0-openjdk-demo-debuginfo-1.8.0.121-6.4

145739 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1028-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7392, CVE-2017-7393, CVE-2017-7394, CVE-2017-7395, CVE-2017-7396

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1028-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00057.html>

SuSE Linux 42.1

x86_64

xorg-x11-Xvnc-1.5.0-40.1

tigervnc-1.5.0-40.1

xorg-x11-Xvnc-debuginfo-1.5.0-40.1

tigervnc-debugsource-1.5.0-40.1

tigervnc-debuginfo-1.5.0-40.1

i586

xorg-x11-Xvnc-1.5.0-40.1

tigervnc-1.5.0-40.1

xorg-x11-Xvnc-debuginfo-1.5.0-40.1

tigervnc-debugsource-1.5.0-40.1

tigervnc-debuginfo-1.5.0-40.1

SuSE Linux 42.2

x86_64

libXvnc-devel-1.6.0-16.5.1

libXvnc1-debuginfo-1.6.0-16.5.1

tigervnc-1.6.0-16.5.1

xorg-x11-Xvnc-debuginfo-1.6.0-16.5.1

libXvnc1-1.6.0-16.5.1

tigervnc-debuginfo-1.6.0-16.5.1

xorg-x11-Xvnc-1.6.0-16.5.1

tigervnc-debugsource-1.6.0-16.5.1

i586

libXvnc-devel-1.6.0-16.5.1

libXvnc1-debuginfo-1.6.0-16.5.1

tigervnc-1.6.0-16.5.1

xorg-x11-Xvnc-debuginfo-1.6.0-16.5.1

libXvnc1-1.6.0-16.5.1

tigervnc-debuginfo-1.6.0-16.5.1

xorg-x11-Xvnc-1.6.0-16.5.1

tigervnc-debugsource-1.6.0-16.5.1

145745 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2289-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1531, CVE-2016-9963, CVE-2017-1000369

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2289-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00109.html>

SuSE Linux 42.2

x86_64

exim-debugsource-4.86.2-10.6.1

eximstats-html-4.86.2-10.6.1

exim-debuginfo-4.86.2-10.6.1

eximon-debuginfo-4.86.2-10.6.1

eximon-4.86.2-10.6.1

exim-4.86.2-10.6.1

SuSE Linux 42.3

x86_64

exim-debuginfo-4.86.2-14.1

exim-debugsource-4.86.2-14.1

eximon-4.86.2-14.1

exim-4.86.2-14.1

eximon-debuginfo-4.86.2-14.1

eximstats-html-4.86.2-14.1

145749 - SuSE Linux 42.2 openSUSE-SU-2017:1933-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000083

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1933-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00083.html>

SuSE Linux 42.2

x86_64

evince-plugin-pdfdocument-3.20.1-2.3.1

typelib-1_0-EvinceView-3_0-3.20.1-2.3.1

evince-3.20.1-2.3.1

libevview3-3-3.20.1-2.3.1

typelib-1_0-EvinceDocument-3_0-3.20.1-2.3.1

evince-devel-3.20.1-2.3.1

evince-plugin-tiffdocument-3.20.1-2.3.1

evince-browser-plugin-debuginfo-3.20.1-2.3.1

libevdocument3-4-3.20.1-2.3.1

evince-plugin-psdocument-3.20.1-2.3.1

evince-plugin-xpsdocument-debuginfo-3.20.1-2.3.1

evince-plugin-dvidocument-debuginfo-3.20.1-2.3.1

libevview3-3-debuginfo-3.20.1-2.3.1

evince-plugin-djvudocument-3.20.1-2.3.1

evince-plugin-djvudocument-debuginfo-3.20.1-2.3.1

evince-browser-plugin-3.20.1-2.3.1

evince-plugin-tiffdocument-debuginfo-3.20.1-2.3.1

nautilus-evincedb3.20.1-2.3.1
nautilus-evincedb3.20.1-2.3.1
evince-plugin-pdfdocument-debuginfo-3.20.1-2.3.1
evince-plugin-xpsdocument-3.20.1-2.3.1
evince-debugsource-3.20.1-2.3.1
evince-debuginfo-3.20.1-2.3.1
evince-plugin-comicsdocument-debuginfo-3.20.1-2.3.1
evince-plugin-comicsdocument-3.20.1-2.3.1
evince-plugin-psdocument-debuginfo-3.20.1-2.3.1
evince-plugin-dvidocument-3.20.1-2.3.1
libevdocument3-4-debuginfo-3.20.1-2.3.1

noarch
evince-lang-3.20.1-2.3.1

145751 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0023-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9848, CVE-2016-8707, CVE-2016-8866, CVE-2016-9556, CVE-2016-9559, CVE-2016-9773

Description

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

openSUSE-SU-2017:0023-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00012.html>

SuSE Linux 42.1

i586
libMagick++-6_Q16-3-6.8.8.1-27.1
ImageMagick-extra-6.8.8.1-27.1
libMagickWand-6_Q16-1-6.8.8.1-27.1
perl-PerlMagick-debuginfo-6.8.8.1-27.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-27.1
perl-PerlMagick-6.8.8.1-27.1
libMagickCore-6_Q16-1-6.8.8.1-27.1
ImageMagick-6.8.8.1-27.1
ImageMagick-debuginfo-6.8.8.1-27.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-27.1
libMagick++-devel-6.8.8.1-27.1
ImageMagick-extra-debuginfo-6.8.8.1-27.1
ImageMagick-devel-6.8.8.1-27.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-27.1
ImageMagick-debugsource-6.8.8.1-27.1

noarch
ImageMagick-doc-6.8.8.1-27.1

x86_64
libMagick++-6_Q16-3-6.8.8.1-27.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-27.1
ImageMagick-extra-6.8.8.1-27.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-27.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-27.1

libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-27.1
libMagickWand-6_Q16-1-6.8.8.1-27.1
perl-PerlMagick-debuginfo-6.8.8.1-27.1
libMagick++-6_Q16-3-32bit-6.8.8.1-27.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-27.1
perl-PerlMagick-6.8.8.1-27.1
libMagick++-devel-32bit-6.8.8.1-27.1
libMagickCore-6_Q16-1-6.8.8.1-27.1
ImageMagick-6.8.8.1-27.1
ImageMagick-debuginfo-6.8.8.1-27.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-27.1
libMagick++-devel-6.8.8.1-27.1
ImageMagick-extra-debuginfo-6.8.8.1-27.1
ImageMagick-devel-6.8.8.1-27.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-27.1
ImageMagick-debugsource-6.8.8.1-27.1
ImageMagick-devel-32bit-6.8.8.1-27.1
libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-27.1

SuSE Linux 42.2

i586

ImageMagick-6.8.8.1-25.1
ImageMagick-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-6.8.8.1-25.1
ImageMagick-devel-6.8.8.1-25.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-25.1
ImageMagick-debugsource-6.8.8.1-25.1
perl-PerlMagick-6.8.8.1-25.1
ImageMagick-extra-debuginfo-6.8.8.1-25.1
libMagick++-devel-6.8.8.1-25.1
ImageMagick-extra-6.8.8.1-25.1
libMagickWand-6_Q16-1-6.8.8.1-25.1
libMagick++-6_Q16-3-6.8.8.1-25.1
perl-PerlMagick-debuginfo-6.8.8.1-25.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-25.1

noarch

ImageMagick-doc-6.8.8.1-25.1

x86_64

libMagick++-devel-32bit-6.8.8.1-25.1
ImageMagick-6.8.8.1-25.1
libMagick++-6_Q16-3-32bit-6.8.8.1-25.1
ImageMagick-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-6.8.8.1-25.1
ImageMagick-devel-6.8.8.1-25.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-25.1
ImageMagick-debugsource-6.8.8.1-25.1
perl-PerlMagick-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-25.1
ImageMagick-extra-debuginfo-6.8.8.1-25.1
ImageMagick-devel-32bit-6.8.8.1-25.1
libMagick++-devel-6.8.8.1-25.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-25.1
ImageMagick-extra-6.8.8.1-25.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-25.1
libMagickWand-6_Q16-1-6.8.8.1-25.1
libMagick++-6_Q16-3-6.8.8.1-25.1

libMagick++-6_Q16-3-debuginfo-32bit-6.8.8.1-25.1
perl-PerlMagick-debuginfo-6.8.8.1-25.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-25.1

145754 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0552-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2399

Description

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

openSUSE-SU-2017:0552-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00102.html>

SuSE Linux 42.1

x86_64

libquicktime0-debuginfo-32bit-1.2.4cvs20150223-4.1
libquicktime0-32bit-1.2.4cvs20150223-4.1
libquicktime0-1.2.4cvs20150223-4.1
libquicktime0-debuginfo-1.2.4cvs20150223-4.1
libquicktime-debugsource-1.2.4cvs20150223-4.1
libquicktime-tools-1.2.4cvs20150223-4.1
libquicktime-tools-debuginfo-1.2.4cvs20150223-4.1
libquicktime-devel-1.2.4cvs20150223-4.1

i586

libquicktime0-1.2.4cvs20150223-4.1
libquicktime0-debuginfo-1.2.4cvs20150223-4.1
libquicktime-debugsource-1.2.4cvs20150223-4.1
libquicktime-tools-1.2.4cvs20150223-4.1
libquicktime-tools-debuginfo-1.2.4cvs20150223-4.1
libquicktime-devel-1.2.4cvs20150223-4.1

SuSE Linux 42.2

x86_64

libquicktime-devel-1.2.4cvs20150223-6.1
libquicktime0-1.2.4cvs20150223-6.1
libquicktime0-debuginfo-1.2.4cvs20150223-6.1
libquicktime-tools-1.2.4cvs20150223-6.1
libquicktime0-32bit-1.2.4cvs20150223-6.1
libquicktime-debugsource-1.2.4cvs20150223-6.1
libquicktime0-debuginfo-32bit-1.2.4cvs20150223-6.1
libquicktime-tools-debuginfo-1.2.4cvs20150223-6.1

i586

libquicktime-devel-1.2.4cvs20150223-6.1
libquicktime0-1.2.4cvs20150223-6.1
libquicktime0-debuginfo-1.2.4cvs20150223-6.1
libquicktime-tools-1.2.4cvs20150223-6.1
libquicktime-debugsource-1.2.4cvs20150223-6.1
libquicktime-tools-debuginfo-1.2.4cvs20150223-6.1

145762 - SuSE Linux 42.2 openSUSE-SU-2017:0199-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5219

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0199-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00112.html>

SuSE Linux 42.2

x86_64

v8-debugsource-5.3.332-3.1

libv8-5-5.3.332-3.1

v8-5.3.332-3.1

v8-devel-5.3.332-3.1

v8-debuginfo-5.3.332-3.1

v8-private-headers-devel-5.3.332-3.1

libv8-5-debuginfo-5.3.332-3.1

i586

v8-debugsource-5.3.332-3.1

libv8-5-5.3.332-3.1

v8-5.3.332-3.1

v8-devel-5.3.332-3.1

v8-debuginfo-5.3.332-3.1

v8-private-headers-devel-5.3.332-3.1

libv8-5-debuginfo-5.3.332-3.1

145766 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2056-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7511, CVE-2017-7515, CVE-2017-9406, CVE-2017-9408, CVE-2017-9775, CVE-2017-9776

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2056-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00015.html>

SuSE Linux 42.2

x86_64

libpoppler-qt5-devel-0.43.0-2.3.1

libpoppler-glib8-debuginfo-0.43.0-2.3.1

poppler-qt-debugsource-0.43.0-2.3.1
poppler-tools-0.43.0-2.3.1
libpoppler-glib8-32bit-0.43.0-2.3.1
poppler-qt5-debugsource-0.43.0-2.3.1
libpoppler-cpp0-32bit-0.43.0-2.3.1
libpoppler-qt4-4-debuginfo-0.43.0-2.3.1
libpoppler60-0.43.0-2.3.1
libpoppler60-32bit-0.43.0-2.3.1
libpoppler-qt5-1-0.43.0-2.3.1
libpoppler-qt4-4-32bit-0.43.0-2.3.1
libpoppler-glib-devel-0.43.0-2.3.1
libpoppler-qt5-1-32bit-0.43.0-2.3.1
libpoppler-qt4-devel-0.43.0-2.3.1
libpoppler-glib8-0.43.0-2.3.1
libpoppler-cpp0-debuginfo-0.43.0-2.3.1
libpoppler-cpp0-debuginfo-32bit-0.43.0-2.3.1
libpoppler-glib8-debuginfo-32bit-0.43.0-2.3.1
libpoppler-qt5-1-debuginfo-0.43.0-2.3.1
libpoppler-qt4-4-0.43.0-2.3.1
libpoppler-qt5-1-debuginfo-32bit-0.43.0-2.3.1
typelib-1_0-Poppler-0_18-0.43.0-2.3.1
poppler-tools-debuginfo-0.43.0-2.3.1
libpoppler60-debuginfo-0.43.0-2.3.1
libpoppler-qt4-4-debuginfo-32bit-0.43.0-2.3.1
libpoppler60-debuginfo-32bit-0.43.0-2.3.1
poppler-debugsource-0.43.0-2.3.1
libpoppler-cpp0-0.43.0-2.3.1
libpoppler-devel-0.43.0-2.3.1

i586

poppler-qt-debugsource-0.43.0-2.3.1
libpoppler-qt4-4-0.43.0-2.3.1
libpoppler-glib-devel-0.43.0-2.3.1
libpoppler60-debuginfo-0.43.0-2.3.1
libpoppler-qt4-4-debuginfo-0.43.0-2.3.1
libpoppler-qt5-devel-0.43.0-2.3.1
libpoppler-qt5-1-debuginfo-0.43.0-2.3.1
libpoppler-glib8-debuginfo-0.43.0-2.3.1
libpoppler-cpp0-debuginfo-0.43.0-2.3.1
libpoppler-cpp0-0.43.0-2.3.1
poppler-qt5-debugsource-0.43.0-2.3.1
libpoppler-qt4-devel-0.43.0-2.3.1
poppler-tools-debuginfo-0.43.0-2.3.1
libpoppler-qt5-1-0.43.0-2.3.1
poppler-tools-0.43.0-2.3.1
libpoppler60-0.43.0-2.3.1
libpoppler-glib8-0.43.0-2.3.1
libpoppler-devel-0.43.0-2.3.1
typelib-1_0-Poppler-0_18-0.43.0-2.3.1
poppler-debugsource-0.43.0-2.3.1

SuSE Linux 42.3

x86_64

libpoppler60-32bit-0.43.0-5.1
libpoppler-qt4-4-debuginfo-0.43.0-5.1
libpoppler-qt4-4-32bit-0.43.0-5.1
libpoppler-cpp0-32bit-0.43.0-5.1
libpoppler-qt5-1-debuginfo-0.43.0-5.1
libpoppler-qt4-devel-0.43.0-5.1
libpoppler-qt5-1-debuginfo-32bit-0.43.0-5.1

libpoppler-glib8-debuginfo-32bit-0.43.0-5.1
libpoppler60-debuginfo-32bit-0.43.0-5.1
libpoppler-devel-0.43.0-5.1
libpoppler-cpp0-0.43.0-5.1
libpoppler-qt5-devel-0.43.0-5.1
poppler-tools-debuginfo-0.43.0-5.1
libpoppler-glib8-0.43.0-5.1
libpoppler60-debuginfo-0.43.0-5.1
libpoppler-glib8-32bit-0.43.0-5.1
poppler-tools-0.43.0-5.1
libpoppler-glib8-debuginfo-0.43.0-5.1
libpoppler-qt5-1-32bit-0.43.0-5.1
poppler-qt-debugsource-0.43.0-5.1
libpoppler60-0.43.0-5.1
poppler-debugsource-0.43.0-5.1
libpoppler-qt4-4-debuginfo-32bit-0.43.0-5.1
libpoppler-cpp0-debuginfo-32bit-0.43.0-5.1
libpoppler-cpp0-debuginfo-0.43.0-5.1
poppler-qt5-debugsource-0.43.0-5.1
libpoppler-glib-devel-0.43.0-5.1
libpoppler-qt5-1-0.43.0-5.1
libpoppler-qt4-4-0.43.0-5.1
typelib-1_0-Poppler-0_18-0.43.0-5.1

i586

poppler-debugsource-0.43.0-5.1
poppler-tools-0.43.0-5.1
libpoppler-glib8-debuginfo-0.43.0-5.1
libpoppler-qt4-devel-0.43.0-5.1
libpoppler-glib8-0.43.0-5.1
libpoppler-qt5-1-0.43.0-5.1
libpoppler-cpp0-debuginfo-0.43.0-5.1
libpoppler-glib-devel-0.43.0-5.1
libpoppler60-debuginfo-0.43.0-5.1
libpoppler-cpp0-0.43.0-5.1
libpoppler-qt4-4-0.43.0-5.1
libpoppler-qt5-1-debuginfo-0.43.0-5.1
libpoppler60-0.43.0-5.1
poppler-qt5-debugsource-0.43.0-5.1
poppler-qt-debugsource-0.43.0-5.1
libpoppler-devel-0.43.0-5.1
typelib-1_0-Poppler-0_18-0.43.0-5.1
libpoppler-qt5-devel-0.43.0-5.1
poppler-tools-debuginfo-0.43.0-5.1
libpoppler-qt4-4-debuginfo-0.43.0-5.1

145768 - SuSE Linux 42.2 openSUSE-SU-2017:1426-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5209, CVE-2017-5545, CVE-2017-5834, CVE-2017-5835, CVE-2017-5836, CVE-2017-6440, CVE-2017-7982

Description

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

openSUSE-SU-2017:1426-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00094.html>

SuSE Linux 42.2

x86_64

libplist3-debuginfo-1.12-7.3.1

plistutil-1.12-7.3.1

libplist++-devel-1.12-7.3.1

python-plist-1.12-7.3.1

python-plist-debuginfo-1.12-7.3.1

libplist-devel-1.12-7.3.1

libplist3-32bit-1.12-7.3.1

libplist++3-32bit-1.12-7.3.1

libplist++3-debuginfo-32bit-1.12-7.3.1

libplist++3-1.12-7.3.1

libplist-debugsource-1.12-7.3.1

libplist3-debuginfo-32bit-1.12-7.3.1

libplist3-1.12-7.3.1

plistutil-debuginfo-1.12-7.3.1

libplist++3-debuginfo-1.12-7.3.1

i586

libplist++-devel-1.12-7.3.1

plistutil-1.12-7.3.1

libplist++3-1.12-7.3.1

plistutil-debuginfo-1.12-7.3.1

python-plist-1.12-7.3.1

libplist-debugsource-1.12-7.3.1

libplist-devel-1.12-7.3.1

libplist3-debuginfo-1.12-7.3.1

libplist++3-debuginfo-1.12-7.3.1

python-plist-debuginfo-1.12-7.3.1

libplist3-1.12-7.3.1

145776 - SuSE Linux 42.2 openSUSE-SU-2017:0982-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8994

Description

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

openSUSE-SU-2017:0982-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00041.html>

SuSE Linux 42.2

i586

php7-pspell-debuginfo-7.0.7-14.3.1

php7-tidy-7.0.7-14.3.1

php7-sockets-7.0.7-14.3.1

php7-soap-7.0.7-14.3.1

php7-odbc-debuginfo-7.0.7-14.3.1

php7-shmop-debuginfo-7.0.7-14.3.1
php7-bz2-7.0.7-14.3.1
php7-sysvsem-7.0.7-14.3.1
php7-pcntl-debuginfo-7.0.7-14.3.1
php7-mcrypt-debuginfo-7.0.7-14.3.1
php7-ftp-debuginfo-7.0.7-14.3.1
php7-sqlite-7.0.7-14.3.1
php7-imap-7.0.7-14.3.1
php7-opcache-debuginfo-7.0.7-14.3.1
php7-odbc-7.0.7-14.3.1
php7-bcmath-7.0.7-14.3.1
php7-wddx-7.0.7-14.3.1
php7-openssl-7.0.7-14.3.1
php7-xmlreader-7.0.7-14.3.1
php7-sysvmsg-debuginfo-7.0.7-14.3.1
php7-7.0.7-14.3.1
php7-firebird-7.0.7-14.3.1
php7-phar-7.0.7-14.3.1
php7-wddx-debuginfo-7.0.7-14.3.1
php7-bz2-debuginfo-7.0.7-14.3.1
php7-shmop-7.0.7-14.3.1
php7-zip-7.0.7-14.3.1
php7-xmlwriter-debuginfo-7.0.7-14.3.1
php7-zlib-7.0.7-14.3.1
php7-calendar-debuginfo-7.0.7-14.3.1
php7-xmlreader-debuginfo-7.0.7-14.3.1
php7-bcmath-debuginfo-7.0.7-14.3.1
php7-gettext-7.0.7-14.3.1
php7-ctype-7.0.7-14.3.1
php7-iconv-7.0.7-14.3.1
php7-sysvshm-debuginfo-7.0.7-14.3.1
php7-opcache-7.0.7-14.3.1
php7-xsl-debuginfo-7.0.7-14.3.1
php7-zip-debuginfo-7.0.7-14.3.1
php7-sqlite-debuginfo-7.0.7-14.3.1
php7-exif-7.0.7-14.3.1
php7-phar-debuginfo-7.0.7-14.3.1
php7-ldap-7.0.7-14.3.1
php7-curl-debuginfo-7.0.7-14.3.1
php7-dba-debuginfo-7.0.7-14.3.1
php7-intl-debuginfo-7.0.7-14.3.1
php7-pcntl-7.0.7-14.3.1
apache2-mod_php7-debuginfo-7.0.7-14.3.1
php7-curl-7.0.7-14.3.1
php7-fastcgi-7.0.7-14.3.1
php7-gmp-debuginfo-7.0.7-14.3.1
php7-pgsql-7.0.7-14.3.1
php7-enchanted-debuginfo-7.0.7-14.3.1
php7-fileinfo-debuginfo-7.0.7-14.3.1
php7-fpm-debuginfo-7.0.7-14.3.1
php7-pspell-7.0.7-14.3.1
php7-gd-7.0.7-14.3.1
php7-soap-debuginfo-7.0.7-14.3.1
php7-sockets-debuginfo-7.0.7-14.3.1
php7-pdo-7.0.7-14.3.1
php7-openssl-debuginfo-7.0.7-14.3.1
php7-exif-debuginfo-7.0.7-14.3.1
php7-mbstring-debuginfo-7.0.7-14.3.1
php7-mysql-7.0.7-14.3.1
php7-xmlwriter-7.0.7-14.3.1

php7-xmlrpc-7.0.7-14.3.1
php7-tidy-debuginfo-7.0.7-14.3.1
php7-snmp-7.0.7-14.3.1
php7-fastcgi-debuginfo-7.0.7-14.3.1
php7-tokenizer-7.0.7-14.3.1
php7-pgsql-debuginfo-7.0.7-14.3.1
php7-snmp-debuginfo-7.0.7-14.3.1
php7-ldap-debuginfo-7.0.7-14.3.1
php7-json-debuginfo-7.0.7-14.3.1
php7-sysvshm-7.0.7-14.3.1
php7-xsl-7.0.7-14.3.1
php7-gd-debuginfo-7.0.7-14.3.1
php7-mysql-debuginfo-7.0.7-14.3.1
php7-intl-7.0.7-14.3.1
php7-fileinfo-7.0.7-14.3.1
php7-calendar-7.0.7-14.3.1
php7-dba-7.0.7-14.3.1
php7-readline-7.0.7-14.3.1
php7-pdo-debuginfo-7.0.7-14.3.1
php7-iconv-debuginfo-7.0.7-14.3.1
php7-devel-7.0.7-14.3.1
php7-readline-debuginfo-7.0.7-14.3.1
php7-dom-7.0.7-14.3.1
php7-debugsource-7.0.7-14.3.1
php7-fpm-7.0.7-14.3.1
php7-json-7.0.7-14.3.1
php7-posix-debuginfo-7.0.7-14.3.1
apache2-mod_php7-7.0.7-14.3.1
php7-gmp-7.0.7-14.3.1
php7-ftp-7.0.7-14.3.1
php7-sysvmsg-7.0.7-14.3.1
php7-tokenizer-debuginfo-7.0.7-14.3.1
php7-mcrypt-7.0.7-14.3.1
php7-gettext-debuginfo-7.0.7-14.3.1
php7-sysvsem-debuginfo-7.0.7-14.3.1
php7-posix-7.0.7-14.3.1
php7-xmlrpc-debuginfo-7.0.7-14.3.1
php7-enchanted-7.0.7-14.3.1
php7-ctype-debuginfo-7.0.7-14.3.1
php7-debuginfo-7.0.7-14.3.1
php7-dom-debuginfo-7.0.7-14.3.1
php7-mbstring-7.0.7-14.3.1
php7-zlib-debuginfo-7.0.7-14.3.1
php7-firebird-debuginfo-7.0.7-14.3.1

noarch

php7-pear-7.0.7-14.3.1
php7-pear-Archive_Tar-7.0.7-14.3.1

x86_64

php7-pspell-debuginfo-7.0.7-14.3.1
php7-tidy-7.0.7-14.3.1
php7-sockets-7.0.7-14.3.1
php7-soap-7.0.7-14.3.1
php7-odbc-debuginfo-7.0.7-14.3.1
php7-shmop-debuginfo-7.0.7-14.3.1
php7-bz2-7.0.7-14.3.1
php7-sysvsem-7.0.7-14.3.1
php7-pcntl-debuginfo-7.0.7-14.3.1

php7-mcrypt-debuginfo-7.0.7-14.3.1
php7-ftp-debuginfo-7.0.7-14.3.1
php7-sqlite-7.0.7-14.3.1
php7-imap-7.0.7-14.3.1
php7-opcache-debuginfo-7.0.7-14.3.1
php7-odbc-7.0.7-14.3.1
php7-bcmath-7.0.7-14.3.1
php7-wddx-7.0.7-14.3.1
php7-openssl-7.0.7-14.3.1
php7-xmlreader-7.0.7-14.3.1
php7-sysvmsg-debuginfo-7.0.7-14.3.1
php7-7.0.7-14.3.1
php7-firebird-7.0.7-14.3.1
php7-phar-7.0.7-14.3.1
php7-wddx-debuginfo-7.0.7-14.3.1
php7-bz2-debuginfo-7.0.7-14.3.1
php7-shmop-7.0.7-14.3.1
php7-zip-7.0.7-14.3.1
php7-xmlwriter-debuginfo-7.0.7-14.3.1
php7-zlib-7.0.7-14.3.1
php7-calendar-debuginfo-7.0.7-14.3.1
php7-xmlreader-debuginfo-7.0.7-14.3.1
php7-bcmath-debuginfo-7.0.7-14.3.1
php7-gettext-7.0.7-14.3.1
php7-ctype-7.0.7-14.3.1
php7-iconv-7.0.7-14.3.1
php7-sysvshm-debuginfo-7.0.7-14.3.1
php7-opcache-7.0.7-14.3.1
php7-xsl-debuginfo-7.0.7-14.3.1
php7-zip-debuginfo-7.0.7-14.3.1
php7-sqlite-debuginfo-7.0.7-14.3.1
php7-exif-7.0.7-14.3.1
php7-phar-debuginfo-7.0.7-14.3.1
php7-ldap-7.0.7-14.3.1
php7-curl-debuginfo-7.0.7-14.3.1
php7-dba-debuginfo-7.0.7-14.3.1
php7-intl-debuginfo-7.0.7-14.3.1
php7-pcntl-7.0.7-14.3.1
apache2-mod_php7-debuginfo-7.0.7-14.3.1
php7-curl-7.0.7-14.3.1
php7-fastcgi-7.0.7-14.3.1
php7-gmp-debuginfo-7.0.7-14.3.1
php7-pgsql-7.0.7-14.3.1
php7-enchanted-debuginfo-7.0.7-14.3.1
php7-fileinfo-debuginfo-7.0.7-14.3.1
php7-fpm-debuginfo-7.0.7-14.3.1
php7-pspell-7.0.7-14.3.1
php7-gd-7.0.7-14.3.1
php7-soap-debuginfo-7.0.7-14.3.1
php7-sockets-debuginfo-7.0.7-14.3.1
php7-pdo-7.0.7-14.3.1
php7-openssl-debuginfo-7.0.7-14.3.1
php7-exif-debuginfo-7.0.7-14.3.1
php7-mbstring-debuginfo-7.0.7-14.3.1
php7-mysql-7.0.7-14.3.1
php7-xmlwriter-7.0.7-14.3.1
php7-xmlrpc-7.0.7-14.3.1
php7-tidy-debuginfo-7.0.7-14.3.1
php7-snmp-7.0.7-14.3.1
php7-fastcgi-debuginfo-7.0.7-14.3.1

php7-tokenizer-7.0.7-14.3.1
php7-pgsql-debuginfo-7.0.7-14.3.1
php7-snmp-debuginfo-7.0.7-14.3.1
php7-imap-debuginfo-7.0.7-14.3.1
php7-ldap-debuginfo-7.0.7-14.3.1
php7-json-debuginfo-7.0.7-14.3.1
php7-sysvshm-7.0.7-14.3.1
php7-xsl-7.0.7-14.3.1
php7-gd-debuginfo-7.0.7-14.3.1
php7-mysql-debuginfo-7.0.7-14.3.1
php7-intl-7.0.7-14.3.1
php7-fileinfo-7.0.7-14.3.1
php7-calendar-7.0.7-14.3.1
php7-dba-7.0.7-14.3.1
php7-readline-7.0.7-14.3.1
php7-pdo-debuginfo-7.0.7-14.3.1
php7-iconv-debuginfo-7.0.7-14.3.1
php7-devel-7.0.7-14.3.1
php7-readline-debuginfo-7.0.7-14.3.1
php7-dom-7.0.7-14.3.1
php7-debugsource-7.0.7-14.3.1
php7-fpm-7.0.7-14.3.1
php7-json-7.0.7-14.3.1
php7-posix-debuginfo-7.0.7-14.3.1
apache2-mod_php7-7.0.7-14.3.1
php7-gmp-7.0.7-14.3.1
php7-ftp-7.0.7-14.3.1
php7-sysvmsg-7.0.7-14.3.1
php7-tokenizer-debuginfo-7.0.7-14.3.1
php7-mcrypt-7.0.7-14.3.1
php7-gettext-debuginfo-7.0.7-14.3.1
php7-sysvsem-debuginfo-7.0.7-14.3.1
php7-posix-7.0.7-14.3.1
php7-xmlrpc-debuginfo-7.0.7-14.3.1
php7-enchanted-7.0.7-14.3.1
php7-ctype-debuginfo-7.0.7-14.3.1
php7-debuginfo-7.0.7-14.3.1
php7-dom-debuginfo-7.0.7-14.3.1
php7-mbstring-7.0.7-14.3.1
php7-zlib-debuginfo-7.0.7-14.3.1
php7-firebird-debuginfo-7.0.7-14.3.1

145778 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2190-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8872

Description

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

openSUSE-SU-2017:2190-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00067.html>

SuSE Linux 42.2

i586

libxml2-debugsource-2.9.4-5.17.1

libxml2-2-2.9.4-5.17.1

libxml2-devel-2.9.4-5.17.1

libxml2-tools-2.9.4-5.17.1

python-libxml2-debuginfo-2.9.4-5.17.1

libxml2-tools-debuginfo-2.9.4-5.17.1

python-libxml2-debugsource-2.9.4-5.17.1

python-libxml2-2.9.4-5.17.1

libxml2-2-debuginfo-2.9.4-5.17.1

noarch

libxml2-doc-2.9.4-5.17.1

x86_64

libxml2-debugsource-2.9.4-5.17.1

libxml2-2-debuginfo-32bit-2.9.4-5.17.1

libxml2-2-2.9.4-5.17.1

libxml2-devel-2.9.4-5.17.1

libxml2-2-32bit-2.9.4-5.17.1

libxml2-tools-2.9.4-5.17.1

libxml2-devel-32bit-2.9.4-5.17.1

python-libxml2-debuginfo-2.9.4-5.17.1

libxml2-tools-debuginfo-2.9.4-5.17.1

python-libxml2-debugsource-2.9.4-5.17.1

python-libxml2-2.9.4-5.17.1

libxml2-2-debuginfo-2.9.4-5.17.1

SuSE Linux 42.3

i586

libxml2-2-debuginfo-2.9.4-12.1

libxml2-tools-debuginfo-2.9.4-12.1

libxml2-tools-2.9.4-12.1

libxml2-devel-2.9.4-12.1

python-libxml2-debugsource-2.9.4-12.1

python-libxml2-debuginfo-2.9.4-12.1

libxml2-debugsource-2.9.4-12.1

libxml2-2-2.9.4-12.1

python-libxml2-2.9.4-12.1

noarch

libxml2-doc-2.9.4-12.1

x86_64

libxml2-2-debuginfo-2.9.4-12.1

libxml2-tools-debuginfo-2.9.4-12.1

libxml2-devel-32bit-2.9.4-12.1

libxml2-2-debuginfo-32bit-2.9.4-12.1

libxml2-tools-2.9.4-12.1

libxml2-devel-2.9.4-12.1

python-libxml2-debugsource-2.9.4-12.1

python-libxml2-debuginfo-2.9.4-12.1

libxml2-debugsource-2.9.4-12.1

libxml2-2-2.9.4-12.1

libxml2-2-32bit-2.9.4-12.1

python-libxml2-2.9.4-12.1

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

Risk Level: Medium

CVE: CVE-2017-5627, CVE-2017-5628, CVE-2017-5896

Description

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

openSUSE-SU-2017:0504-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00084.html>

SuSE Linux 42.1

x86_64

mupdf-1.10a-15.1

mupdf-devel-static-1.10a-15.1

i586

mupdf-1.10a-15.1

mupdf-devel-static-1.10a-15.1

SuSE Linux 42.2

x86_64

mupdf-1.10a-11.2

mupdf-devel-static-1.10a-11.2

i586

mupdf-1.10a-11.2

mupdf-devel-static-1.10a-11.2

145786 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0790-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2784

Description

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

openSUSE-SU-2017:0790-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00072.html>

SuSE Linux 42.1

x86_64

libmbedtls9-debuginfo-32bit-1.3.19-15.1

mbedtls9-debugsource-1.3.19-15.1

libmbedtls9-debuginfo-1.3.19-15.1

mbedtls9-devel-1.3.19-15.1

libmbedtls9-1.3.19-15.1

libmbedtls9-32bit-1.3.19-15.1

i586
mbedtls-debugsource-1.3.19-15.1
libmbedtls9-debuginfo-1.3.19-15.1
libmbedtls9-1.3.19-15.1
mbedtls-devel-1.3.19-15.1

SuSE Linux 42.2
x86_64
libmbedtls9-debuginfo-32bit-1.3.19-15.1
mbedtls-debugsource-1.3.19-15.1
libmbedtls9-debuginfo-1.3.19-15.1
mbedtls-devel-1.3.19-15.1
libmbedtls9-1.3.19-15.1
libmbedtls9-32bit-1.3.19-15.1

i586
mbedtls-debugsource-1.3.19-15.1
libmbedtls9-debuginfo-1.3.19-15.1
libmbedtls9-1.3.19-15.1
mbedtls-devel-1.3.19-15.1

145787 - SuSE Linux 42.2 openSUSE-SU-2017:1422-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8386

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1422-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00090.html>

SuSE Linux 42.2
x86_64
git-daemon-2.12.3-5.6.1
git-credential-gnome-keyring-debuginfo-2.12.3-5.6.1
git-debugsource-2.12.3-5.6.1
git-daemon-debuginfo-2.12.3-5.6.1
git-svn-debuginfo-2.12.3-5.6.1
gitk-2.12.3-5.6.1
git-email-2.12.3-5.6.1
git-credential-gnome-keyring-2.12.3-5.6.1
git-arch-2.12.3-5.6.1
git-web-2.12.3-5.6.1
git-core-debuginfo-2.12.3-5.6.1
git-svn-2.12.3-5.6.1
git-2.12.3-5.6.1
git-core-2.12.3-5.6.1
git-cvs-2.12.3-5.6.1
git-gui-2.12.3-5.6.1

noarch
git-doc-2.12.3-5.6.1

145796 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0140-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5330

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0140-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00073.html>

SuSE Linux 42.1

x86_64

libkerfuffle15-debuginfo-15.12.3-18.1

ark-15.12.3-18.1

libkerfuffle15-15.12.3-18.1

ark-debugsource-15.12.3-18.1

ark-debuginfo-15.12.3-18.1

i586

libkerfuffle15-debuginfo-15.12.3-18.1

ark-15.12.3-18.1

libkerfuffle15-15.12.3-18.1

ark-debugsource-15.12.3-18.1

ark-debuginfo-15.12.3-18.1

SuSE Linux 42.2

x86_64

libkerfuffle16-debuginfo-16.08.2-3.1

ark-16.08.2-3.1

libkerfuffle16-16.08.2-3.1

ark-debugsource-16.08.2-3.1

ark-debuginfo-16.08.2-3.1

i586

libkerfuffle16-debuginfo-16.08.2-3.1

ark-16.08.2-3.1

libkerfuffle16-16.08.2-3.1

ark-debugsource-16.08.2-3.1

ark-debuginfo-16.08.2-3.1

145809 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2002-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5824, CVE-2016-5827, CVE-2016-9584

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2002-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00108.html>

SuSE Linux 42.2

i586
libical-devel-static-1.0.1-13.3.1
libical-debugsource-1.0.1-13.3.1
libical-devel-1.0.1-13.3.1
libical1-debuginfo-1.0.1-13.3.1
libical1-1.0.1-13.3.1

noarch
libical-doc-1.0.1-13.3.1

x86_64

libical1-debuginfo-1.0.1-13.3.1
libical1-32bit-1.0.1-13.3.1
libical-debugsource-1.0.1-13.3.1
libical1-1.0.1-13.3.1
libical1-debuginfo-32bit-1.0.1-13.3.1
libical-devel-1.0.1-13.3.1
libical-devel-static-1.0.1-13.3.1

SuSE Linux 42.3

i586
libical1-1.0.1-16.1
libical1-debuginfo-1.0.1-16.1
libical-devel-static-1.0.1-16.1
libical-debugsource-1.0.1-16.1
libical-devel-1.0.1-16.1

noarch
libical-doc-1.0.1-16.1

x86_64

libical1-debuginfo-32bit-1.0.1-16.1
libical-debugsource-1.0.1-16.1
libical1-1.0.1-16.1
libical1-32bit-1.0.1-16.1
libical-devel-static-1.0.1-16.1
libical1-debuginfo-1.0.1-16.1
libical-devel-1.0.1-16.1

145828 - SuSE Linux 42.2 openSUSE-SU-2017:0819-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6429

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0819-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00084.html>

SuSE Linux 42.2
x86_64
tcpreplay-debugsource-4.1.2-5.3.1
tcpreplay-debuginfo-4.1.2-5.3.1
tcpreplay-4.1.2-5.3.1

145832 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0486-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3312, CVE-2017-3317, CVE-2017-3318

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0486-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00074.html>

SuSE Linux 42.1
x86_64
libmysqlclient18-debuginfo-10.0.29-18.1
libmysqlclient18-32bit-10.0.29-18.1
mariadb-test-debuginfo-10.0.29-18.1
mariadb-errormessages-10.0.29-18.1
mariadb-10.0.29-18.1
libmysqlclient_r18-32bit-10.0.29-18.1
mariadb-debuginfo-10.0.29-18.1
mariadb-bench-debuginfo-10.0.29-18.1
mariadb-tools-debuginfo-10.0.29-18.1
mariadb-debugsource-10.0.29-18.1
mariadb-client-debuginfo-10.0.29-18.1
libmysqld18-10.0.29-18.1
mariadb-bench-10.0.29-18.1
mariadb-client-10.0.29-18.1
libmysqlclient18-debuginfo-32bit-10.0.29-18.1
libmysqld-devel-10.0.29-18.1
mariadb-tools-10.0.29-18.1
libmysqlclient18-10.0.29-18.1
libmysqld18-debuginfo-10.0.29-18.1
libmysqlclient_r18-10.0.29-18.1
mariadb-test-10.0.29-18.1
libmysqlclient-devel-10.0.29-18.1

i586
libmysqlclient18-debuginfo-10.0.29-18.1
mariadb-test-debuginfo-10.0.29-18.1
mariadb-errormessages-10.0.29-18.1
mariadb-10.0.29-18.1

mariadb-debuginfo-10.0.29-18.1
mariadb-bench-debuginfo-10.0.29-18.1
mariadb-tools-debuginfo-10.0.29-18.1
mariadb-debugsource-10.0.29-18.1
mariadb-client-debuginfo-10.0.29-18.1
libmysqld18-10.0.29-18.1
mariadb-bench-10.0.29-18.1
mariadb-client-10.0.29-18.1
libmysqld-devel-10.0.29-18.1
mariadb-tools-10.0.29-18.1
libmysqlclient18-10.0.29-18.1
libmysqld18-debuginfo-10.0.29-18.1
libmysqlclient_r18-10.0.29-18.1
mariadb-test-10.0.29-18.1
libmysqlclient-devel-10.0.29-18.1

SuSE Linux 42.2

x86_64

libmysqlclient18-debuginfo-10.0.29-18.1
libmysqlclient18-32bit-10.0.29-18.1
mariadb-test-debuginfo-10.0.29-18.1
mariadb-errormessages-10.0.29-18.1
mariadb-10.0.29-18.1
libmysqlclient_r18-32bit-10.0.29-18.1
mariadb-debuginfo-10.0.29-18.1
mariadb-bench-debuginfo-10.0.29-18.1
mariadb-tools-debuginfo-10.0.29-18.1
mariadb-debugsource-10.0.29-18.1
mariadb-client-debuginfo-10.0.29-18.1
libmysqld18-10.0.29-18.1
mariadb-bench-10.0.29-18.1
mariadb-client-10.0.29-18.1
libmysqlclient18-debuginfo-32bit-10.0.29-18.1
libmysqld-devel-10.0.29-18.1
mariadb-tools-10.0.29-18.1
libmysqlclient18-10.0.29-18.1
libmysqld18-debuginfo-10.0.29-18.1
libmysqlclient_r18-10.0.29-18.1
mariadb-test-10.0.29-18.1
libmysqlclient-devel-10.0.29-18.1

i586

libmysqlclient18-debuginfo-10.0.29-18.1
mariadb-test-debuginfo-10.0.29-18.1
mariadb-errormessages-10.0.29-18.1
mariadb-10.0.29-18.1
mariadb-debuginfo-10.0.29-18.1
mariadb-bench-debuginfo-10.0.29-18.1
mariadb-tools-debuginfo-10.0.29-18.1
mariadb-debugsource-10.0.29-18.1
mariadb-client-debuginfo-10.0.29-18.1
libmysqld18-10.0.29-18.1
mariadb-bench-10.0.29-18.1
mariadb-client-10.0.29-18.1
libmysqld-devel-10.0.29-18.1
mariadb-tools-10.0.29-18.1
libmysqlclient18-10.0.29-18.1
libmysqld18-debuginfo-10.0.29-18.1
libmysqlclient_r18-10.0.29-18.1
mariadb-test-10.0.29-18.1

145835 - SuSE Linux 42.2 openSUSE-SU-2017:0075-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9445, CVE-2016-9446, CVE-2016-9447

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0075-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00048.html>

SuSE Linux 42.2

i586

libgstcodecparsers-0_10-23-debuginfo-0.10.23-24.1
gstreamer-0_10-plugins-bad-0.10.23-24.1
libgstvdp-0_10-23-debuginfo-0.10.23-24.1
libgstbasevideo-0_10-23-debuginfo-0.10.23-24.1
libgstbasecamerabinsrc-0_10-23-debuginfo-0.10.23-24.1
libgstcodecparsers-0_10-23-0.10.23-24.1
gstreamer-0_10-plugins-bad-doc-0.10.23-24.1
gstreamer-0_10-plugins-bad-debuginfo-0.10.23-24.1
libgstbasevideo-0_10-23-0.10.23-24.1
libgstsignalprocessor-0_10-23-debuginfo-0.10.23-24.1
libgstsignalprocessor-0_10-23-0.10.23-24.1
libgstbasecamerabinsrc-0_10-23-0.10.23-24.1
libgstphotography-0_10-23-debuginfo-0.10.23-24.1
gstreamer-0_10-plugins-bad-devel-0.10.23-24.1
libgstvdp-0_10-23-0.10.23-24.1
libgstphotography-0_10-23-0.10.23-24.1
gstreamer-0_10-plugins-bad-debugsource-0.10.23-24.1

noarch

gstreamer-0_10-plugins-bad-lang-0.10.23-24.1

x86_64

gstreamer-0_10-plugins-bad-0.10.23-24.1
libgstvdp-0_10-23-32bit-0.10.23-24.1
libgstbasecamerabinsrc-0_10-23-debuginfo-32bit-0.10.23-24.1
gstreamer-0_10-plugins-bad-debuginfo-0.10.23-24.1
libgstphotography-0_10-23-debuginfo-32bit-0.10.23-24.1
libgstsignalprocessor-0_10-23-debuginfo-0.10.23-24.1
libgstbasevideo-0_10-23-debuginfo-0.10.23-24.1
libgstbasecamerabinsrc-0_10-23-debuginfo-0.10.23-24.1
libgstcodecparsers-0_10-23-0.10.23-24.1
libgstcodecparsers-0_10-23-32bit-0.10.23-24.1
gstreamer-0_10-plugins-bad-doc-0.10.23-24.1
libgstbasevideo-0_10-23-debuginfo-32bit-0.10.23-24.1
libgstbasevideo-0_10-23-0.10.23-24.1
libgstsignalprocessor-0_10-23-32bit-0.10.23-24.1
libgstsignalprocessor-0_10-23-debuginfo-32bit-0.10.23-24.1
libgstphotography-0_10-23-debuginfo-0.10.23-24.1

gststreamer-0_10-plugins-bad-devel-0.10.23-24.1
gststreamer-0_10-plugins-bad-debuginfo-32bit-0.10.23-24.1
libgstbasecamerabinsrc-0_10-23-0.10.23-24.1
libgstbasevideo-0_10-23-32bit-0.10.23-24.1
libgstcodecparsers-0_10-23-debuginfo-32bit-0.10.23-24.1
libgstphotography-0_10-23-32bit-0.10.23-24.1
gststreamer-0_10-plugins-bad-32bit-0.10.23-24.1
libgstsignalprocessor-0_10-23-0.10.23-24.1
libgstvdp-0_10-23-debuginfo-0.10.23-24.1
libgstvdp-0_10-23-0.10.23-24.1
libgstphotography-0_10-23-0.10.23-24.1
gststreamer-0_10-plugins-bad-debugsource-0.10.23-24.1
libgstbasecamerabinsrc-0_10-23-32bit-0.10.23-24.1
libgstcodecparsers-0_10-23-debuginfo-0.10.23-24.1
libgstvdp-0_10-23-debuginfo-32bit-0.10.23-24.1

145839 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1203-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10220, CVE-2016-9601, CVE-2017-5951, CVE-2017-7207, CVE-2017-8291

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1203-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00022.html>

SuSE Linux 42.1

x86_64

ghostscript-mini-debuginfo-9.15-17.1
ghostscript-debuginfo-9.15-17.1
ghostscript-mini-devel-9.15-17.1
ghostscript-devel-9.15-17.1
ghostscript-mini-debugsource-9.15-17.1
ghostscript-x11-debuginfo-9.15-17.1
ghostscript-debugsource-9.15-17.1
ghostscript-mini-9.15-17.1
ghostscript-x11-9.15-17.1
ghostscript-9.15-17.1

i586

ghostscript-mini-debuginfo-9.15-17.1
ghostscript-debuginfo-9.15-17.1
ghostscript-mini-devel-9.15-17.1
ghostscript-devel-9.15-17.1
ghostscript-mini-debugsource-9.15-17.1
ghostscript-x11-debuginfo-9.15-17.1
ghostscript-debugsource-9.15-17.1
ghostscript-mini-9.15-17.1
ghostscript-x11-9.15-17.1
ghostscript-9.15-17.1

SuSE Linux 42.2

x86_64
ghostscript-mini-debugsource-9.15-11.3.1
ghostscript-debuginfo-9.15-11.3.1
ghostscript-devel-9.15-11.3.1
ghostscript-mini-devel-9.15-11.3.1
ghostscript-mini-debuginfo-9.15-11.3.1
ghostscript-debugsource-9.15-11.3.1
ghostscript-9.15-11.3.1
ghostscript-mini-9.15-11.3.1
ghostscript-x11-debuginfo-9.15-11.3.1
ghostscript-x11-9.15-11.3.1

i586
ghostscript-mini-debugsource-9.15-11.3.1
ghostscript-debuginfo-9.15-11.3.1
ghostscript-devel-9.15-11.3.1
ghostscript-mini-devel-9.15-11.3.1
ghostscript-mini-debuginfo-9.15-11.3.1
ghostscript-debugsource-9.15-11.3.1
ghostscript-9.15-11.3.1
ghostscript-mini-9.15-11.3.1
ghostscript-x11-debuginfo-9.15-11.3.1
ghostscript-x11-9.15-11.3.1

145840 - SuSE Linux 42.2 openSUSE-SU-2017:0072-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9445, CVE-2016-9446, CVE-2016-9809, CVE-2016-9812, CVE-2016-9813

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0072-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00045.html>

SuSE Linux 42.2

i586
libgstbasecamerabinsrc-1_0-0-1.8.3-3.1
libgstgl-1_0-0-debuginfo-1.8.3-3.1
libgstadaptivedemux-1_0-0-1.8.3-3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-1.8.3-3.1
libgstmpegts-1_0-0-1.8.3-3.1
libgstphotography-1_0-0-debuginfo-1.8.3-3.1
libgstwayland-1_0-0-debuginfo-1.8.3-3.1
libgsturidownloader-1_0-0-debuginfo-1.8.3-3.1
libgstbadvideo-1_0-0-1.8.3-3.1
libgstbadvideo-1_0-0-debuginfo-1.8.3-3.1
libgsturidownloader-1_0-0-1.8.3-3.1
libgstplayer-1_0-0-1.8.3-3.1
gstreamer-plugins-bad-doc-1.8.3-3.1
libgstmpegts-1_0-0-debuginfo-1.8.3-3.1
libgstbadaudio-1_0-0-debuginfo-1.8.3-3.1
libgstcodecparsers-1_0-0-1.8.3-3.1

libgstcodecparsers-1_0-0-debuginfo-1.8.3-3.1
gstreamer-plugins-bad-debuginfo-1.8.3-3.1
libgstplayer-1_0-0-debuginfo-1.8.3-3.1
libgstbadbase-1_0-0-debuginfo-1.8.3-3.1
libgstinsertbin-1_0-0-debuginfo-1.8.3-3.1
gstreamer-plugins-bad-devel-1.8.3-3.1
gstreamer-plugins-bad-1.8.3-3.1
libgstbadbase-1_0-0-1.8.3-3.1
gstreamer-plugins-bad-debugsource-1.8.3-3.1
libgstgl-1_0-0-1.8.3-3.1
libgstphotography-1_0-0-1.8.3-3.1
libgstwayland-1_0-0-1.8.3-3.1
libgstbadaudio-1_0-0-1.8.3-3.1
libgstadaptivedemux-1_0-0-debuginfo-1.8.3-3.1
libgstinsertbin-1_0-0-1.8.3-3.1
libgstvdpaudio-debuginfo-1.8.3-3.1
libgstvdpaudio-1.8.3-3.1

noarch
gstreamer-plugins-bad-lang-1.8.3-3.1

x86_64
libgstphotography-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstbasecamerabinsrc-1_0-0-1.8.3-3.1
libgstgl-1_0-0-debuginfo-1.8.3-3.1
libgstadaptivedemux-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstmpegts-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstcodecparsers-1_0-0-32bit-1.8.3-3.1
libgstadaptivedemux-1_0-0-1.8.3-3.1
libgstvdpaudio-32bit-1.8.3-3.1
libgsturidownloader-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-1.8.3-3.1
libgstcodecparsers-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstmpegts-1_0-0-1.8.3-3.1
libgstphotography-1_0-0-debuginfo-1.8.3-3.1
libgstwayland-1_0-0-debuginfo-1.8.3-3.1
libgsturidownloader-1_0-0-debuginfo-1.8.3-3.1
libgstbadvideo-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstbadbase-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstbadvideo-1_0-0-1.8.3-3.1
libgstbadvideo-1_0-0-debuginfo-1.8.3-3.1
libgsturidownloader-1_0-0-1.8.3-3.1
libgstplayer-1_0-0-1.8.3-3.1
gstreamer-plugins-bad-doc-1.8.3-3.1
libgstadaptivedemux-1_0-0-32bit-1.8.3-3.1
libgstbadbase-1_0-0-32bit-1.8.3-3.1
libgstmpegts-1_0-0-debuginfo-1.8.3-3.1
libgstbadaudio-1_0-0-debuginfo-1.8.3-3.1
libgstcodecparsers-1_0-0-1.8.3-3.1
libgstcodecparsers-1_0-0-debuginfo-1.8.3-3.1
gstreamer-plugins-bad-debuginfo-1.8.3-3.1
libgstplayer-1_0-0-debuginfo-1.8.3-3.1
libgsturidownloader-1_0-0-32bit-1.8.3-3.1
libgstbadaudio-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstbadbase-1_0-0-debuginfo-1.8.3-3.1
libgstbasecamerabinsrc-1_0-0-32bit-1.8.3-3.1
libgstinsertbin-1_0-0-debuginfo-1.8.3-3.1
gstreamer-plugins-bad-devel-1.8.3-3.1
gstreamer-plugins-bad-1.8.3-3.1
libgstbadbase-1_0-0-1.8.3-3.1

libgstinsertbin-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstgl-1_0-0-debuginfo-32bit-1.8.3-3.1
gstreamer-plugins-bad-debugsource-1.8.3-3.1
libgstgl-1_0-0-1.8.3-3.1
libgstinsertbin-1_0-0-32bit-1.8.3-3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstgl-1_0-0-32bit-1.8.3-3.1
gstreamer-plugins-bad-debuginfo-32bit-1.8.3-3.1
gstreamer-plugins-bad-32bit-1.8.3-3.1
libgstphotography-1_0-0-1.8.3-3.1
libgstwayland-1_0-0-1.8.3-3.1
libgstbadaudio-1_0-0-1.8.3-3.1
libgstplayer-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstvpau-debuginfo-32bit-1.8.3-3.1
libgstwayland-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstplayer-1_0-0-32bit-1.8.3-3.1
libgstphotography-1_0-0-32bit-1.8.3-3.1
libgstadaptive-demux-1_0-0-debuginfo-1.8.3-3.1
libgstwayland-1_0-0-32bit-1.8.3-3.1
libgstinsertbin-1_0-0-1.8.3-3.1
libgstbadvideo-1_0-0-32bit-1.8.3-3.1
libgstbadaudio-1_0-0-32bit-1.8.3-3.1
libgstmpegts-1_0-0-32bit-1.8.3-3.1
libgstvpau-debuginfo-1.8.3-3.1
libgstvpau-1.8.3-3.1

145843 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0738-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5029, CVE-2017-5030, CVE-2017-5031, CVE-2017-5032, CVE-2017-5033, CVE-2017-5034, CVE-2017-5035, CVE-2017-5036, CVE-2017-5037, CVE-2017-5038, CVE-2017-5039, CVE-2017-5040, CVE-2017-5041, CVE-2017-5042, CVE-2017-5043, CVE-2017-5044, CVE-2017-5045, CVE-2017-5046

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0738-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00052.html>

SuSE Linux 42.1

x86_64

chromium-debuginfo-57.0.2987.98-105.2
chromedriver-57.0.2987.98-105.2
chromedriver-debuginfo-57.0.2987.98-105.2
chromium-57.0.2987.98-105.2
chromium-debugsource-57.0.2987.98-105.2

SuSE Linux 42.2

x86_64

chromium-debuginfo-57.0.2987.98-105.2
chromedriver-57.0.2987.98-105.2
chromedriver-debuginfo-57.0.2987.98-105.2
chromium-57.0.2987.98-105.2

145855 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1275-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8364

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1275-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00055.html>

SuSE Linux 42.1

x86_64

rzip-debuginfo-2.1-151.1

rzip-2.1-151.1

rzip-debugsource-2.1-151.1

i586

rzip-debuginfo-2.1-151.1

rzip-2.1-151.1

rzip-debugsource-2.1-151.1

SuSE Linux 42.2

x86_64

rzip-2.1-151.3.1

rzip-debuginfo-2.1-151.3.1

rzip-debugsource-2.1-151.3.1

i586

rzip-2.1-151.3.1

rzip-debuginfo-2.1-151.3.1

rzip-debugsource-2.1-151.3.1

145858 - SuSE Linux 42.1 openSUSE-SU-2017:0291-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9809

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0291-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00147.html>

SuSE Linux 42.1

i586

libgstphotography-0_10-23-0.10.23-25.1
libgstbasecamerabinsrc-0_10-23-0.10.23-25.1
libgstsignalprocessor-0_10-23-0.10.23-25.1
libgstvdp-0_10-23-debuginfo-0.10.23-25.1
gstreamer-0_10-plugins-bad-devel-0.10.23-25.1
libgstphotography-0_10-23-debuginfo-0.10.23-25.1
gstreamer-0_10-plugins-bad-debugsource-0.10.23-25.1
gstreamer-0_10-plugins-bad-debuginfo-0.10.23-25.1
libgstbasevideo-0_10-23-debuginfo-0.10.23-25.1
gstreamer-0_10-plugins-bad-0.10.23-25.1
libgstcodecparsers-0_10-23-0.10.23-25.1
libgstbasecamerabinsrc-0_10-23-debuginfo-0.10.23-25.1
libgstbasevideo-0_10-23-0.10.23-25.1
libgstcodecparsers-0_10-23-debuginfo-0.10.23-25.1
gstreamer-0_10-plugins-bad-doc-0.10.23-25.1
libgstsignalprocessor-0_10-23-debuginfo-0.10.23-25.1
libgstvdp-0_10-23-0.10.23-25.1

noarch

gstreamer-0_10-plugins-bad-lang-0.10.23-25.1

x86_64

libgstphotography-0_10-23-debuginfo-0.10.23-25.1
gstreamer-0_10-plugins-bad-debuginfo-0.10.23-25.1
libgstbasecamerabinsrc-0_10-23-debuginfo-32bit-0.10.23-25.1
libgstvdp-0_10-23-debuginfo-0.10.23-25.1
gstreamer-0_10-plugins-bad-debuginfo-32bit-0.10.23-25.1
libgstcodecparsers-0_10-23-32bit-0.10.23-25.1
libgstsignalprocessor-0_10-23-0.10.23-25.1
libgstcodecparsers-0_10-23-0.10.23-25.1
libgstbasecamerabinsrc-0_10-23-debuginfo-0.10.23-25.1
libgstphotography-0_10-23-0.10.23-25.1
libgstcodecparsers-0_10-23-debuginfo-0.10.23-25.1
libgstsignalprocessor-0_10-23-debuginfo-32bit-0.10.23-25.1
gstreamer-0_10-plugins-bad-32bit-0.10.23-25.1
libgstbasevideo-0_10-23-32bit-0.10.23-25.1
libgstbasevideo-0_10-23-0.10.23-25.1
gstreamer-0_10-plugins-bad-doc-0.10.23-25.1
libgstvdp-0_10-23-debuginfo-32bit-0.10.23-25.1
libgstvdp-0_10-23-0.10.23-25.1
libgstphotography-0_10-23-32bit-0.10.23-25.1
gstreamer-0_10-plugins-bad-devel-0.10.23-25.1
libgstbasevideo-0_10-23-debuginfo-32bit-0.10.23-25.1
libgstcodecparsers-0_10-23-debuginfo-32bit-0.10.23-25.1
libgstphotography-0_10-23-debuginfo-32bit-0.10.23-25.1
gstreamer-0_10-plugins-bad-0.10.23-25.1
libgstsignalprocessor-0_10-23-debuginfo-0.10.23-25.1
libgstbasecamerabinsrc-0_10-23-0.10.23-25.1
libgstsignalprocessor-0_10-23-32bit-0.10.23-25.1
libgstvdp-0_10-23-32bit-0.10.23-25.1
libgstbasevideo-0_10-23-debuginfo-0.10.23-25.1
gstreamer-0_10-plugins-bad-debugsource-0.10.23-25.1
libgstbasecamerabinsrc-0_10-23-32bit-0.10.23-25.1

145860 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0074-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8127, CVE-2016-3622, CVE-2016-3658, CVE-2016-5321, CVE-2016-5323, CVE-2016-5652, CVE-2016-5875, CVE-2016-9273, CVE-2016-9297, CVE-2016-9448, CVE-2016-9453

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0074-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00047.html>

SuSE Linux 42.1

x86_64

libtiff5-debuginfo-32bit-4.0.7-12.1

libtiff5-4.0.7-12.1

tiff-4.0.7-12.1

libtiff-devel-32bit-4.0.7-12.1

tiff-debugsource-4.0.7-12.1

libtiff5-debuginfo-4.0.7-12.1

tiff-debuginfo-4.0.7-12.1

libtiff-devel-4.0.7-12.1

libtiff5-32bit-4.0.7-12.1

i586

libtiff5-4.0.7-12.1

tiff-4.0.7-12.1

tiff-debugsource-4.0.7-12.1

libtiff5-debuginfo-4.0.7-12.1

tiff-debuginfo-4.0.7-12.1

libtiff-devel-4.0.7-12.1

SuSE Linux 42.2

x86_64

libtiff5-debuginfo-32bit-4.0.7-12.1

libtiff5-4.0.7-12.1

tiff-4.0.7-12.1

libtiff-devel-32bit-4.0.7-12.1

tiff-debugsource-4.0.7-12.1

libtiff5-debuginfo-4.0.7-12.1

tiff-debuginfo-4.0.7-12.1

libtiff-devel-4.0.7-12.1

libtiff5-32bit-4.0.7-12.1

i586

libtiff5-4.0.7-12.1

tiff-4.0.7-12.1

tiff-debugsource-4.0.7-12.1

libtiff5-debuginfo-4.0.7-12.1

tiff-debuginfo-4.0.7-12.1

libtiff-devel-4.0.7-12.1

145866 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2180-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11103, CVE-2017-6594

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2180-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00062.html>

SuSE Linux 42.2

x86_64

libheimdal-devel-7.4.0-2.3.1

libheimdal-debuginfo-7.4.0-2.3.1

libheimdal-debugsource-7.4.0-2.3.1

libheimdal-7.4.0-2.3.1

i586

libheimdal-devel-7.4.0-2.3.1

libheimdal-debuginfo-7.4.0-2.3.1

libheimdal-debugsource-7.4.0-2.3.1

libheimdal-7.4.0-2.3.1

SuSE Linux 42.3

x86_64

libheimdal-devel-7.4.0-3.1

libheimdal-debugsource-7.4.0-3.1

libheimdal-debuginfo-7.4.0-3.1

libheimdal-7.4.0-3.1

i586

libheimdal-devel-7.4.0-3.1

libheimdal-debugsource-7.4.0-3.1

libheimdal-debuginfo-7.4.0-3.1

libheimdal-7.4.0-3.1

145877 - SuSE Linux 42.2 openSUSE-SU-2017:1843-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7506

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1843-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00053.html>

SuSE Linux 42.2

x86_64

spice-client-0.12.7-5.4.1

libspice-server1-debuginfo-0.12.7-5.4.1

libspice-server-devel-0.12.7-5.4.1
spice-debugsource-0.12.7-5.4.1
libspice-server1-0.12.7-5.4.1

i586
spice-client-0.12.7-5.4.1
libspice-server1-debuginfo-0.12.7-5.4.1
libspice-server-devel-0.12.7-5.4.1
spice-debugsource-0.12.7-5.4.1
libspice-server1-0.12.7-5.4.1

145885 - SuSE Linux 42.1 openSUSE-SU-2017:1141-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3513, CVE-2017-3538, CVE-2017-3558, CVE-2017-3559, CVE-2017-3561, CVE-2017-3563, CVE-2017-3575, CVE-2017-3576, CVE-2017-3587

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1141-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00002.html>

SuSE Linux 42.1
x86_64
virtualbox-debuginfo-5.0.40-40.1
virtualbox-guest-x11-debuginfo-5.0.40-40.1
virtualbox-qt-5.0.40-40.1
virtualbox-guest-kmp-default-5.0.40_k4.1.39_53-40.1
virtualbox-guest-tools-debuginfo-5.0.40-40.1
python-virtualbox-5.0.40-40.1
virtualbox-5.0.40-40.1
virtualbox-websrv-debuginfo-5.0.40-40.1
virtualbox-debugsource-5.0.40-40.1
virtualbox-guest-tools-5.0.40-40.1
virtualbox-guest-x11-5.0.40-40.1
python-virtualbox-debuginfo-5.0.40-40.1
virtualbox-devel-5.0.40-40.1
virtualbox-websrv-5.0.40-40.1
virtualbox-guest-kmp-default-debuginfo-5.0.40_k4.1.39_53-40.1
virtualbox-host-kmp-default-debuginfo-5.0.40_k4.1.39_53-40.1
virtualbox-qt-debuginfo-5.0.40-40.1
virtualbox-host-kmp-default-5.0.40_k4.1.39_53-40.1

noarch
virtualbox-host-source-5.0.40-40.1
virtualbox-guest-desktop-icons-5.0.40-40.1

145889 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2016-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9788

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2016-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00122.html>

SuSE Linux 42.2

i586

apache2-debuginfo-2.4.23-8.9.1
apache2-event-2.4.23-8.9.1
apache2-event-debuginfo-2.4.23-8.9.1
apache2-prefork-2.4.23-8.9.1
apache2-utils-2.4.23-8.9.1
apache2-prefork-debuginfo-2.4.23-8.9.1
apache2-2.4.23-8.9.1
apache2-devel-2.4.23-8.9.1
apache2-utils-debuginfo-2.4.23-8.9.1
apache2-worker-debuginfo-2.4.23-8.9.1
apache2-debugsource-2.4.23-8.9.1
apache2-worker-2.4.23-8.9.1
apache2-example-pages-2.4.23-8.9.1

noarch

apache2-doc-2.4.23-8.9.1

x86_64

apache2-debuginfo-2.4.23-8.9.1
apache2-event-2.4.23-8.9.1
apache2-event-debuginfo-2.4.23-8.9.1
apache2-prefork-2.4.23-8.9.1
apache2-utils-2.4.23-8.9.1
apache2-prefork-debuginfo-2.4.23-8.9.1
apache2-2.4.23-8.9.1
apache2-devel-2.4.23-8.9.1
apache2-utils-debuginfo-2.4.23-8.9.1
apache2-worker-debuginfo-2.4.23-8.9.1
apache2-debugsource-2.4.23-8.9.1
apache2-worker-2.4.23-8.9.1
apache2-example-pages-2.4.23-8.9.1

SuSE Linux 42.3

i586

apache2-devel-2.4.23-13.1
apache2-event-debuginfo-2.4.23-13.1
apache2-prefork-2.4.23-13.1
apache2-debuginfo-2.4.23-13.1
apache2-prefork-debuginfo-2.4.23-13.1
apache2-utils-debuginfo-2.4.23-13.1
apache2-example-pages-2.4.23-13.1
apache2-worker-debuginfo-2.4.23-13.1
apache2-worker-2.4.23-13.1
apache2-event-2.4.23-13.1
apache2-2.4.23-13.1

apache2-debugsource-2.4.23-13.1
apache2-utils-2.4.23-13.1

noarch
apache2-doc-2.4.23-13.1

x86_64
apache2-devel-2.4.23-13.1
apache2-event-debuginfo-2.4.23-13.1
apache2-prefork-2.4.23-13.1
apache2-debuginfo-2.4.23-13.1
apache2-prefork-debuginfo-2.4.23-13.1
apache2-utils-debuginfo-2.4.23-13.1
apache2-example-pages-2.4.23-13.1
apache2-worker-debuginfo-2.4.23-13.1
apache2-worker-2.4.23-13.1
apache2-event-2.4.23-13.1
apache2-2.4.23-13.1
apache2-debugsource-2.4.23-13.1
apache2-utils-2.4.23-13.1

145895 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2185-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12678

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2185-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00076.html>

SuSE Linux 42.2

x86_64
libtag_c0-32bit-1.11-2.3.1
libtag1-debuginfo-1.11-2.3.1
taglib-debuginfo-1.11-2.3.1
libtag1-1.11-2.3.1
libtag1-debuginfo-32bit-1.11-2.3.1
libtag_c0-debuginfo-32bit-1.11-2.3.1
libtag_c0-1.11-2.3.1
libtag1-32bit-1.11-2.3.1
taglib-debugsource-1.11-2.3.1
taglib-1.11-2.3.1
libtag_c0-debuginfo-1.11-2.3.1
libtag-devel-1.11-2.3.1

i586

libtag1-debuginfo-1.11-2.3.1
taglib-debuginfo-1.11-2.3.1
libtag1-1.11-2.3.1
libtag_c0-1.11-2.3.1
taglib-debugsource-1.11-2.3.1

taglib-1.11-2.3.1
libtag_c0-debuginfo-1.11-2.3.1
libtag-devel-1.11-2.3.1

SuSE Linux 42.3

x86_64
libtag1-1.11-5.1
libtag1-debuginfo-32bit-1.11-5.1
libtag_c0-debuginfo-1.11-5.1
taglib-debugsource-1.11-5.1
libtag_c0-32bit-1.11-5.1
libtag1-32bit-1.11-5.1
libtag-devel-1.11-5.1
taglib-debuginfo-1.11-5.1
libtag_c0-1.11-5.1
libtag_c0-debuginfo-32bit-1.11-5.1
libtag1-debuginfo-1.11-5.1
taglib-1.11-5.1

i586

libtag1-1.11-5.1
libtag_c0-debuginfo-1.11-5.1
taglib-debugsource-1.11-5.1
libtag-devel-1.11-5.1
taglib-debuginfo-1.11-5.1
libtag_c0-1.11-5.1
libtag1-debuginfo-1.11-5.1
taglib-1.11-5.1

163451 - Oracle Enterprise Linux ELSA-2017-2550 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9776

Description

The scan detected that the host is missing the following update:
ELSA-2017-2550

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-August/007168.html>

OEL6

x86_64
poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-qt-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9

i386

poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-qt-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9

163452 - Oracle Enterprise Linux ELSA-2017-2551 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9775, CVE-2017-9776

Description

The scan detected that the host is missing the following update:
ELSA-2017-2551

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-August/007167.html>

OEL7
x86_64
poppler-utils-0.26.5-17.el7_4
poppler-qt-0.26.5-17.el7_4
poppler-demos-0.26.5-17.el7_4
poppler-glib-0.26.5-17.el7_4
poppler-devel-0.26.5-17.el7_4
poppler-cpp-0.26.5-17.el7_4
poppler-qt-devel-0.26.5-17.el7_4
poppler-0.26.5-17.el7_4
poppler-cpp-devel-0.26.5-17.el7_4
poppler-glib-devel-0.26.5-17.el7_4

170866 - Amazon Linux AMI ALAS-2017-879 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10207, CVE-2017-5581, CVE-2017-7392, CVE-2017-7393, CVE-2017-7394, CVE-2017-7395, CVE-2017-7396

Description

The scan detected that the host is missing the following update:
ALAS-2017-879

Observation

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

<https://alas.aws.amazon.com/ALAS-2017-879.html>

Amazon Linux AMI

x86_64
tigervnc-debuginfo-1.8.0-1.32.amzn1
tigervnc-server-1.8.0-1.32.amzn1
tigervnc-1.8.0-1.32.amzn1
tigervnc-server-module-1.8.0-1.32.amzn1

i686
tigervnc-1.8.0-1.32.amzn1
tigervnc-server-1.8.0-1.32.amzn1
tigervnc-debuginfo-1.8.0-1.32.amzn1
tigervnc-server-module-1.8.0-1.32.amzn1

175254 - Scientific Linux Security ERRATA Moderate: poppler on SL6.x i386/x86_64 (1708-24152)

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

Risk Level: Medium

CVE: CVE-2017-9776

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: poppler on SL6.x i386/x86_64 (1708-24152)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=24152>

SL6
x86_64
poppler-qt-devel-0.12.4-12.el6_9
poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-debuginfo-0.12.4-12.el6_9

i386
poppler-qt-devel-0.12.4-12.el6_9
poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-debuginfo-0.12.4-12.el6_9

175255 - Scientific Linux Security ERRATA Moderate: poppler on SL7.x x86_64 (1708-23809)

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

Risk Level: Medium

CVE: CVE-2017-9775, CVE-2017-9776

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: poppler on SL7.x x86_64 (1708-23809)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=23809>

SL7
x86_64
poppler-debuginfo-0.26.5-17.el7_4
poppler-cpp-devel-0.26.5-17.el7_4
poppler-qt-0.26.5-17.el7_4
poppler-demos-0.26.5-17.el7_4
poppler-glib-0.26.5-17.el7_4
poppler-devel-0.26.5-17.el7_4
poppler-utils-0.26.5-17.el7_4
poppler-qt-devel-0.26.5-17.el7_4
poppler-0.26.5-17.el7_4
poppler-cpp-0.26.5-17.el7_4
poppler-glib-devel-0.26.5-17.el7_4

192591 - Fedora Linux 25 FEDORA-2017-98e8569b33 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7069, CVE-2017-7557

Description

The scan detected that the host is missing the following update:
FEDORA-2017-98e8569b33

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=2>

Fedora Core 25

dnsmdist-1.2.0-1.fc25

192596 - Fedora Linux 26 FEDORA-2017-487fae29b4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7069, CVE-2017-7557

Description

The scan detected that the host is missing the following update:
FEDORA-2017-487fae29b4

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

dnsmdist-1.2.0-1.fc26

192600 - Fedora Linux 25 FEDORA-2017-2317191f8a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12678

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2317191f8a

Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 25

taglib-1.11.1-5.fc25

22332 - (K15311661) F5 BIG-IP NodeJS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-2086

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the NodeJS component. Successful exploitation could allow an attacker to conduct HTTP request smuggling attack and bypass the security restrictions to reach the web server on the target system.

22344 - SpiderControl SCADA Web Server Path Traversal Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-12694

Description

A vulnerability is present in some versions of SpiderControl SCADA Web Server.

Observation

SpiderControl SCADA Web Server is a software management platform.

A vulnerability is present in some versions of SpiderControl SCADA Web Server. The flaw lies in directory-traversal sequences. Successful exploitation could allow a remote attacker to disclose sensitive information.

22350 - (K91084571) F5 BIG-IP PHP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8873

Description

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

Observation

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

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

130871 - Debian Linux 8.0, 9.0 DSA-3962-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11185

Description

The scan detected that the host is missing the following update:
DSA-3962-1

Observation

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

<http://www.debian.org/security/2017/dsa-3962>

Debian 8.0
all
strongswan_5.2.1-6+deb8u5

Debian 9.0
all
strongswan_5.5.1-4+deb9u1

141701 - Red Hat Enterprise Linux RHSA-2017-2569 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7551

Description

The scan detected that the host is missing the following update:
RHSA-2017-2569

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-September/msg00001.html>

RHEL7D

x86_64
389-ds-base-devel-1.3.6.1-19.el7_4
389-ds-base-1.3.6.1-19.el7_4
389-ds-base-debuginfo-1.3.6.1-19.el7_4
389-ds-base-snmp-1.3.6.1-19.el7_4
389-ds-base-libs-1.3.6.1-19.el7_4

RHEL7S

x86_64
389-ds-base-devel-1.3.6.1-19.el7_4
389-ds-base-1.3.6.1-19.el7_4
389-ds-base-debuginfo-1.3.6.1-19.el7_4
389-ds-base-snmp-1.3.6.1-19.el7_4
389-ds-base-libs-1.3.6.1-19.el7_4

RHEL7WS

x86_64
389-ds-base-devel-1.3.6.1-19.el7_4
389-ds-base-1.3.6.1-19.el7_4
389-ds-base-debuginfo-1.3.6.1-19.el7_4
389-ds-base-snmp-1.3.6.1-19.el7_4
389-ds-base-libs-1.3.6.1-19.el7_4

145508 - SuSE Linux 42.2 openSUSE-SU-2017:0429-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10173

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0429-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00047.html>

SuSE Linux 42.2

x86_64
ruby2.1-rubygem-minitar-0.5.4-3.1
ruby2.1-rubygem-minitar-doc-0.5.4-3.1

i586

ruby2.1-rubygem-minitar-0.5.4-3.1

145513 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2184-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12067

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2184-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00077.html>

SuSE Linux 42.2

x86_64

libpotrace0-debuginfo-1.15-10.3.1

potrace-debugsource-1.15-10.3.1

potrace-debuginfo-1.15-10.3.1

potrace-devel-1.15-10.3.1

libpotrace0-1.15-10.3.1

potrace-1.15-10.3.1

i586

libpotrace0-debuginfo-1.15-10.3.1

potrace-debugsource-1.15-10.3.1

potrace-debuginfo-1.15-10.3.1

potrace-devel-1.15-10.3.1

libpotrace0-1.15-10.3.1

potrace-1.15-10.3.1

SuSE Linux 42.3

x86_64

potrace-debuginfo-1.15-13.1

potrace-1.15-13.1

potrace-debugsource-1.15-13.1

libpotrace0-debuginfo-1.15-13.1

potrace-devel-1.15-13.1

libpotrace0-1.15-13.1

i586

potrace-debuginfo-1.15-13.1

potrace-1.15-13.1

potrace-debugsource-1.15-13.1

libpotrace0-debuginfo-1.15-13.1

potrace-devel-1.15-13.1

libpotrace0-1.15-13.1

145522 - SuSE Linux 42.2 openSUSE-SU-2017:1844-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9217

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1844-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00054.html>

SuSE Linux 42.2

i586

libudev1-debuginfo-228-25.6.1

systemd-mini-sysvinit-228-25.6.1

udev-mini-debuginfo-228-25.6.1

libsystemd0-mini-debuginfo-228-25.6.1

udev-228-25.6.1

libudev-mini1-228-25.6.1

libudev1-228-25.6.1

systemd-mini-debugsource-228-25.6.1

systemd-228-25.6.1

udev-debuginfo-228-25.6.1

systemd-logger-228-25.6.1

systemd-debugsource-228-25.6.1

libudev-devel-228-25.6.1

nss-myhostname-228-25.6.1

nss-myhostname-debuginfo-228-25.6.1

nss-mymachines-debuginfo-228-25.6.1

libudev-mini-devel-228-25.6.1

systemd-mini-228-25.6.1

libsystemd0-228-25.6.1

systemd-mini-devel-228-25.6.1

systemd-debuginfo-228-25.6.1

libsystemd0-debuginfo-228-25.6.1

systemd-mini-debuginfo-228-25.6.1

libudev-mini1-debuginfo-228-25.6.1

udev-mini-228-25.6.1

systemd-devel-228-25.6.1

systemd-sysvinit-228-25.6.1

nss-mymachines-228-25.6.1

libsystemd0-mini-228-25.6.1

noarch

systemd-bash-completion-228-25.6.1

systemd-mini-bash-completion-228-25.6.1

x86_64

libudev1-debuginfo-228-25.6.1

systemd-mini-sysvinit-228-25.6.1

udev-mini-debuginfo-228-25.6.1

libsystemd0-mini-debuginfo-228-25.6.1

udev-228-25.6.1

systemd-debuginfo-32bit-228-25.6.1

libudev-mini1-228-25.6.1

libudev1-debuginfo-32bit-228-25.6.1

libudev1-228-25.6.1

systemd-mini-debugsource-228-25.6.1

systemd-228-25.6.1

udev-debuginfo-228-25.6.1

systemd-logger-228-25.6.1
systemd-debugsource-228-25.6.1
libudev-devel-228-25.6.1
nss-myhostname-228-25.6.1
nss-myhostname-debuginfo-228-25.6.1
nss-mymachines-debuginfo-228-25.6.1
libudev1-32bit-228-25.6.1
libudev-mini-devel-228-25.6.1
systemd-mini-228-25.6.1
libsystemd0-debuginfo-32bit-228-25.6.1
nss-myhostname-32bit-228-25.6.1
libsystemd0-228-25.6.1
systemd-mini-devel-228-25.6.1
systemd-debuginfo-228-25.6.1
libsystemd0-debuginfo-228-25.6.1
systemd-mini-debuginfo-228-25.6.1
libsystemd0-32bit-228-25.6.1
libudev-mini1-debuginfo-228-25.6.1
udev-mini-228-25.6.1
nss-myhostname-debuginfo-32bit-228-25.6.1
systemd-devel-228-25.6.1
systemd-sysvinit-228-25.6.1
systemd-32bit-228-25.6.1
nss-mymachines-228-25.6.1
libsystemd0-mini-228-25.6.1

145531 - SuSE Linux 42.2 openSUSE-SU-2017:0259-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8688, CVE-2016-9928

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0259-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00130.html>

SuSE Linux 42.2

noarch

python3-sleekxmp-1.3.1-3.1

145539 - SuSE Linux 42.2 openSUSE-SU-2017:0941-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7055, CVE-2017-3731, CVE-2017-3732

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0941-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00025.html>

SuSE Linux 42.2

i586

nodejs4-devel-4.7.3-5.3.1

nodejs4-debuginfo-4.7.3-5.3.1

nodejs4-4.7.3-5.3.1

nodejs4-debugsource-4.7.3-5.3.1

npm4-4.7.3-5.3.1

noarch

nodejs4-docs-4.7.3-5.3.1

x86_64

nodejs4-devel-4.7.3-5.3.1

nodejs4-debuginfo-4.7.3-5.3.1

nodejs4-4.7.3-5.3.1

nodejs4-debugsource-4.7.3-5.3.1

npm4-4.7.3-5.3.1

145543 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2347-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10791, CVE-2017-10792, CVE-2017-12958, CVE-2017-12959, CVE-2017-12960, CVE-2017-12961

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2347-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00006.html>

SuSE Linux 42.2

x86_64

pspp-devel-1.0.1-2.6.1

pspp-debuginfo-1.0.1-2.6.1

pspp-1.0.1-2.6.1

pspp-debugsource-1.0.1-2.6.1

SuSE Linux 42.3

x86_64

pspp-debuginfo-1.0.1-8.1

pspp-devel-1.0.1-8.1

pspp-debugsource-1.0.1-8.1

pspp-1.0.1-8.1

145549 - SuSE Linux 42.1 openSUSE-SU-2017:0903-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0903-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00120.html>

SuSE Linux 42.1

i586

apache2-event-2.4.16-18.1

apache2-debuginfo-2.4.16-18.1

apache2-event-debuginfo-2.4.16-18.1

apache2-debugsource-2.4.16-18.1

apache2-2.4.16-18.1

apache2-worker-debuginfo-2.4.16-18.1

apache2-devel-2.4.16-18.1

apache2-utils-2.4.16-18.1

apache2-prefork-2.4.16-18.1

apache2-worker-2.4.16-18.1

apache2-prefork-debuginfo-2.4.16-18.1

apache2-example-pages-2.4.16-18.1

apache2-utils-debuginfo-2.4.16-18.1

noarch

apache2-doc-2.4.16-18.1

x86_64

apache2-event-2.4.16-18.1

apache2-debuginfo-2.4.16-18.1

apache2-event-debuginfo-2.4.16-18.1

apache2-debugsource-2.4.16-18.1

apache2-2.4.16-18.1

apache2-worker-debuginfo-2.4.16-18.1

apache2-devel-2.4.16-18.1

apache2-utils-2.4.16-18.1

apache2-prefork-2.4.16-18.1

apache2-worker-2.4.16-18.1

apache2-prefork-debuginfo-2.4.16-18.1

apache2-example-pages-2.4.16-18.1

apache2-utils-debuginfo-2.4.16-18.1

145560 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:1960-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9262, CVE-2016-9388, CVE-2016-9389, CVE-2016-9390, CVE-2016-9391, CVE-2016-9392, CVE-2016-9393, CVE-2016-9394, CVE-2017-1000050

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1960-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00092.html>

SuSE Linux 42.2

x86_64

libjasper1-1.900.14-175.6.1

jasper-1.900.14-175.6.1

libjasper1-32bit-1.900.14-175.6.1

jasper-debuginfo-1.900.14-175.6.1

libjasper1-debuginfo-32bit-1.900.14-175.6.1

libjasper-devel-1.900.14-175.6.1

libjasper1-debuginfo-1.900.14-175.6.1

jasper-debugsource-1.900.14-175.6.1

i586

libjasper1-1.900.14-175.6.1

jasper-1.900.14-175.6.1

jasper-debuginfo-1.900.14-175.6.1

libjasper-devel-1.900.14-175.6.1

libjasper1-debuginfo-1.900.14-175.6.1

jasper-debugsource-1.900.14-175.6.1

SuSE Linux 42.3

x86_64

libjasper1-debuginfo-32bit-1.900.14-179.1

libjasper1-32bit-1.900.14-179.1

jasper-debugsource-1.900.14-179.1

jasper-1.900.14-179.1

libjasper1-debuginfo-1.900.14-179.1

libjasper1-1.900.14-179.1

jasper-debuginfo-1.900.14-179.1

libjasper-devel-1.900.14-179.1

i586

jasper-debugsource-1.900.14-179.1

jasper-1.900.14-179.1

libjasper1-debuginfo-1.900.14-179.1

libjasper1-1.900.14-179.1

jasper-debuginfo-1.900.14-179.1

libjasper-devel-1.900.14-179.1

145561 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0006-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9933

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0006-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00002.html>

SuSE Linux 42.1

x86_64

gd-debuginfo-32bit-2.1.0-16.1

gd-32bit-2.1.0-16.1

gd-debugsource-2.1.0-16.1

gd-2.1.0-16.1

gd-debuginfo-2.1.0-16.1

gd-devel-2.1.0-16.1

i586

gd-devel-2.1.0-16.1

gd-debuginfo-2.1.0-16.1

gd-2.1.0-16.1

gd-debugsource-2.1.0-16.1

SuSE Linux 42.2

x86_64

gd-2.1.0-13.1

gd-devel-2.1.0-13.1

gd-debuginfo-32bit-2.1.0-13.1

gd-debugsource-2.1.0-13.1

gd-debuginfo-2.1.0-13.1

gd-32bit-2.1.0-13.1

i586

gd-2.1.0-13.1

gd-debugsource-2.1.0-13.1

gd-debuginfo-2.1.0-13.1

gd-devel-2.1.0-13.1

145565 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0669-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10189

Description

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

openSUSE-SU-2017:0669-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00026.html>

SuSE Linux 42.1

x86_64

bitlbee-doc-3.4.1-5.1

bitlbee-3.4.1-5.1

bitlbee-debuginfo-3.4.1-5.1

bitlbee-debugsource-3.4.1-5.1

i586

bitlbee-doc-3.4.1-5.1

bitlbee-3.4.1-5.1

bitlbee-debuginfo-3.4.1-5.1
bitlbee-debugsource-3.4.1-5.1

SuSE Linux 42.2
x86_64
bitlbee-debuginfo-3.4.2-3.1
bitlbee-doc-3.4.2-3.1
bitlbee-3.4.2-3.1
bitlbee-devel-3.4.2-3.1

145582 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0668-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9179

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0668-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00027.html>

SuSE Linux 42.1
x86_64
lynx-debuginfo-2.8.7-5.1
lynx-2.8.7-5.1
lynx-debugsource-2.8.7-5.1

i586
lynx-debuginfo-2.8.7-5.1
lynx-2.8.7-5.1
lynx-debugsource-2.8.7-5.1

SuSE Linux 42.2
x86_64
lynx-debuginfo-2.8.7-6.1
lynx-2.8.7-6.1
lynx-debugsource-2.8.7-6.1

i586
lynx-debuginfo-2.8.7-6.1
lynx-2.8.7-6.1
lynx-debugsource-2.8.7-6.1

145583 - SuSE Linux 42.2 openSUSE-SU-2017:1066-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10198, CVE-2016-10199, CVE-2017-5840, CVE-2017-5841, CVE-2017-5845

Description

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

openSUSE-SU-2017:1066-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00073.html>

SuSE Linux 42.2

i586

gststreamer-plugins-good-debuginfo-1.8.3-5.3.1
gststreamer-plugins-good-extra-1.8.3-5.3.1
gststreamer-plugins-good-extra-debuginfo-1.8.3-5.3.1
gststreamer-plugins-good-doc-1.8.3-5.3.1
gststreamer-plugins-good-1.8.3-5.3.1
gststreamer-plugins-good-debugsource-1.8.3-5.3.1

noarch

gststreamer-plugins-good-lang-1.8.3-5.3.1

x86_64

gststreamer-plugins-good-debuginfo-1.8.3-5.3.1
gststreamer-plugins-good-extra-1.8.3-5.3.1
gststreamer-plugins-good-extra-debuginfo-1.8.3-5.3.1
gststreamer-plugins-good-doc-1.8.3-5.3.1
gststreamer-plugins-good-extra-debuginfo-32bit-1.8.3-5.3.1
gststreamer-plugins-good-1.8.3-5.3.1
gststreamer-plugins-good-debugsource-1.8.3-5.3.1
gststreamer-plugins-good-32bit-1.8.3-5.3.1
gststreamer-plugins-good-extra-32bit-1.8.3-5.3.1
gststreamer-plugins-good-debuginfo-32bit-1.8.3-5.3.1

145584 - SuSE Linux 42.2 openSUSE-SU-2017:1032-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5843, CVE-2017-5848

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1032-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00059.html>

SuSE Linux 42.2

i586

libgstbadbase-1_0-0-1.8.3-5.3.1
libgstphotography-1_0-0-1.8.3-5.3.1
gststreamer-plugins-bad-devel-1.8.3-5.3.1
libgstadaptivedemux-1_0-0-1.8.3-5.3.1
libgstwayland-1_0-0-1.8.3-5.3.1
gststreamer-plugins-bad-1.8.3-5.3.1
libgstbasecamerabinsrc-1_0-0-1.8.3-5.3.1

gstreamer-plugins-bad-debugsource-1.8.3-5.3.1
gstreamer-plugins-bad-debuginfo-1.8.3-5.3.1
libgstbadaudio-1_0-0-1.8.3-5.3.1
libgstinsertbin-1_0-0-1.8.3-5.3.1
libgstbadaudio-1_0-0-debuginfo-1.8.3-5.3.1
libgstvdpaudio-debuginfo-1.8.3-5.3.1
libgstbadvideo-1_0-0-debuginfo-1.8.3-5.3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-1.8.3-5.3.1
libgstmpegts-1_0-0-1.8.3-5.3.1
libgstvdpaudio-1.8.3-5.3.1
libgstcodecparsers-1_0-0-1.8.3-5.3.1
libgsturidownloader-1_0-0-1.8.3-5.3.1
libgstcodecparsers-1_0-0-debuginfo-1.8.3-5.3.1
libgstbadbase-1_0-0-debuginfo-1.8.3-5.3.1
libgsturidownloader-1_0-0-debuginfo-1.8.3-5.3.1
libgstadaptivedemux-1_0-0-debuginfo-1.8.3-5.3.1
libgstwayland-1_0-0-debuginfo-1.8.3-5.3.1
libgstgl-1_0-0-1.8.3-5.3.1
libgstmpegts-1_0-0-debuginfo-1.8.3-5.3.1
libgstinsertbin-1_0-0-debuginfo-1.8.3-5.3.1
libgstplayer-1_0-0-debuginfo-1.8.3-5.3.1
libgstgl-1_0-0-debuginfo-1.8.3-5.3.1
libgstbadvideo-1_0-0-1.8.3-5.3.1
gstreamer-plugins-bad-doc-1.8.3-5.3.1
libgstphotography-1_0-0-debuginfo-1.8.3-5.3.1
libgstplayer-1_0-0-1.8.3-5.3.1

noarch

gstreamer-plugins-bad-lang-1.8.3-5.3.1

x86_64

libgstbadbase-1_0-0-1.8.3-5.3.1
libgstinsertbin-1_0-0-32bit-1.8.3-5.3.1
libgstphotography-1_0-0-1.8.3-5.3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstgl-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstvdpaudio-32bit-1.8.3-5.3.1
gstreamer-plugins-bad-devel-1.8.3-5.3.1
gstreamer-plugins-bad-debuginfo-32bit-1.8.3-5.3.1
libgstadaptivedemux-1_0-0-1.8.3-5.3.1
libgstwayland-1_0-0-1.8.3-5.3.1
libgstwayland-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstphotography-1_0-0-32bit-1.8.3-5.3.1
gstreamer-plugins-bad-1.8.3-5.3.1
libgstbasecamerabinsrc-1_0-0-1.8.3-5.3.1
gstreamer-plugins-bad-debugsource-1.8.3-5.3.1
gstreamer-plugins-bad-debuginfo-1.8.3-5.3.1
libgstvdpaudio-debuginfo-32bit-1.8.3-5.3.1
libgstphotography-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstbadaudio-1_0-0-1.8.3-5.3.1
libgstbadaudio-1_0-0-32bit-1.8.3-5.3.1
libgstinsertbin-1_0-0-1.8.3-5.3.1
libgstbadaudio-1_0-0-debuginfo-1.8.3-5.3.1
libgstvdpaudio-debuginfo-1.8.3-5.3.1
libgstcodecparsers-1_0-0-32bit-1.8.3-5.3.1
libgstcodecparsers-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstbadvideo-1_0-0-debuginfo-1.8.3-5.3.1
libgstbasecamerabinsrc-1_0-0-debuginfo-1.8.3-5.3.1
libgstplayer-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstmpegts-1_0-0-1.8.3-5.3.1

libgstadaptivedemux-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstvdpa-1.8.3-5.3.1
libgstbasecamerabinsrc-1_0-0-32bit-1.8.3-5.3.1
libgstbadbase-1_0-0-32bit-1.8.3-5.3.1
libgstcodecparsers-1_0-0-1.8.3-5.3.1
libgsturidownloader-1_0-0-1.8.3-5.3.1
libgstcodecparsers-1_0-0-debuginfo-1.8.3-5.3.1
libgstbadbase-1_0-0-debuginfo-1.8.3-5.3.1
libgsturidownloader-1_0-0-32bit-1.8.3-5.3.1
libgsturidownloader-1_0-0-debuginfo-1.8.3-5.3.1
libgstadaptivedemux-1_0-0-debuginfo-1.8.3-5.3.1
libgstwayland-1_0-0-debuginfo-1.8.3-5.3.1
libgstgl-1_0-0-1.8.3-5.3.1
libgstmpegts-1_0-0-debuginfo-1.8.3-5.3.1
libgstinsertbin-1_0-0-debuginfo-1.8.3-5.3.1
libgstbadvideo-1_0-0-32bit-1.8.3-5.3.1
libgstbadaudio-1_0-0-debuginfo-32bit-1.8.3-5.3.1
gstreamer-plugins-bad-32bit-1.8.3-5.3.1
libgstbadvideo-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstplayer-1_0-0-debuginfo-1.8.3-5.3.1
libgstwayland-1_0-0-32bit-1.8.3-5.3.1
libgstmpegts-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstgl-1_0-0-debuginfo-1.8.3-5.3.1
libgstbadvideo-1_0-0-1.8.3-5.3.1
libgstinsertbin-1_0-0-debuginfo-32bit-1.8.3-5.3.1
gstreamer-plugins-bad-doc-1.8.3-5.3.1
libgstmpegts-1_0-0-32bit-1.8.3-5.3.1
libgstplayer-1_0-0-32bit-1.8.3-5.3.1
libgstadaptivedemux-1_0-0-32bit-1.8.3-5.3.1
libgstgl-1_0-0-32bit-1.8.3-5.3.1
libgstphotography-1_0-0-debuginfo-1.8.3-5.3.1
libgsturidownloader-1_0-0-debuginfo-32bit-1.8.3-5.3.1
libgstplayer-1_0-0-1.8.3-5.3.1
libgstbadbase-1_0-0-debuginfo-32bit-1.8.3-5.3.1

145587 - SuSE Linux 42.1 openSUSE-SU-2017:0649-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6318

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0649-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00016.html>

SuSE Linux 42.1

x86_64

sane-backends-debuginfo-32bit-1.0.24-5.1

sane-backends-1.0.24-5.1

sane-backends-debuginfo-1.0.24-5.1

sane-backends-32bit-1.0.24-5.1

sane-backends-devel-1.0.24-5.1

sane-backends-debugsource-1.0.24-5.1
sane-backends-autoconfig-1.0.24-5.1

i586

sane-backends-devel-1.0.24-5.1
sane-backends-autoconfig-1.0.24-5.1
sane-backends-debuginfo-1.0.24-5.1
sane-backends-debugsource-1.0.24-5.1
sane-backends-1.0.24-5.1

145594 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0444-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10207

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0444-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00053.html>

SuSE Linux 42.1

x86_64
xorg-x11-Xvnc-debuginfo-1.5.0-32.1
tigervnc-debugsource-1.5.0-32.1
tigervnc-debuginfo-1.5.0-32.1
tigervnc-1.5.0-32.1
xorg-x11-Xvnc-1.5.0-32.1

i586

xorg-x11-Xvnc-debuginfo-1.5.0-32.1
tigervnc-debugsource-1.5.0-32.1
tigervnc-debuginfo-1.5.0-32.1
tigervnc-1.5.0-32.1
xorg-x11-Xvnc-1.5.0-32.1

SuSE Linux 42.2

x86_64
libXvnc-devel-1.6.0-11.1
tigervnc-1.6.0-11.1
tigervnc-debuginfo-1.6.0-11.1
libXvnc1-1.6.0-11.1
libXvnc1-debuginfo-1.6.0-11.1
xorg-x11-Xvnc-debuginfo-1.6.0-11.1
xorg-x11-Xvnc-1.6.0-11.1
tigervnc-debugsource-1.6.0-11.1

i586

libXvnc-devel-1.6.0-11.1
tigervnc-1.6.0-11.1
tigervnc-debuginfo-1.6.0-11.1
libXvnc1-1.6.0-11.1
libXvnc1-debuginfo-1.6.0-11.1

xorg-x11-Xvnc-debuginfo-1.6.0-11.1
xorg-x11-Xvnc-1.6.0-11.1
tigervnc-debugsource-1.6.0-11.1

145601 - SuSE Linux 42.2 openSUSE-SU-2017:1521-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7483

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1521-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00028.html>

SuSE Linux 42.2

x86_64

rxvt-unicode-debuginfo-9.21-6.3.1

rxvt-unicode-9.21-6.3.1

rxvt-unicode-debugsource-9.21-6.3.1

i586

rxvt-unicode-debuginfo-9.21-6.3.1

rxvt-unicode-9.21-6.3.1

rxvt-unicode-debugsource-9.21-6.3.1

145610 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:1957-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9765

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1957-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00089.html>

SuSE Linux 42.2

x86_64

gsoap-devel-2.8.33-2.3.1

gsoap-debugsource-2.8.33-2.3.1

gsoap-devel-debuginfo-2.8.33-2.3.1

libgsoap-2_8_33-debuginfo-2.8.33-2.3.1

libgsoap-2_8_33-2.8.33-2.3.1

i586

gsoap-devel-2.8.33-2.3.1
gsoap-debugsource-2.8.33-2.3.1
gsoap-devel-debuginfo-2.8.33-2.3.1
libgsoap-2_8_33-debuginfo-2.8.33-2.3.1
libgsoap-2_8_33-2.8.33-2.3.1

SuSE Linux 42.3
i586

gsoap-debugsource-2.8.46-3.1
gsoap-devel-2.8.46-3.1
libgsoap-2_8_46-debuginfo-2.8.46-3.1
libgsoap-2_8_46-2.8.46-3.1
gsoap-devel-debuginfo-2.8.46-3.1

noarch
gsoap-doc-2.8.46-3.1

x86_64
gsoap-debugsource-2.8.46-3.1
gsoap-devel-2.8.46-3.1
libgsoap-2_8_46-debuginfo-2.8.46-3.1
libgsoap-2_8_46-2.8.46-3.1
gsoap-devel-debuginfo-2.8.46-3.1

145613 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0363-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6271

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0363-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00009.html>

SuSE Linux 42.1
x86_64
libbzrtp0-debuginfo-32bit-1.0.3-5.1
libbzrtp0-32bit-1.0.3-5.1
libbzrtp0-debuginfo-1.0.3-5.1
libbzrtp0-1.0.3-5.1
bzrtp-debugsource-1.0.3-5.1
bzrtp-devel-1.0.3-5.1

i586
bzrtp-devel-1.0.3-5.1
libbzrtp0-1.0.3-5.1
bzrtp-debugsource-1.0.3-5.1
libbzrtp0-debuginfo-1.0.3-5.1

SuSE Linux 42.2
x86_64
libbzrtp0-debuginfo-32bit-1.0.3-6.1

bzrtp-debugsource-1.0.3-6.1
libbzrtp0-debuginfo-1.0.3-6.1
libbzrtp0-32bit-1.0.3-6.1
bzrtp-devel-1.0.3-6.1
libbzrtp0-1.0.3-6.1

i586
libbzrtp0-1.0.3-6.1
bzrtp-devel-1.0.3-6.1
bzrtp-debugsource-1.0.3-6.1
libbzrtp0-debuginfo-1.0.3-6.1

145622 - SuSE Linux 42.2 openSUSE-SU-2017:1495-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7484, CVE-2017-7485, CVE-2017-7486

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1495-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00012.html>

SuSE Linux 42.2

i586
postgresql93-libs-debugsource-9.3.17-5.9.1
postgresql93-devel-9.3.17-5.9.1
postgresql93-devel-debuginfo-9.3.17-5.9.1

noarch
postgresql93-docs-9.3.17-5.9.1

x86_64
postgresql93-debugsource-9.3.17-5.9.1
postgresql93-9.3.17-5.9.1
postgresql93-debuginfo-9.3.17-5.9.1
postgresql93-contrib-9.3.17-5.9.1
postgresql93-plpython-debuginfo-9.3.17-5.9.1
postgresql93-test-9.3.17-5.9.1
postgresql93-server-9.3.17-5.9.1
postgresql93-libs-debugsource-9.3.17-5.9.1
postgresql93-plperl-9.3.17-5.9.1
postgresql93-plperl-debuginfo-9.3.17-5.9.1
postgresql93-devel-9.3.17-5.9.1
postgresql93-pltcl-9.3.17-5.9.1
postgresql93-pltcl-debuginfo-9.3.17-5.9.1
postgresql93-devel-debuginfo-9.3.17-5.9.1
postgresql93-server-debuginfo-9.3.17-5.9.1
postgresql93-plpython-9.3.17-5.9.1
postgresql93-contrib-debuginfo-9.3.17-5.9.1

145623 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0362-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4450

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0362-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00008.html>

SuSE Linux 42.1

x86_64

nginx-debuginfo-1.8.1-8.1

nginx-debugsource-1.8.1-8.1

nginx-1.8.1-8.1

i586

nginx-debuginfo-1.8.1-8.1

nginx-debugsource-1.8.1-8.1

nginx-1.8.1-8.1

SuSE Linux 42.2

x86_64

nginx-debuginfo-1.8.1-8.1

nginx-debugsource-1.8.1-8.1

nginx-1.8.1-8.1

i586

nginx-debuginfo-1.8.1-8.1

nginx-debugsource-1.8.1-8.1

nginx-1.8.1-8.1

145635 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0016-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8899

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0016-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00008.html>

SuSE Linux 42.1

x86_64

dnsmasq-utils-2.71-9.1

dnsmasq-debugsource-2.71-9.1

dnsmasq-2.71-9.1
dnsmasq-debuginfo-2.71-9.1
dnsmasq-utils-debuginfo-2.71-9.1

i586

dnsmasq-utils-2.71-9.1
dnsmasq-debugsource-2.71-9.1
dnsmasq-2.71-9.1
dnsmasq-debuginfo-2.71-9.1
dnsmasq-utils-debuginfo-2.71-9.1

SuSE Linux 42.2

x86_64
dnsmasq-2.71-8.1
dnsmasq-debuginfo-2.71-8.1
dnsmasq-utils-2.71-8.1
dnsmasq-utils-debuginfo-2.71-8.1
dnsmasq-debugsource-2.71-8.1

i586

dnsmasq-2.71-8.1
dnsmasq-debuginfo-2.71-8.1
dnsmasq-utils-2.71-8.1
dnsmasq-utils-debuginfo-2.71-8.1
dnsmasq-debugsource-2.71-8.1

145657 - SuSE Linux 42.1 openSUSE-SU-2017:0527-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7055, CVE-2017-3731, CVE-2017-3732

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0527-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00095.html>

SuSE Linux 42.1

i586
nodejs-debuginfo-4.7.3-39.1
nodejs-devel-4.7.3-39.1
npm-4.7.3-39.1
nodejs-4.7.3-39.1
nodejs-debugsource-4.7.3-39.1

noarch

nodejs-docs-4.7.3-39.1

x86_64

nodejs-debuginfo-4.7.3-39.1
nodejs-devel-4.7.3-39.1
npm-4.7.3-39.1
nodejs-4.7.3-39.1

145658 - SuSE Linux 42.2 openSUSE-SU-2017:0364-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5596, CVE-2017-5597

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0364-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00010.html>

SuSE Linux 42.2

x86_64

wireshark-2.2.4-7.1

wireshark-ui-qt-debuginfo-2.2.4-7.1

wireshark-ui-gtk-debuginfo-2.2.4-7.1

wireshark-debugsource-2.2.4-7.1

wireshark-ui-gtk-2.2.4-7.1

wireshark-ui-qt-2.2.4-7.1

wireshark-devel-2.2.4-7.1

wireshark-debuginfo-2.2.4-7.1

145663 - SuSE Linux 42.2 openSUSE-SU-2017:0192-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9749, CVE-2016-10002, CVE-2016-10003

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0192-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00107.html>

SuSE Linux 42.2

x86_64

squid-3.5.21-3.1

squid-debugsource-3.5.21-3.1

squid-debuginfo-3.5.21-3.1

i586

squid-3.5.21-3.1

squid-debugsource-3.5.21-3.1

squid-debuginfo-3.5.21-3.1

145670 - SuSE Linux 42.2 openSUSE-SU-2017:0481-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7055, CVE-2017-3731, CVE-2017-3732

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0481-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00069.html>

SuSE Linux 42.2

i586

libopenssl1_0_0-debuginfo-1.0.2j-4.1

libopenssl-devel-1.0.2j-4.1

openssl-1.0.2j-4.1

openssl-debugsource-1.0.2j-4.1

libopenssl1_0_0-1.0.2j-4.1

openssl-debuginfo-1.0.2j-4.1

libopenssl1_0_0-hmac-1.0.2j-4.1

noarch

openssl-doc-1.0.2j-4.1

x86_64

libopenssl1_0_0-debuginfo-1.0.2j-4.1

libopenssl-devel-1.0.2j-4.1

openssl-1.0.2j-4.1

openssl-debugsource-1.0.2j-4.1

libopenssl1_0_0-hmac-32bit-1.0.2j-4.1

libopenssl1_0_0-1.0.2j-4.1

openssl-debuginfo-1.0.2j-4.1

libopenssl1_0_0-hmac-1.0.2j-4.1

libopenssl1_0_0-debuginfo-32bit-1.0.2j-4.1

libopenssl1_0_0-32bit-1.0.2j-4.1

libopenssl-devel-32bit-1.0.2j-4.1

145671 - SuSE Linux 42.1 openSUSE-SU-2017:0580-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5838

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0580-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00120.html>

SuSE Linux 42.1

i586

typelib-1_0-Gst-1_0-1.4.5-5.1

gststreamer-debuginfo-1.4.5-5.1

gststreamer-doc-1.4.5-5.1

gststreamer-debugsource-1.4.5-5.1

gststreamer-utils-debuginfo-1.4.5-5.1

gststreamer-1.4.5-5.1

gststreamer-devel-1.4.5-5.1

gststreamer-utils-1.4.5-5.1

libgststreamer-1_0-0-1.4.5-5.1

libgststreamer-1_0-0-debuginfo-1.4.5-5.1

noarch

gststreamer-lang-1.4.5-5.1

x86_64

gststreamer-debugsource-1.4.5-5.1

gststreamer-doc-1.4.5-5.1

gststreamer-debuginfo-32bit-1.4.5-5.1

libgststreamer-1_0-0-1.4.5-5.1

gststreamer-utils-debuginfo-1.4.5-5.1

gststreamer-debuginfo-1.4.5-5.1

gststreamer-utils-1.4.5-5.1

gststreamer-devel-1.4.5-5.1

libgststreamer-1_0-0-debuginfo-32bit-1.4.5-5.1

gststreamer-32bit-1.4.5-5.1

libgststreamer-1_0-0-32bit-1.4.5-5.1

gststreamer-1.4.5-5.1

libgststreamer-1_0-0-debuginfo-1.4.5-5.1

typelib-1_0-Gst-1_0-1.4.5-5.1

145688 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0372-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8980, CVE-2016-6621

Description

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

openSUSE-SU-2017:0372-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00015.html>

SuSE Linux 42.1

noarch

phpMyAdmin-4.4.15.10-31.2

SuSE Linux 42.2

noarch

phpMyAdmin-4.4.15.10-31.2

145693 - SuSE Linux 42.2 openSUSE-SU-2017:1749-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9604

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1749-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00003.html>

SuSE Linux 42.2

x86_64

kdepim-addons-debuginfo-16.08.2-2.3.1

korganizer-debuginfo-4.14.10-6.5.1

kdepim4-4.14.10-6.5.1

knode-debuginfo-4.14.10-6.5.1

kmail-4.14.10-6.5.1

knotes-debuginfo-4.14.10-6.5.1

kdepim4-debugsource-4.14.10-6.5.1

akregator-debuginfo-4.14.10-6.5.1

libkdepim4-debuginfo-4.14.10-6.5.1

kdepim-addons-16.08.2-2.3.1

kontakt-4.14.10-6.5.1

knotes-4.14.10-6.5.1

kmail-debuginfo-4.14.10-6.5.1

libkdepim4-4.14.10-6.5.1

ktnef-4.14.10-6.5.1

kontakt-debuginfo-4.14.10-6.5.1

knode-4.14.10-6.5.1

akregator-4.14.10-6.5.1

kalarm-debuginfo-4.14.10-6.5.1

ktimetracker-debuginfo-4.14.10-6.5.1

ktimetracker-4.14.10-6.5.1

ktnef-debuginfo-4.14.10-6.5.1

kdepim4-debuginfo-4.14.10-6.5.1

korganizer-4.14.10-6.5.1

kdepim-addons-debugsource-16.08.2-2.3.1

kaddressbook-debuginfo-4.14.10-6.5.1

akonadi-debuginfo-4.14.10-6.5.1

akonadi-4.14.10-6.5.1

kalarm-4.14.10-6.5.1

kaddressbook-4.14.10-6.5.1

145697 - SuSE Linux 42.2 openSUSE-SU-2017:1748-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9604

Description

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

openSUSE-SU-2017:1748-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00002.html>

SuSE Linux 42.2

x86_64

kaddressbook5-16.08.2-2.5.3

messagelib-16.08.2-2.6.1

knotes5-debuginfo-16.08.2-2.5.3

messagelib-debugsource-16.08.2-2.6.1

kmail5-debuginfo-16.08.2-2.5.3

kcontact5-debuginfo-16.08.2-2.5.3

messagelib-devel-16.08.2-2.6.1

kaddressbook5-debuginfo-16.08.2-2.5.3

korganizer5-16.08.2-2.5.3

blogilo5-16.08.2-2.5.3

kalarm5-debuginfo-16.08.2-2.5.3

akregator5-debuginfo-16.08.2-2.5.3

knotes5-16.08.2-2.5.3

korganizer5-debuginfo-16.08.2-2.5.3

ktnef5-16.08.2-2.5.3

akonadi_resources-debuginfo-16.08.2-2.5.3

blogilo5-debuginfo-16.08.2-2.5.3

messagelib-debuginfo-16.08.2-2.6.1

ktnef5-debuginfo-16.08.2-2.5.3

kalarm5-16.08.2-2.5.3

akonadi_resources-16.08.2-2.5.3

kdepim-debugsource-16.08.2-2.5.3

akregator5-16.08.2-2.5.3

kcontact5-16.08.2-2.5.3

kdepim-debuginfo-16.08.2-2.5.3

kdepim-16.08.2-2.5.3

kmail5-16.08.2-2.5.3

145704 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2011-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3633, CVE-2017-3634, CVE-2017-3635, CVE-2017-3636, CVE-2017-3641, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653, CVE-2017-3732

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2011-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00117.html>

SuSE Linux 42.2

x86_64

mysql-community-server-debugsource-5.6.37-24.9.1
libmysql56client_r18-32bit-5.6.37-24.9.1
libmysql56client18-5.6.37-24.9.1
mysql-community-server-test-debuginfo-5.6.37-24.9.1
mysql-community-server-errormessages-5.6.37-24.9.1
mysql-community-server-test-5.6.37-24.9.1
mysql-community-server-debuginfo-5.6.37-24.9.1
mysql-community-server-5.6.37-24.9.1
mysql-community-server-bench-5.6.37-24.9.1
mysql-community-server-tools-5.6.37-24.9.1
mysql-community-server-tools-debuginfo-5.6.37-24.9.1
mysql-community-server-client-5.6.37-24.9.1
mysql-community-server-client-debuginfo-5.6.37-24.9.1
mysql-community-server-bench-debuginfo-5.6.37-24.9.1
libmysql56client18-32bit-5.6.37-24.9.1
libmysql56client18-debuginfo-32bit-5.6.37-24.9.1
libmysql56client_r18-5.6.37-24.9.1
libmysql56client18-debuginfo-5.6.37-24.9.1

i586

mysql-community-server-debugsource-5.6.37-24.9.1
libmysql56client18-5.6.37-24.9.1
mysql-community-server-test-debuginfo-5.6.37-24.9.1
mysql-community-server-errormessages-5.6.37-24.9.1
mysql-community-server-test-5.6.37-24.9.1
mysql-community-server-debuginfo-5.6.37-24.9.1
mysql-community-server-5.6.37-24.9.1
mysql-community-server-bench-5.6.37-24.9.1
mysql-community-server-tools-5.6.37-24.9.1
mysql-community-server-tools-debuginfo-5.6.37-24.9.1
mysql-community-server-client-5.6.37-24.9.1
mysql-community-server-client-debuginfo-5.6.37-24.9.1
mysql-community-server-bench-debuginfo-5.6.37-24.9.1
libmysql56client_r18-5.6.37-24.9.1
libmysql56client18-debuginfo-5.6.37-24.9.1

SuSE Linux 42.3

x86_64

libmysql56client18-debuginfo-32bit-5.6.37-27.1
libmysql56client_r18-5.6.37-27.1
mysql-community-server-debuginfo-5.6.37-27.1
mysql-community-server-5.6.37-27.1
libmysql56client18-32bit-5.6.37-27.1
mysql-community-server-errormessages-5.6.37-27.1
libmysql56client18-5.6.37-27.1
mysql-community-server-bench-5.6.37-27.1
mysql-community-server-debugsource-5.6.37-27.1
mysql-community-server-tools-debuginfo-5.6.37-27.1
mysql-community-server-client-5.6.37-27.1
mysql-community-server-bench-debuginfo-5.6.37-27.1
mysql-community-server-test-debuginfo-5.6.37-27.1
libmysql56client_r18-32bit-5.6.37-27.1
mysql-community-server-client-debuginfo-5.6.37-27.1
libmysql56client18-debuginfo-5.6.37-27.1
mysql-community-server-test-5.6.37-27.1
mysql-community-server-tools-5.6.37-27.1

i586

libmysql56client_r18-5.6.37-27.1
mysql-community-server-debuginfo-5.6.37-27.1

mysql-community-server-5.6.37-27.1
mysql-community-server-errormessages-5.6.37-27.1
libmysql56client18-5.6.37-27.1
mysql-community-server-bench-5.6.37-27.1
mysql-community-server-debugsource-5.6.37-27.1
mysql-community-server-tools-debuginfo-5.6.37-27.1
mysql-community-server-client-5.6.37-27.1
mysql-community-server-bench-debuginfo-5.6.37-27.1
mysql-community-server-test-debuginfo-5.6.37-27.1
mysql-community-server-client-debuginfo-5.6.37-27.1
libmysql56client18-debuginfo-5.6.37-27.1
mysql-community-server-test-5.6.37-27.1
mysql-community-server-tools-5.6.37-27.1

145707 - SuSE Linux 42.2 openSUSE-SU-2017:1505-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9468, CVE-2017-9469

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1505-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00019.html>

SuSE Linux 42.2

x86_64

irssi-debugsource-1.0.3-14.7.1

irssi-debuginfo-1.0.3-14.7.1

irssi-1.0.3-14.7.1

irssi-devel-1.0.3-14.7.1

i586

irssi-debugsource-1.0.3-14.7.1

irssi-debuginfo-1.0.3-14.7.1

irssi-1.0.3-14.7.1

irssi-devel-1.0.3-14.7.1

145715 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2299-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:2299-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003169.html>

SuSE SLES 12 SP2

x86_64
expat-2.1.0-21.3.1
expat-debugsource-2.1.0-21.3.1
libexpat1-debuginfo-32bit-2.1.0-21.3.1
libexpat1-32bit-2.1.0-21.3.1
expat-debuginfo-2.1.0-21.3.1
libexpat1-debuginfo-2.1.0-21.3.1
expat-debuginfo-32bit-2.1.0-21.3.1
libexpat1-2.1.0-21.3.1

SuSE SLED 12 SP3

x86_64
libexpat1-debuginfo-32bit-2.1.0-21.3.1
expat-2.1.0-21.3.1
libexpat1-32bit-2.1.0-21.3.1
expat-debuginfo-2.1.0-21.3.1
expat-debugsource-2.1.0-21.3.1
expat-debuginfo-32bit-2.1.0-21.3.1
libexpat1-debuginfo-2.1.0-21.3.1
libexpat1-2.1.0-21.3.1

SuSE SLED 12 SP2

x86_64
libexpat1-debuginfo-32bit-2.1.0-21.3.1
expat-2.1.0-21.3.1
libexpat1-32bit-2.1.0-21.3.1
expat-debuginfo-2.1.0-21.3.1
expat-debugsource-2.1.0-21.3.1
expat-debuginfo-32bit-2.1.0-21.3.1
libexpat1-debuginfo-2.1.0-21.3.1
libexpat1-2.1.0-21.3.1

SuSE SLES 12 SP3

x86_64
expat-2.1.0-21.3.1
expat-debugsource-2.1.0-21.3.1
libexpat1-debuginfo-32bit-2.1.0-21.3.1
libexpat1-32bit-2.1.0-21.3.1
expat-debuginfo-2.1.0-21.3.1
libexpat1-debuginfo-2.1.0-21.3.1
expat-debuginfo-32bit-2.1.0-21.3.1
libexpat1-2.1.0-21.3.1

145716 - SuSE Linux 42.2 openSUSE-SU-2017:1638-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6329, CVE-2017-7478, CVE-2017-7479

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1638-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00077.html>

SuSE Linux 42.2

x86_64

openvpn-down-root-plugin-debuginfo-2.3.8-8.6.1

openvpn-debuginfo-2.3.8-8.6.1

openvpn-devel-2.3.8-8.6.1

openvpn-debugsource-2.3.8-8.6.1

openvpn-auth-pam-plugin-2.3.8-8.6.1

openvpn-2.3.8-8.6.1

openvpn-down-root-plugin-2.3.8-8.6.1

openvpn-auth-pam-plugin-debuginfo-2.3.8-8.6.1

i586

openvpn-down-root-plugin-debuginfo-2.3.8-8.6.1

openvpn-debuginfo-2.3.8-8.6.1

openvpn-devel-2.3.8-8.6.1

openvpn-debugsource-2.3.8-8.6.1

openvpn-auth-pam-plugin-2.3.8-8.6.1

openvpn-2.3.8-8.6.1

openvpn-down-root-plugin-2.3.8-8.6.1

openvpn-auth-pam-plugin-debuginfo-2.3.8-8.6.1

145718 - SuSE Linux 42.1 openSUSE-SU-2017:0574-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5837, CVE-2017-5839, CVE-2017-5842, CVE-2017-5844

Description

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

openSUSE-SU-2017:0574-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00117.html>

SuSE Linux 42.1

i586

libgsttag-1_0-0-1.4.5-8.1

libgstapp-1_0-0-debuginfo-1.4.5-8.1

gstreamer-plugins-base-1.4.5-8.1

libgsttriff-1_0-0-1.4.5-8.1

libgstaudio-1_0-0-1.4.5-8.1

libgsttag-1_0-0-debuginfo-1.4.5-8.1

typelib-1_0-GstRiff-1_0-1.4.5-8.1

typelib-1_0-GstApp-1_0-1.4.5-8.1

libgstvideo-1_0-0-debuginfo-1.4.5-8.1

gstreamer-plugins-base-debuginfo-1.4.5-8.1

libgstapp-1_0-0-1.4.5-8.1

libgstfft-1_0-0-debuginfo-1.4.5-8.1

typelib-1_0-GstAllocators-1_0-1.4.5-8.1

libgstvideo-1_0-0-1.4.5-8.1

libgstallocators-1_0-0-debuginfo-1.4.5-8.1
typelib-1_0-GstTag-1_0-1.4.5-8.1
libgstsdp-1_0-0-1.4.5-8.1
typelib-1_0-GstFft-1_0-1.4.5-8.1
libgstrtsp-1_0-0-1.4.5-8.1
typelib-1_0-GstSdp-1_0-1.4.5-8.1
libgstfft-1_0-0-1.4.5-8.1
libgstrtp-1_0-0-1.4.5-8.1
typelib-1_0-GstAudio-1_0-1.4.5-8.1
typelib-1_0-GstRtp-1_0-1.4.5-8.1
libgstallocators-1_0-0-1.4.5-8.1
gstreamer-plugins-base-devel-1.4.5-8.1
libgstrtsp-1_0-0-debuginfo-1.4.5-8.1
typelib-1_0-GstPbutils-1_0-1.4.5-8.1
libgstsdp-1_0-0-debuginfo-1.4.5-8.1
typelib-1_0-GstVideo-1_0-1.4.5-8.1
typelib-1_0-GstRtsp-1_0-1.4.5-8.1
libgstaudio-1_0-0-debuginfo-1.4.5-8.1
libgstpbutils-1_0-0-debuginfo-1.4.5-8.1
libgstriff-1_0-0-debuginfo-1.4.5-8.1
gstreamer-plugins-base-debugsource-1.4.5-8.1
libgstpbutils-1_0-0-1.4.5-8.1
libgstrtp-1_0-0-debuginfo-1.4.5-8.1
gstreamer-plugins-base-doc-1.4.5-8.1

noarch

gstreamer-plugins-base-lang-1.4.5-8.1

x86_64

libgsttag-1_0-0-1.4.5-8.1
libgstrtp-1_0-0-32bit-1.4.5-8.1
libgstapp-1_0-0-debuginfo-1.4.5-8.1
libgstaudio-1_0-0-32bit-1.4.5-8.1
libgstfft-1_0-0-32bit-1.4.5-8.1
gstreamer-plugins-base-1.4.5-8.1
libgstrtsp-1_0-0-debuginfo-32bit-1.4.5-8.1
libgstriff-1_0-0-1.4.5-8.1
libgstaudio-1_0-0-1.4.5-8.1
libgstvideo-1_0-0-debuginfo-32bit-1.4.5-8.1
libgsttag-1_0-0-debuginfo-1.4.5-8.1
typelib-1_0-GstRiff-1_0-1.4.5-8.1
typelib-1_0-GstApp-1_0-1.4.5-8.1
libgstallocators-1_0-0-debuginfo-32bit-1.4.5-8.1
gstreamer-plugins-base-debuginfo-32bit-1.4.5-8.1
libgstvideo-1_0-0-debuginfo-1.4.5-8.1
gstreamer-plugins-base-debuginfo-1.4.5-8.1
libgstapp-1_0-0-1.4.5-8.1
libgstfft-1_0-0-debuginfo-1.4.5-8.1
typelib-1_0-GstAllocators-1_0-1.4.5-8.1
libgstpbutils-1_0-0-debuginfo-32bit-1.4.5-8.1
libgstvideo-1_0-0-1.4.5-8.1
libgstallocators-1_0-0-debuginfo-1.4.5-8.1
gstreamer-plugins-base-32bit-1.4.5-8.1
libgstsdp-1_0-0-32bit-1.4.5-8.1
libgstapp-1_0-0-32bit-1.4.5-8.1
libgstvideo-1_0-0-32bit-1.4.5-8.1
typelib-1_0-GstTag-1_0-1.4.5-8.1
libgstsdp-1_0-0-1.4.5-8.1
typelib-1_0-GstFft-1_0-1.4.5-8.1
libgstriff-1_0-0-32bit-1.4.5-8.1

libgststrtp-1_0-0-1.4.5-8.1
typelib-1_0-GstSdp-1_0-1.4.5-8.1
libgstfft-1_0-0-1.4.5-8.1
libgststrtp-1_0-0-1.4.5-8.1
typelib-1_0-GstAudio-1_0-1.4.5-8.1
typelib-1_0-GstRtp-1_0-1.4.5-8.1
libgstallocators-1_0-0-1.4.5-8.1
libgsttag-1_0-0-debuginfo-32bit-1.4.5-8.1
libgstpbutils-1_0-0-32bit-1.4.5-8.1
libgststrtp-1_0-0-debuginfo-32bit-1.4.5-8.1
gstreamer-plugins-base-devel-1.4.5-8.1
libgststrtp-1_0-0-debuginfo-1.4.5-8.1
typelib-1_0-GstPbutils-1_0-1.4.5-8.1
libgstsdp-1_0-0-debuginfo-1.4.5-8.1
libgstfft-1_0-0-debuginfo-32bit-1.4.5-8.1
typelib-1_0-GstVideo-1_0-1.4.5-8.1
typelib-1_0-GstRtp-1_0-1.4.5-8.1
libgstaudio-1_0-0-debuginfo-1.4.5-8.1
libgstallocators-1_0-0-32bit-1.4.5-8.1
libgsttriff-1_0-0-debuginfo-32bit-1.4.5-8.1
libgststrtp-1_0-0-32bit-1.4.5-8.1
libgstapp-1_0-0-debuginfo-32bit-1.4.5-8.1
libgstpbutils-1_0-0-debuginfo-1.4.5-8.1
libgsttriff-1_0-0-debuginfo-1.4.5-8.1
gstreamer-plugins-base-debugsource-1.4.5-8.1
libgstsdp-1_0-0-debuginfo-32bit-1.4.5-8.1
libgstpbutils-1_0-0-1.4.5-8.1
libgstaudio-1_0-0-debuginfo-32bit-1.4.5-8.1
libgststrtp-1_0-0-debuginfo-1.4.5-8.1
libgsttag-1_0-0-32bit-1.4.5-8.1
gstreamer-plugins-base-doc-1.4.5-8.1

145736 - SuSE Linux 42.2 openSUSE-SU-2017:1031-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5838

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1031-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00058.html>

SuSE Linux 42.2

i586

gstreamer-1.8.3-2.3.1
gstreamer-debuginfo-1.8.3-2.3.1
gstreamer-devel-1.8.3-2.3.1
gstreamer-debugsource-1.8.3-2.3.1
gstreamer-doc-1.8.3-2.3.1
gstreamer-utils-debuginfo-1.8.3-2.3.1
libgstreamer-1_0-0-1.8.3-2.3.1
gstreamer-utils-1.8.3-2.3.1

libgstreamer-1_0-0-debuginfo-1.8.3-2.3.1
typelib-1_0-Gst-1_0-1.8.3-2.3.1

noarch
gstreamer-lang-1.8.3-2.3.1

x86_64
gstreamer-1.8.3-2.3.1
gstreamer-doc-1.8.3-2.3.1
gstreamer-debuginfo-1.8.3-2.3.1
gstreamer-32bit-1.8.3-2.3.1
typelib-1_0-Gst-1_0-1.8.3-2.3.1
gstreamer-utils-1.8.3-2.3.1
gstreamer-utils-debuginfo-1.8.3-2.3.1
libgstreamer-1_0-0-32bit-1.8.3-2.3.1
libgstreamer-1_0-0-debuginfo-32bit-1.8.3-2.3.1
gstreamer-debuginfo-32bit-1.8.3-2.3.1
libgstreamer-1_0-0-1.8.3-2.3.1
gstreamer-devel-1.8.3-2.3.1
libgstreamer-1_0-0-debuginfo-1.8.3-2.3.1
gstreamer-debugsource-1.8.3-2.3.1

145737 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2179-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000381, CVE-2017-11499

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2179-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00061.html>

SuSE Linux 42.2
i586
npm4-4.8.4-5.6.1
nodejs4-debugsource-4.8.4-5.6.1
nodejs4-devel-4.8.4-5.6.1
nodejs4-debuginfo-4.8.4-5.6.1
nodejs4-4.8.4-5.6.1

noarch
nodejs4-docs-4.8.4-5.6.1
nodejs-common-1.0-2.1

x86_64
npm4-4.8.4-5.6.1
nodejs4-debugsource-4.8.4-5.6.1
nodejs4-devel-4.8.4-5.6.1
nodejs4-debuginfo-4.8.4-5.6.1
nodejs4-4.8.4-5.6.1

SuSE Linux 42.3

i586
nodejs6-debuginfo-6.11.1-3.1
nodejs4-debugsource-4.8.4-8.1
npm6-6.11.1-3.1
nodejs4-debuginfo-4.8.4-8.1
nodejs6-6.11.1-3.1
nodejs4-devel-4.8.4-8.1
npm4-4.8.4-8.1
nodejs6-debugsource-6.11.1-3.1
nodejs4-4.8.4-8.1
nodejs6-devel-6.11.1-3.1

noarch
nodejs6-docs-6.11.1-3.1
nodejs4-docs-4.8.4-8.1
nodejs-common-1.0-2.1

x86_64
nodejs6-debuginfo-6.11.1-3.1
nodejs4-debugsource-4.8.4-8.1
npm6-6.11.1-3.1
nodejs4-debuginfo-4.8.4-8.1
nodejs6-6.11.1-3.1
nodejs4-devel-4.8.4-8.1
npm4-4.8.4-8.1
nodejs6-debugsource-6.11.1-3.1
nodejs4-4.8.4-8.1
nodejs6-devel-6.11.1-3.1

145750 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2336-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2336-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00004.html>

SuSE Linux 42.2
x86_64
libexpat-devel-2.1.0-21.3.1
libexpat1-debuginfo-32bit-2.1.0-21.3.1
expat-2.1.0-21.3.1
libexpat1-32bit-2.1.0-21.3.1
libexpat-devel-32bit-2.1.0-21.3.1
expat-debuginfo-2.1.0-21.3.1
expat-debugsource-2.1.0-21.3.1
expat-debuginfo-32bit-2.1.0-21.3.1
libexpat1-debuginfo-2.1.0-21.3.1
libexpat1-2.1.0-21.3.1

i586
libexpat-devel-2.1.0-21.3.1
expat-2.1.0-21.3.1
expat-debuginfo-2.1.0-21.3.1
expat-debugsource-2.1.0-21.3.1
libexpat1-debuginfo-2.1.0-21.3.1
libexpat1-2.1.0-21.3.1

SuSE Linux 42.3
x86_64
expat-debugsource-2.1.0-24.1
expat-debuginfo-2.1.0-24.1
libexpat1-32bit-2.1.0-24.1
libexpat-devel-32bit-2.1.0-24.1
libexpat1-2.1.0-24.1
libexpat1-debuginfo-2.1.0-24.1
libexpat-devel-2.1.0-24.1
libexpat1-debuginfo-32bit-2.1.0-24.1
expat-2.1.0-24.1
expat-debuginfo-32bit-2.1.0-24.1

i586
expat-debugsource-2.1.0-24.1
expat-debuginfo-2.1.0-24.1
libexpat1-2.1.0-24.1
libexpat1-debuginfo-2.1.0-24.1
libexpat-devel-2.1.0-24.1
expat-2.1.0-24.1

145753 - SuSE Linux 42.2 openSUSE-SU-2017:1772-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7484, CVE-2017-7485, CVE-2017-7486

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1772-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00016.html>

SuSE Linux 42.2
i586
postgresql94-devel-9.4.12-9.6.1
postgresql94-libs-debugsource-9.4.12-9.6.1
postgresql94-server-9.4.12-9.6.1
postgresql94-test-9.4.12-9.6.1
postgresql94-plpython-9.4.12-9.6.1
postgresql94-9.4.12-9.6.1
postgresql94-contrib-debuginfo-9.4.12-9.6.1
postgresql94-plperl-debuginfo-9.4.12-9.6.1
postgresql94-devel-debuginfo-9.4.12-9.6.1
postgresql94-server-debuginfo-9.4.12-9.6.1
postgresql94-plpython-debuginfo-9.4.12-9.6.1

postgresql94-contrib-9.4.12-9.6.1
postgresql94-plperl-9.4.12-9.6.1
postgresql94-pltcl-debuginfo-9.4.12-9.6.1
postgresql94-debuginfo-9.4.12-9.6.1
postgresql94-debugsource-9.4.12-9.6.1
postgresql94-pltcl-9.4.12-9.6.1

noarch
postgresql94-docs-9.4.12-9.6.1

x86_64
postgresql94-devel-9.4.12-9.6.1
postgresql94-libs-debugsource-9.4.12-9.6.1
postgresql94-server-9.4.12-9.6.1
postgresql94-test-9.4.12-9.6.1
postgresql94-plpython-9.4.12-9.6.1
postgresql94-9.4.12-9.6.1
postgresql94-contrib-debuginfo-9.4.12-9.6.1
postgresql94-plperl-debuginfo-9.4.12-9.6.1
postgresql94-devel-debuginfo-9.4.12-9.6.1
postgresql94-server-debuginfo-9.4.12-9.6.1
postgresql94-plpython-debuginfo-9.4.12-9.6.1
postgresql94-contrib-9.4.12-9.6.1
postgresql94-plperl-9.4.12-9.6.1
postgresql94-pltcl-debuginfo-9.4.12-9.6.1
postgresql94-debuginfo-9.4.12-9.6.1
postgresql94-debugsource-9.4.12-9.6.1
postgresql94-pltcl-9.4.12-9.6.1

145760 - SuSE Linux 42.2 openSUSE-SU-2017:1150-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8073

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1150-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00005.html>

SuSE Linux 42.2

i586
weechat-aspell-1.5-2.3.1
weechat-python-debuginfo-1.5-2.3.1
weechat-doc-1.5-2.3.1
weechat-python-1.5-2.3.1
weechat-debuginfo-1.5-2.3.1
weechat-guile-debuginfo-1.5-2.3.1
weechat-lua-debuginfo-1.5-2.3.1
weechat-ruby-debuginfo-1.5-2.3.1
weechat-ruby-1.5-2.3.1
weechat-devel-1.5-2.3.1
weechat-perl-1.5-2.3.1

weechat-tcl-debuginfo-1.5-2.3.1
weechat-perl-debuginfo-1.5-2.3.1
weechat-lua-1.5-2.3.1
weechat-debugsource-1.5-2.3.1
weechat-aspell-debuginfo-1.5-2.3.1
weechat-1.5-2.3.1
weechat-tcl-1.5-2.3.1
weechat-guile-1.5-2.3.1

noarch
weechat-lang-1.5-2.3.1

x86_64
weechat-aspell-1.5-2.3.1
weechat-python-debuginfo-1.5-2.3.1
weechat-doc-1.5-2.3.1
weechat-python-1.5-2.3.1
weechat-debuginfo-1.5-2.3.1
weechat-guile-debuginfo-1.5-2.3.1
weechat-lua-debuginfo-1.5-2.3.1
weechat-ruby-debuginfo-1.5-2.3.1
weechat-ruby-1.5-2.3.1
weechat-devel-1.5-2.3.1
weechat-perl-1.5-2.3.1
weechat-tcl-debuginfo-1.5-2.3.1
weechat-perl-debuginfo-1.5-2.3.1
weechat-lua-1.5-2.3.1
weechat-debugsource-1.5-2.3.1
weechat-aspell-debuginfo-1.5-2.3.1
weechat-1.5-2.3.1
weechat-tcl-1.5-2.3.1
weechat-guile-1.5-2.3.1

145773 - SuSE Linux 42.2 openSUSE-SU-2017:1857-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000381

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1857-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00059.html>

SuSE Linux 42.2
x86_64
libcares2-debuginfo-1.9.1-8.3.1
libcares2-debuginfo-32bit-1.9.1-8.3.1
libcares-devel-1.9.1-8.3.1
libcares2-1.9.1-8.3.1
libcares2-32bit-1.9.1-8.3.1
libcares2-debugsource-1.9.1-8.3.1

i586
libcares-devel-1.9.1-8.3.1
libcares2-1.9.1-8.3.1
libcares2-debuginfo-1.9.1-8.3.1
libcares2-debugsource-1.9.1-8.3.1

145784 - SuSE Linux 42.1 openSUSE-SU-2017:0925-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3695, CVE-2014-3696, CVE-2014-3698, CVE-2017-2640

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0925-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00013.html>

SuSE Linux 42.1

i586
libpurple-devel-2.10.11-9.1
libpurple-meanwhile-2.10.11-9.1
pidgin-debuginfo-2.10.11-9.1
libpurple-debuginfo-2.10.11-9.1
pidgin-debugsource-2.10.11-9.1
pidgin-2.10.11-9.1
libpurple-2.10.11-9.1
finch-2.10.11-9.1
pidgin-devel-2.10.11-9.1
finch-devel-2.10.11-9.1
libpurple-tcl-2.10.11-9.1
finch-debuginfo-2.10.11-9.1
libpurple-meanwhile-debuginfo-2.10.11-9.1
libpurple-tcl-debuginfo-2.10.11-9.1

noarch

libpurple-lang-2.10.11-9.1
libpurple-branding-upstream-2.10.11-9.1

x86_64

libpurple-devel-2.10.11-9.1
libpurple-meanwhile-2.10.11-9.1
pidgin-debuginfo-2.10.11-9.1
libpurple-debuginfo-2.10.11-9.1
pidgin-debugsource-2.10.11-9.1
pidgin-2.10.11-9.1
libpurple-2.10.11-9.1
finch-2.10.11-9.1
pidgin-devel-2.10.11-9.1
finch-devel-2.10.11-9.1
libpurple-tcl-2.10.11-9.1
finch-debuginfo-2.10.11-9.1
libpurple-meanwhile-debuginfo-2.10.11-9.1
libpurple-tcl-debuginfo-2.10.11-9.1

145791 - SuSE Linux 42.2 openSUSE-SU-2017:2003-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7529

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2003-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00109.html>

SuSE Linux 42.2
x86_64
nginx-1.8.1-10.5.1
nginx-debuginfo-1.8.1-10.5.1
nginx-debugsource-1.8.1-10.5.1

i586
nginx-1.8.1-10.5.1
nginx-debuginfo-1.8.1-10.5.1
nginx-debugsource-1.8.1-10.5.1

145797 - SuSE Linux 42.2 openSUSE-SU-2017:0897-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0897-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00117.html>

SuSE Linux 42.2
i586
apache2-utils-debuginfo-2.4.23-8.3.1
apache2-worker-debuginfo-2.4.23-8.3.1
apache2-example-pages-2.4.23-8.3.1
apache2-devel-2.4.23-8.3.1
apache2-2.4.23-8.3.1
apache2-debugsource-2.4.23-8.3.1
apache2-event-2.4.23-8.3.1
apache2-utils-2.4.23-8.3.1
apache2-prefork-debuginfo-2.4.23-8.3.1
apache2-debuginfo-2.4.23-8.3.1

apache2-prefork-2.4.23-8.3.1
apache2-event-debuginfo-2.4.23-8.3.1
apache2-worker-2.4.23-8.3.1

noarch
apache2-doc-2.4.23-8.3.1

x86_64
apache2-utils-debuginfo-2.4.23-8.3.1
apache2-worker-debuginfo-2.4.23-8.3.1
apache2-example-pages-2.4.23-8.3.1
apache2-devel-2.4.23-8.3.1
apache2-2.4.23-8.3.1
apache2-debugsource-2.4.23-8.3.1
apache2-event-2.4.23-8.3.1
apache2-utils-2.4.23-8.3.1
apache2-prefork-debuginfo-2.4.23-8.3.1
apache2-debuginfo-2.4.23-8.3.1
apache2-prefork-2.4.23-8.3.1
apache2-event-debuginfo-2.4.23-8.3.1
apache2-worker-2.4.23-8.3.1

145800 - SuSE Linux 42.2 openSUSE-SU-2017:1475-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-3302, CVE-2017-3313

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1475-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00001.html>

SuSE Linux 42.2

x86_64
mariadb-client-10.0.30-20.4.1
mariadb-debugsource-10.0.30-20.4.1
mariadb-bench-10.0.30-20.4.1
mariadb-debuginfo-10.0.30-20.4.1
mariadb-10.0.30-20.4.1
mariadb-client-debuginfo-10.0.30-20.4.1
mariadb-tools-debuginfo-10.0.30-20.4.1
mariadb-tools-10.0.30-20.4.1
libmysqlclient18-debuginfo-32bit-10.0.30-20.4.1
mariadb-errormessages-10.0.30-20.4.1
libmysqlclient-devel-10.0.30-20.4.1
libmysqld18-debuginfo-10.0.30-20.4.1
mariadb-test-10.0.30-20.4.1
libmysqlclient18-10.0.30-20.4.1
libmysqlclient18-32bit-10.0.30-20.4.1
libmysqlclient_r18-10.0.30-20.4.1
libmysqlclient18-debuginfo-10.0.30-20.4.1
mariadb-test-debuginfo-10.0.30-20.4.1

libmysqld18-10.0.30-20.4.1
libmysqlclient_r18-32bit-10.0.30-20.4.1
libmysqld-devel-10.0.30-20.4.1
mariadb-bench-debuginfo-10.0.30-20.4.1

i586

mariadb-client-10.0.30-20.4.1
mariadb-debugsource-10.0.30-20.4.1
mariadb-bench-10.0.30-20.4.1
mariadb-debuginfo-10.0.30-20.4.1
mariadb-10.0.30-20.4.1
mariadb-client-debuginfo-10.0.30-20.4.1
mariadb-tools-debuginfo-10.0.30-20.4.1
mariadb-tools-10.0.30-20.4.1
mariadb-errormessages-10.0.30-20.4.1
libmysqlclient-devel-10.0.30-20.4.1
libmysqld18-debuginfo-10.0.30-20.4.1
mariadb-test-10.0.30-20.4.1
libmysqlclient18-10.0.30-20.4.1
libmysqlclient_r18-10.0.30-20.4.1
libmysqlclient18-debuginfo-10.0.30-20.4.1
mariadb-test-debuginfo-10.0.30-20.4.1
libmysqld18-10.0.30-20.4.1
libmysqld-devel-10.0.30-20.4.1
mariadb-bench-debuginfo-10.0.30-20.4.1

145802 - SuSE Linux 42.2 openSUSE-SU-2017:1533-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6489

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1533-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00032.html>

SuSE Linux 42.2

x86_64

libhogweed2-debuginfo-32bit-2.7.1-10.3.1
libhogweed2-debuginfo-2.7.1-10.3.1
libnettle-debugsource-2.7.1-10.3.1
nettle-debuginfo-2.7.1-10.3.1
libnettle4-2.7.1-10.3.1
libnettle-devel-2.7.1-10.3.1
libnettle4-debuginfo-32bit-2.7.1-10.3.1
libnettle4-debuginfo-2.7.1-10.3.1
nettle-2.7.1-10.3.1
libnettle-devel-32bit-2.7.1-10.3.1
libhogweed2-2.7.1-10.3.1
libnettle4-32bit-2.7.1-10.3.1
libhogweed2-32bit-2.7.1-10.3.1

i586
libhogweed2-debuginfo-2.7.1-10.3.1
libnettle4-debuginfo-2.7.1-10.3.1
libhogweed2-2.7.1-10.3.1
nettle-2.7.1-10.3.1
libnettle-debugsource-2.7.1-10.3.1
libnettle4-2.7.1-10.3.1
libnettle-devel-2.7.1-10.3.1
nettle-debuginfo-2.7.1-10.3.1

145813 - SuSE Linux 42.2 openSUSE-SU-2017:1106-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5837, CVE-2017-5839, CVE-2017-5842, CVE-2017-5844

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1106-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00095.html>

SuSE Linux 42.2

i586
libgstsd-1_0-0-1.8.3-5.3.2
gststreamer-plugins-base-1.8.3-5.3.2
libgstvideo-1_0-0-1.8.3-5.3.2
libgstpbutils-1_0-0-1.8.3-5.3.2
typelib-1_0-GstAllocators-1_0-1.8.3-5.3.2
libgstaudio-1_0-0-1.8.3-5.3.2
typelib-1_0-GstFft-1_0-1.8.3-5.3.2
libgstallocators-1_0-0-debuginfo-1.8.3-5.3.2
libgstsd-1_0-0-debuginfo-1.8.3-5.3.2
gststreamer-plugins-base-devel-1.8.3-5.3.2
libgstfft-1_0-0-debuginfo-1.8.3-5.3.2
libgststrtp-1_0-0-debuginfo-1.8.3-5.3.2
gststreamer-plugins-base-debuginfo-1.8.3-5.3.2
typelib-1_0-GstAudio-1_0-1.8.3-5.3.2
libgstfft-1_0-0-1.8.3-5.3.2
typelib-1_0-GstVideo-1_0-1.8.3-5.3.2
gststreamer-plugins-base-debugsource-1.8.3-5.3.2
libgstapp-1_0-0-1.8.3-5.3.2
libgstallocators-1_0-0-1.8.3-5.3.2
libgstvideo-1_0-0-debuginfo-1.8.3-5.3.2
libgstpbutils-1_0-0-debuginfo-1.8.3-5.3.2
typelib-1_0-GstTag-1_0-1.8.3-5.3.2
typelib-1_0-GstApp-1_0-1.8.3-5.3.2
typelib-1_0-GstSdp-1_0-1.8.3-5.3.2
libgsttriff-1_0-0-1.8.3-5.3.2
libgsttag-1_0-0-1.8.3-5.3.2
libgststrtp-1_0-0-1.8.3-5.3.2
typelib-1_0-GstRtsp-1_0-1.8.3-5.3.2
libgststrtp-1_0-0-1.8.3-5.3.2
libgstapp-1_0-0-debuginfo-1.8.3-5.3.2

gstreamer-plugins-base-doc-1.8.3-5.3.2
typelib-1_0-GstPbutils-1_0-1.8.3-5.3.2
libgsttag-1_0-0-debuginfo-1.8.3-5.3.2
typelib-1_0-GstRtp-1_0-1.8.3-5.3.2
libgstrtp-1_0-0-debuginfo-1.8.3-5.3.2
libgstaudio-1_0-0-debuginfo-1.8.3-5.3.2
libgstriff-1_0-0-debuginfo-1.8.3-5.3.2

noarch
gstreamer-plugins-base-lang-1.8.3-5.3.2

x86_64
libgstsd-1_0-0-1.8.3-5.3.2
libgstvideo-1_0-0-32bit-1.8.3-5.3.2
libgstrtp-1_0-0-32bit-1.8.3-5.3.2
libgstsd-1_0-0-debuginfo-32bit-1.8.3-5.3.2
gstreamer-plugins-base-1.8.3-5.3.2
libgstsd-1_0-0-32bit-1.8.3-5.3.2
libgstaudio-1_0-0-debuginfo-32bit-1.8.3-5.3.2
libgstvideo-1_0-0-1.8.3-5.3.2
libgstallocators-1_0-0-debuginfo-32bit-1.8.3-5.3.2
libgstpbutils-1_0-0-1.8.3-5.3.2
libgstvideo-1_0-0-debuginfo-32bit-1.8.3-5.3.2
typelib-1_0-GstAllocators-1_0-1.8.3-5.3.2
libgstaudio-1_0-0-1.8.3-5.3.2
typelib-1_0-GstFft-1_0-1.8.3-5.3.2
libgstrtp-1_0-0-debuginfo-32bit-1.8.3-5.3.2
libgstallocators-1_0-0-debuginfo-1.8.3-5.3.2
gstreamer-plugins-base-debuginfo-32bit-1.8.3-5.3.2
gstreamer-plugins-base-32bit-1.8.3-5.3.2
libgstsd-1_0-0-debuginfo-1.8.3-5.3.2
gstreamer-plugins-base-devel-1.8.3-5.3.2
libgstriff-1_0-0-32bit-1.8.3-5.3.2
libgstpbutils-1_0-0-debuginfo-32bit-1.8.3-5.3.2
libgstaudio-1_0-0-32bit-1.8.3-5.3.2
libgstfft-1_0-0-debuginfo-1.8.3-5.3.2
libgstrtp-1_0-0-debuginfo-1.8.3-5.3.2
gstreamer-plugins-base-debuginfo-1.8.3-5.3.2
typelib-1_0-GstAudio-1_0-1.8.3-5.3.2
libgstfft-1_0-0-1.8.3-5.3.2
libgstapp-1_0-0-debuginfo-32bit-1.8.3-5.3.2
typelib-1_0-GstVideo-1_0-1.8.3-5.3.2
gstreamer-plugins-base-debugsource-1.8.3-5.3.2
libgstapp-1_0-0-1.8.3-5.3.2
libgstallocators-1_0-0-1.8.3-5.3.2
libgstfft-1_0-0-debuginfo-32bit-1.8.3-5.3.2
libgstvideo-1_0-0-debuginfo-1.8.3-5.3.2
libgstpbutils-1_0-0-debuginfo-1.8.3-5.3.2
typelib-1_0-GstTag-1_0-1.8.3-5.3.2
typelib-1_0-GstApp-1_0-1.8.3-5.3.2
typelib-1_0-GstSdp-1_0-1.8.3-5.3.2
libgsttag-1_0-0-32bit-1.8.3-5.3.2
gstreamer-plugins-base-devel-32bit-1.8.3-5.3.2
libgstriff-1_0-0-1.8.3-5.3.2
libgsttag-1_0-0-1.8.3-5.3.2
libgstrtp-1_0-0-debuginfo-32bit-1.8.3-5.3.2
libgstrtp-1_0-0-1.8.3-5.3.2
libgstriff-1_0-0-debuginfo-32bit-1.8.3-5.3.2
typelib-1_0-GstRtp-1_0-1.8.3-5.3.2
libgstallocators-1_0-0-32bit-1.8.3-5.3.2

libgstrtsp-1_0-0-1.8.3-5.3.2
libgsttag-1_0-0-debuginfo-32bit-1.8.3-5.3.2
libgstapp-1_0-0-debuginfo-1.8.3-5.3.2
gstreamer-plugins-base-doc-1.8.3-5.3.2
typelib-1_0-GstPbutils-1_0-1.8.3-5.3.2
libgstapp-1_0-0-32bit-1.8.3-5.3.2
libgsttag-1_0-0-debuginfo-1.8.3-5.3.2
typelib-1_0-GstRtp-1_0-1.8.3-5.3.2
libgstpbutils-1_0-0-32bit-1.8.3-5.3.2
libgstrtp-1_0-0-debuginfo-1.8.3-5.3.2
libgstrtsp-1_0-0-32bit-1.8.3-5.3.2
libgstaudio-1_0-0-debuginfo-1.8.3-5.3.2
libgstfft-1_0-0-32bit-1.8.3-5.3.2
libgstriff-1_0-0-debuginfo-1.8.3-5.3.2

145814 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0193-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9131, CVE-2016-9147, CVE-2016-9444

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:0193-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00108.html>

SuSE Linux 42.1

i586

bind-libs-9.9.9P1-45.1
bind-utils-debuginfo-9.9.9P1-45.1
bind-chrootenv-9.9.9P1-45.1
bind-debugsource-9.9.9P1-45.1
bind-debuginfo-9.9.9P1-45.1
bind-lwresd-9.9.9P1-45.1
bind-devel-9.9.9P1-45.1
bind-9.9.9P1-45.1
bind-utils-9.9.9P1-45.1
bind-libs-debuginfo-9.9.9P1-45.1
bind-lwresd-debuginfo-9.9.9P1-45.1

noarch

bind-doc-9.9.9P1-45.1

x86_64

bind-utils-9.9.9P1-45.1
bind-libs-debuginfo-9.9.9P1-45.1
bind-devel-9.9.9P1-45.1
bind-debugsource-9.9.9P1-45.1
bind-libs-9.9.9P1-45.1
bind-9.9.9P1-45.1
bind-lwresd-debuginfo-9.9.9P1-45.1
bind-utils-debuginfo-9.9.9P1-45.1
bind-libs-32bit-9.9.9P1-45.1

bind-debuginfo-9.9.9P1-45.1
bind-chrootenv-9.9.9P1-45.1
bind-libs-debuginfo-32bit-9.9.9P1-45.1
bind-lwresd-9.9.9P1-45.1

SuSE Linux 42.2

i586

bind-debuginfo-9.9.9P1-43.1
bind-utils-9.9.9P1-43.1
bind-9.9.9P1-43.1
bind-debugsource-9.9.9P1-43.1
bind-chrootenv-9.9.9P1-43.1
bind-lwresd-debuginfo-9.9.9P1-43.1
bind-lwresd-9.9.9P1-43.1
bind-libs-debuginfo-9.9.9P1-43.1
bind-utils-debuginfo-9.9.9P1-43.1
bind-libs-9.9.9P1-43.1
bind-devel-9.9.9P1-43.1

noarch

bind-doc-9.9.9P1-43.1

x86_64

bind-debuginfo-9.9.9P1-43.1
bind-lwresd-debuginfo-9.9.9P1-43.1
bind-libs-32bit-9.9.9P1-43.1
bind-9.9.9P1-43.1
bind-libs-debuginfo-32bit-9.9.9P1-43.1
bind-utils-debuginfo-9.9.9P1-43.1
bind-utils-9.9.9P1-43.1
bind-lwresd-9.9.9P1-43.1
bind-libs-debuginfo-9.9.9P1-43.1
bind-devel-9.9.9P1-43.1
bind-libs-9.9.9P1-43.1
bind-chrootenv-9.9.9P1-43.1
bind-debugsource-9.9.9P1-43.1

145818 - SuSE Linux 42.2 openSUSE-SU-2017:1680-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-7508, CVE-2017-7520, CVE-2017-7521

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1680-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00093.html>

SuSE Linux 42.2

x86_64

openvpn-down-root-plugin-2.3.8-8.10.1
openvpn-auth-pam-plugin-2.3.8-8.10.1
openvpn-2.3.8-8.10.1

openvpn-auth-pam-plugin-debuginfo-2.3.8-8.10.1
openvpn-debuginfo-2.3.8-8.10.1
openvpn-debugsource-2.3.8-8.10.1
openvpn-down-root-plugin-debuginfo-2.3.8-8.10.1
openvpn-devel-2.3.8-8.10.1

i586

openvpn-down-root-plugin-2.3.8-8.10.1
openvpn-auth-pam-plugin-2.3.8-8.10.1
openvpn-2.3.8-8.10.1
openvpn-auth-pam-plugin-debuginfo-2.3.8-8.10.1
openvpn-debuginfo-2.3.8-8.10.1
openvpn-debugsource-2.3.8-8.10.1
openvpn-down-root-plugin-debuginfo-2.3.8-8.10.1
openvpn-devel-2.3.8-8.10.1

145830 - SuSE Linux 42.1 openSUSE-SU-2017:0223-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-9749, CVE-2016-10002

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0223-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00124.html>

SuSE Linux 42.1

x86_64

squid-debugsource-3.3.14-12.1
squid-debuginfo-3.3.14-12.1
squid-3.3.14-12.1

i586

squid-debugsource-3.3.14-12.1
squid-debuginfo-3.3.14-12.1
squid-3.3.14-12.1

145833 - SuSE Linux 42.1 openSUSE-SU-2017:1076-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10198, CVE-2016-10199, CVE-2017-5840, CVE-2017-5841, CVE-2017-5845

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1076-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00081.html>

SuSE Linux 42.1

i586

gststreamer-plugins-good-debugsource-1.4.5-8.1
gststreamer-plugins-good-doc-1.4.5-8.1
gststreamer-plugins-good-extra-debuginfo-1.4.5-8.1
gststreamer-plugins-good-debuginfo-1.4.5-8.1
gststreamer-plugins-good-extra-1.4.5-8.1
gststreamer-plugins-good-1.4.5-8.1

noarch

gststreamer-plugins-good-lang-1.4.5-8.1

x86_64

gststreamer-plugins-good-debugsource-1.4.5-8.1
gststreamer-plugins-good-extra-32bit-1.4.5-8.1
gststreamer-plugins-good-doc-1.4.5-8.1
gststreamer-plugins-good-extra-debuginfo-32bit-1.4.5-8.1
gststreamer-plugins-good-extra-debuginfo-1.4.5-8.1
gststreamer-plugins-good-32bit-1.4.5-8.1
gststreamer-plugins-good-debuginfo-1.4.5-8.1
gststreamer-plugins-good-extra-1.4.5-8.1
gststreamer-plugins-good-1.4.5-8.1
gststreamer-plugins-good-debuginfo-32bit-1.4.5-8.1

145836 - SuSE Linux 42.2 openSUSE-SU-2017:1612-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:1612-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00071.html>

SuSE Linux 42.2

i586

libxml2-2-2.9.4-5.6.1
python-libxml2-2.9.4-5.6.1
libxml2-2-debuginfo-2.9.4-5.6.1
libxml2-debugsource-2.9.4-5.6.1
python-libxml2-debugsource-2.9.4-5.6.1
libxml2-tools-2.9.4-5.6.1
libxml2-devel-2.9.4-5.6.1
python-libxml2-debuginfo-2.9.4-5.6.1
libxml2-tools-debuginfo-2.9.4-5.6.1

noarch

libxml2-doc-2.9.4-5.6.1

x86_64
libxml2-2-2.9.4-5.6.1
libxml2-devel-32bit-2.9.4-5.6.1
libxml2-2-32bit-2.9.4-5.6.1
python-libxml2-2.9.4-5.6.1
libxml2-2-debuginfo-2.9.4-5.6.1
libxml2-debugsource-2.9.4-5.6.1
python-libxml2-debugsource-2.9.4-5.6.1
libxml2-tools-2.9.4-5.6.1
libxml2-devel-2.9.4-5.6.1
python-libxml2-debuginfo-2.9.4-5.6.1
libxml2-2-debuginfo-32bit-2.9.4-5.6.1
libxml2-tools-debuginfo-2.9.4-5.6.1

145844 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0667-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9181

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0667-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00028.html>

SuSE Linux 42.1
noarch
perl-Image-Info-1.39-4.1

SuSE Linux 42.2
noarch
perl-Image-Info-1.39-5.1

145871 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0482-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-8605

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0482-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00070.html>

SuSE Linux 42.1
x86_64

libguilereadline-v-18-18-debuginfo-2.0.9-7.1
guile-devel-2.0.9-7.1
guile-debuginfo-2.0.9-7.1
libguilereadline-v-18-18-2.0.9-7.1
guile-modules-2_0-2.0.9-7.1
libguile-2_0-22-2.0.9-7.1
libguile-2_0-22-debuginfo-2.0.9-7.1
guile-2.0.9-7.1
guile-debugsource-2.0.9-7.1

i586

libguilereadline-v-18-18-debuginfo-2.0.9-7.1
guile-devel-2.0.9-7.1
guile-debuginfo-2.0.9-7.1
libguilereadline-v-18-18-2.0.9-7.1
guile-modules-2_0-2.0.9-7.1
libguile-2_0-22-2.0.9-7.1
libguile-2_0-22-debuginfo-2.0.9-7.1
guile-2.0.9-7.1
guile-debugsource-2.0.9-7.1

SuSE Linux 42.2

x86_64

guile-modules-2_0-2.0.9-8.1
guile-debugsource-2.0.9-8.1
libguilereadline-v-18-18-2.0.9-8.1
guile-2.0.9-8.1
guile-debuginfo-2.0.9-8.1
guile-devel-2.0.9-8.1
libguilereadline-v-18-18-debuginfo-2.0.9-8.1
libguile-2_0-22-2.0.9-8.1
libguile-2_0-22-debuginfo-2.0.9-8.1

i586

guile-modules-2_0-2.0.9-8.1
guile-debugsource-2.0.9-8.1
libguilereadline-v-18-18-2.0.9-8.1
guile-2.0.9-8.1
guile-debuginfo-2.0.9-8.1
guile-devel-2.0.9-8.1
libguilereadline-v-18-18-debuginfo-2.0.9-8.1
libguile-2_0-22-2.0.9-8.1
libguile-2_0-22-debuginfo-2.0.9-8.1

145876 - SuSE Linux 42.2 openSUSE-SU-2017:0994-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2007-3126

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:0994-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00046.html>

SuSE Linux 42.2

i586

libgimpui-2_0-0-2.8.18-2.3.1

gimp-2.8.18-2.3.1

gimp-help-browser-2.8.18-2.3.1

libgimpui-2_0-0-debuginfo-2.8.18-2.3.1

gimp-devel-2.8.18-2.3.1

gimp-help-browser-debuginfo-2.8.18-2.3.1

gimp-devel-debuginfo-2.8.18-2.3.1

gimp-plugin-aa-debuginfo-2.8.18-2.3.1

gimp-debugsource-2.8.18-2.3.1

gimp-plugin-aa-2.8.18-2.3.1

libgimp-2_0-0-2.8.18-2.3.1

gimp-plugins-python-debuginfo-2.8.18-2.3.1

gimp-plugins-python-2.8.18-2.3.1

gimp-debuginfo-2.8.18-2.3.1

libgimp-2_0-0-debuginfo-2.8.18-2.3.1

noarch

gimp-lang-2.8.18-2.3.1

x86_64

libgimpui-2_0-0-2.8.18-2.3.1

gimp-2.8.18-2.3.1

gimp-help-browser-2.8.18-2.3.1

libgimpui-2_0-0-32bit-2.8.18-2.3.1

libgimpui-2_0-0-debuginfo-2.8.18-2.3.1

gimp-devel-2.8.18-2.3.1

gimp-help-browser-debuginfo-2.8.18-2.3.1

gimp-devel-debuginfo-2.8.18-2.3.1

gimp-plugin-aa-debuginfo-2.8.18-2.3.1

gimp-debugsource-2.8.18-2.3.1

libgimp-2_0-0-debuginfo-32bit-2.8.18-2.3.1

gimp-plugin-aa-2.8.18-2.3.1

libgimpui-2_0-0-debuginfo-32bit-2.8.18-2.3.1

libgimp-2_0-0-32bit-2.8.18-2.3.1

libgimp-2_0-0-2.8.18-2.3.1

gimp-plugins-python-debuginfo-2.8.18-2.3.1

gimp-plugins-python-2.8.18-2.3.1

gimp-debuginfo-2.8.18-2.3.1

libgimp-2_0-0-debuginfo-2.8.18-2.3.1

145879 - SuSE Linux 42.2 openSUSE-SU-2017:0297-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-8740

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:0297-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00149.html>

SuSE Linux 42.2

i586

apache2-prefork-debuginfo-2.4.23-6.1

apache2-devel-2.4.23-6.1

apache2-debuginfo-2.4.23-6.1

apache2-event-debuginfo-2.4.23-6.1

apache2-event-2.4.23-6.1

apache2-utils-2.4.23-6.1

apache2-debugsource-2.4.23-6.1

apache2-utils-debuginfo-2.4.23-6.1

apache2-worker-2.4.23-6.1

apache2-worker-debuginfo-2.4.23-6.1

apache2-prefork-2.4.23-6.1

apache2-2.4.23-6.1

apache2-example-pages-2.4.23-6.1

noarch

apache2-doc-2.4.23-6.1

x86_64

apache2-prefork-debuginfo-2.4.23-6.1

apache2-devel-2.4.23-6.1

apache2-debuginfo-2.4.23-6.1

apache2-event-debuginfo-2.4.23-6.1

apache2-event-2.4.23-6.1

apache2-utils-2.4.23-6.1

apache2-debugsource-2.4.23-6.1

apache2-utils-debuginfo-2.4.23-6.1

apache2-worker-2.4.23-6.1

apache2-worker-debuginfo-2.4.23-6.1

apache2-prefork-2.4.23-6.1

apache2-2.4.23-6.1

apache2-example-pages-2.4.23-6.1

145881 - SuSE Linux 42.2 openSUSE-SU-2017:1875-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-7507, CVE-2017-7869

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:1875-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00064.html>

SuSE Linux 42.2

x86_64

gnutls-3.2.15-11.3.1

libgnutls-openssl27-debuginfo-3.2.15-11.3.1

libgnutls28-debuginfo-3.2.15-11.3.1

libgnutls-openssl-devel-3.2.15-11.3.1

libgnutls28-3.2.15-11.3.1
gnutls-debuginfo-3.2.15-11.3.1
libgnutls-devel-3.2.15-11.3.1
libgnutls-openssl27-3.2.15-11.3.1
libgnutls28-debuginfo-32bit-3.2.15-11.3.1
libgnutls28-32bit-3.2.15-11.3.1
libgnutlsxx28-3.2.15-11.3.1
gnutls-debugsource-3.2.15-11.3.1
libgnutls-devel-32bit-3.2.15-11.3.1
libgnutlsxx-devel-3.2.15-11.3.1
libgnutlsxx28-debuginfo-3.2.15-11.3.1

i586

libgnutls-devel-3.2.15-11.3.1
libgnutlsxx28-debuginfo-3.2.15-11.3.1
libgnutls-openssl27-3.2.15-11.3.1
gnutls-3.2.15-11.3.1
libgnutls-openssl-devel-3.2.15-11.3.1
libgnutlsxx-devel-3.2.15-11.3.1
libgnutls28-debuginfo-3.2.15-11.3.1
gnutls-debuginfo-3.2.15-11.3.1
libgnutlsxx28-3.2.15-11.3.1
gnutls-debugsource-3.2.15-11.3.1
libgnutls28-3.2.15-11.3.1
libgnutls-openssl27-debuginfo-3.2.15-11.3.1

145888 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0937-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10087

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0937-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00022.html>

SuSE Linux 42.1

x86_64

libpng16-16-debuginfo-32bit-1.6.8-10.1
libpng16-tools-debuginfo-1.6.8-10.1
libpng16-tools-1.6.8-10.1
libpng16-devel-32bit-1.6.8-10.1
libpng16-compatible-devel-32bit-1.6.8-10.1
libpng16-16-debuginfo-1.6.8-10.1
libpng16-16-32bit-1.6.8-10.1
libpng16-compatible-devel-1.6.8-10.1
libpng16-debugsource-1.6.8-10.1
libpng16-16-1.6.8-10.1
libpng16-devel-1.6.8-10.1

i586

libpng16-tools-debuginfo-1.6.8-10.1

libpng16-tools-1.6.8-10.1
libpng16-16-debuginfo-1.6.8-10.1
libpng16-compat-devel-1.6.8-10.1
libpng16-debugsource-1.6.8-10.1
libpng16-16-1.6.8-10.1
libpng16-devel-1.6.8-10.1

SuSE Linux 42.2

x86_64

libpng16-tools-debuginfo-1.6.8-9.3.1
libpng16-devel-32bit-1.6.8-9.3.1
libpng16-compat-devel-1.6.8-9.3.1
libpng16-16-debuginfo-1.6.8-9.3.1
libpng16-16-1.6.8-9.3.1
libpng16-devel-1.6.8-9.3.1
libpng16-tools-1.6.8-9.3.1
libpng16-16-32bit-1.6.8-9.3.1
libpng16-compat-devel-32bit-1.6.8-9.3.1
libpng16-16-debuginfo-32bit-1.6.8-9.3.1
libpng16-debugsource-1.6.8-9.3.1

i586

libpng16-tools-debuginfo-1.6.8-9.3.1
libpng16-compat-devel-1.6.8-9.3.1
libpng16-16-debuginfo-1.6.8-9.3.1
libpng16-16-1.6.8-9.3.1
libpng16-devel-1.6.8-9.3.1
libpng16-tools-1.6.8-9.3.1
libpng16-debugsource-1.6.8-9.3.1

145899 - SuSE Linux 42.2 openSUSE-SU-2017:1569-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-0375, CVE-2017-0376

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1569-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00047.html>

SuSE Linux 42.2

x86_64

tor-debuginfo-0.2.9.11-8.3.1
tor-debugsource-0.2.9.11-8.3.1
tor-0.2.9.11-8.3.1

i586

tor-debuginfo-0.2.9.11-8.3.1
tor-debugsource-0.2.9.11-8.3.1
tor-0.2.9.11-8.3.1

160293 - CentOS 6 CESA-2017-2550 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2550

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.centos.org/pipermail/centos-announce/2017-August/022527.html>

CentOS 6

x86_64

poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-qt-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9

i686

poppler-devel-0.12.4-12.el6_9
poppler-qt-0.12.4-12.el6_9
poppler-qt4-devel-0.12.4-12.el6_9
poppler-glib-devel-0.12.4-12.el6_9
poppler-utils-0.12.4-12.el6_9
poppler-qt4-0.12.4-12.el6_9
poppler-0.12.4-12.el6_9
poppler-qt-devel-0.12.4-12.el6_9
poppler-glib-0.12.4-12.el6_9

160294 - CentOS 6 CESA-2017-2563 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
CESA-2017-2563

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.centos.org/pipermail/centos-announce/2017-August/022529.html>

CentOS 6

x86_64
openssh-5.3p1-123.el6_9
openssh-server-5.3p1-123.el6_9
pam_ssh_agent_auth-0.9.3-123.el6_9
openssh-askpass-5.3p1-123.el6_9
openssh-ldap-5.3p1-123.el6_9
openssh-clients-5.3p1-123.el6_9

i686
openssh-5.3p1-123.el6_9
openssh-server-5.3p1-123.el6_9
pam_ssh_agent_auth-0.9.3-123.el6_9
openssh-askpass-5.3p1-123.el6_9
openssh-ldap-5.3p1-123.el6_9
openssh-clients-5.3p1-123.el6_9

163450 - Oracle Enterprise Linux ELSA-2017-2569 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-7551

Description

The scan detected that the host is missing the following update:
ELSA-2017-2569

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-September/007177.html>

OEL7
x86_64
389-ds-base-devel-1.3.6.1-19.el7_4
389-ds-base-1.3.6.1-19.el7_4
389-ds-base-libs-1.3.6.1-19.el7_4
389-ds-base-snmp-1.3.6.1-19.el7_4

170855 - Amazon Linux AMI ALAS-2017-889 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000099, CVE-2017-1000100, CVE-2017-1000101

Description

The scan detected that the host is missing the following update:
ALAS-2017-889

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://alas.aws.amazon.com/ALAS-2017-889.html>

Amazon Linux AMI

x86_64
libcurl-7.51.0-9.75.amzn1
curl-debuginfo-7.51.0-9.75.amzn1
libcurl-devel-7.51.0-9.75.amzn1
curl-7.51.0-9.75.amzn1

i686
libcurl-7.51.0-9.75.amzn1
curl-debuginfo-7.51.0-9.75.amzn1
libcurl-devel-7.51.0-9.75.amzn1
curl-7.51.0-9.75.amzn1

170856 - Amazon Linux AMI ALAS-2017-888 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-3633, CVE-2017-3634, CVE-2017-3635, CVE-2017-3641, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Description

The scan detected that the host is missing the following update:
ALAS-2017-888

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://alas.aws.amazon.com/ALAS-2017-888.html>

Amazon Linux AMI

x86_64
mysql56-bench-5.6.37-1.26.amzn1
mysql56-embedded-devel-5.6.37-1.26.amzn1
mysql56-errmsg-5.6.37-1.26.amzn1
mysql56-common-5.6.37-1.26.amzn1
mysql56-embedded-5.6.37-1.26.amzn1
mysql56-5.6.37-1.26.amzn1
mysql56-debuginfo-5.6.37-1.26.amzn1
mysql56-devel-5.6.37-1.26.amzn1
mysql56-libs-5.6.37-1.26.amzn1
mysql56-test-5.6.37-1.26.amzn1
mysql56-server-5.6.37-1.26.amzn1

i686
mysql56-bench-5.6.37-1.26.amzn1
mysql56-embedded-devel-5.6.37-1.26.amzn1
mysql56-errmsg-5.6.37-1.26.amzn1
mysql56-5.6.37-1.26.amzn1
mysql56-embedded-5.6.37-1.26.amzn1
mysql56-test-5.6.37-1.26.amzn1
mysql56-common-5.6.37-1.26.amzn1
mysql56-libs-5.6.37-1.26.amzn1
mysql56-debuginfo-5.6.37-1.26.amzn1
mysql56-devel-5.6.37-1.26.amzn1
mysql56-server-5.6.37-1.26.amzn1

170857 - Amazon Linux AMI ALAS-2017-880 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-7798

Description

The scan detected that the host is missing the following update:

ALAS-2017-880

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://alas.aws.amazon.com/ALAS-2017-880.html>

Amazon Linux AMI

i686

rubygem23-bigdecimal-1.2.8-1.15.amzn1

rubygem23-psych-2.1.0-1.15.amzn1

ruby23-devel-2.3.4-1.15.amzn1

ruby23-2.3.4-1.15.amzn1

ruby23-libs-2.3.4-1.15.amzn1

ruby23-debuginfo-2.3.4-1.15.amzn1

rubygem23-io-console-0.4.5-1.15.amzn1

noarch

ruby23-doc-2.3.4-1.15.amzn1

ruby23-irb-2.3.4-1.15.amzn1

rubygem23-did_you_mean-1.0.0-1.15.amzn1

rubygems23-2.5.2-1.15.amzn1

rubygems23-devel-2.5.2-1.15.amzn1

x86_64

rubygem23-bigdecimal-1.2.8-1.15.amzn1

rubygem23-psych-2.1.0-1.15.amzn1

ruby23-devel-2.3.4-1.15.amzn1

ruby23-2.3.4-1.15.amzn1

ruby23-libs-2.3.4-1.15.amzn1

ruby23-debuginfo-2.3.4-1.15.amzn1

rubygem23-io-console-0.4.5-1.15.amzn1

175256 - Scientific Linux Security ERRATA Moderate: 389-ds-base on SL7.x x86_64 (1709-80)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2017-7551

Description

The scan detected that the host is missing the following update:

Security ERRATA Moderate: 389-ds-base on SL7.x x86_64 (1709-80)

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1709&L=scientific-linux-errata&F=&S=&P=80>

SL7
x86_64
389-ds-base-devel-1.3.6.1-19.el7_4
389-ds-base-1.3.6.1-19.el7_4
389-ds-base-debuginfo-1.3.6.1-19.el7_4
389-ds-base-snmp-1.3.6.1-19.el7_4
389-ds-base-libs-1.3.6.1-19.el7_4

182433 - FreeBSD libcrypt Side-channel Attack Vulnerability (22f28bb3-8d98-11e7-8c37-e8e0b747a45a)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-0379

Description

The scan detected that the host is missing the following update:

libcrypt -- side-channel attack vulnerability (22f28bb3-8d98-11e7-8c37-e8e0b747a45a)

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.vuxml.org/freebsd/22f28bb3-8d98-11e7-8c37-e8e0b747a45a.html>

Affected packages:

libcrypt < 1.8.1

192588 - Fedora Linux 27 FEDORA-2017-908f063bb6 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-10664, CVE-2017-11334, CVE-2017-9330, CVE-2017-9524

Description

The scan detected that the host is missing the following update:

FEDORA-2017-908f063bb6

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 27

xen-4.9.0-9.fc27

192590 - Fedora Linux 26 FEDORA-2017-b7f1197c23 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-10664, CVE-2017-11334, CVE-2017-9330, CVE-2017-9524

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b7f1197c23

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 26

xen-4.8.1-8.fc26

22330 - (K21531693) F5 BIG-IP Libssh2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-0787

Description

An Information Disclosure vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

An Information Disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in libssh2 library before version 1.7.0. Successful exploitation could allow an attacker to decrypt or intercept SSH sessions.

22331 - (K63712424) F5 BIG-IP PHP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8935

Description

A vulnerability is present in some versions of F5's BIG-IP Products.

Observation

F5's BIG-IP Products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the PHP. Successful exploitation could allow an attacker to conduct cross-site scripting attacks.

132398 - Oracle VM OVMSA-2017-0150 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6210

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0150

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000777.html>

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000778.html>

OVM3.3

x86_64

openssh-5.3p1-123.el6_9

openssh-server-5.3p1-123.el6_9

openssh-clients-5.3p1-123.el6_9

OVM3.4

x86_64

openssh-5.3p1-123.el6_9

openssh-server-5.3p1-123.el6_9

openssh-clients-5.3p1-123.el6_9

141700 - Red Hat Enterprise Linux RHSA-2017-2563 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6210

Description

The scan detected that the host is missing the following update:
RHSA-2017-2563

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-August/msg00086.html>

RHEL6D

x86_64

openssh-5.3p1-123.el6_9

openssh-server-5.3p1-123.el6_9

pam_ssh_agent_auth-0.9.3-123.el6_9

openssh-askpass-5.3p1-123.el6_9

openssh-ldap-5.3p1-123.el6_9

openssh-debuginfo-5.3p1-123.el6_9

openssh-clients-5.3p1-123.el6_9

i386

openssh-5.3p1-123.el6_9

openssh-server-5.3p1-123.el6_9

pam_ssh_agent_auth-0.9.3-123.el6_9

openssh-askpass-5.3p1-123.el6_9

openssh-ldap-5.3p1-123.el6_9

openssh-debuginfo-5.3p1-123.el6_9

openssh-clients-5.3p1-123.el6_9

RHEL6S

i386

openssh-5.3p1-123.el6_9

openssh-server-5.3p1-123.el6_9

pam_ssh_agent_auth-0.9.3-123.el6_9
openssh-askpass-5.3p1-123.el6_9
openssh-ldap-5.3p1-123.el6_9
openssh-debuginfo-5.3p1-123.el6_9
openssh-clients-5.3p1-123.el6_9

x86_64
openssh-5.3p1-123.el6_9
openssh-server-5.3p1-123.el6_9
pam_ssh_agent_auth-0.9.3-123.el6_9
openssh-askpass-5.3p1-123.el6_9
openssh-ldap-5.3p1-123.el6_9
openssh-debuginfo-5.3p1-123.el6_9
openssh-clients-5.3p1-123.el6_9

RHEL6WS
x86_64
openssh-5.3p1-123.el6_9
openssh-server-5.3p1-123.el6_9
openssh-debuginfo-5.3p1-123.el6_9
openssh-clients-5.3p1-123.el6_9
openssh-askpass-5.3p1-123.el6_9

i386
openssh-5.3p1-123.el6_9
openssh-server-5.3p1-123.el6_9
openssh-debuginfo-5.3p1-123.el6_9
openssh-clients-5.3p1-123.el6_9
openssh-askpass-5.3p1-123.el6_9

145521 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0680-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6410

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0680-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00038.html>

SuSE Linux 42.1
i586
libkde4-debuginfo-4.14.18-15.2
libkdecore4-devel-4.14.18-15.2
libkde4-4.14.18-15.2
libkde4-devel-4.14.18-15.2
kio-devel-5.21.0-23.2
libkdecore4-devel-debuginfo-4.14.18-15.2
kio-debuginfo-5.21.0-23.2
libksuseinstall1-4.14.18-15.2
kdelibs4-branding-upstream-4.14.18-15.2
kdelibs4-doc-4.14.18-15.2

kio-debugsource-5.21.0-23.2
kdelibs4-doc-debuginfo-4.14.18-15.2
libkdecore4-debuginfo-4.14.18-15.2
kio-5.21.0-23.2
kdelibs4-core-4.14.18-15.2
libkdecore4-4.14.18-15.2
kdelibs4-debuginfo-4.14.18-15.2
libksuseinstall-devel-4.14.18-15.2
libksuseinstall1-debuginfo-4.14.18-15.2
kio-core-5.21.0-23.2
kdelibs4-core-debuginfo-4.14.18-15.2
kio-core-debuginfo-5.21.0-23.2
kdelibs4-debugsource-4.14.18-15.2
kdelibs4-4.14.18-15.2
kio-devel-debuginfo-5.21.0-23.2

noarch
kdelibs4-apidocs-4.14.18-15.2
kio-lang-5.21.0-23.2

x86_64
libksuseinstall1-32bit-4.14.18-15.2
kio-debuginfo-5.21.0-23.2
kdelibs4-debugsource-4.14.18-15.2
kio-core-debuginfo-32bit-5.21.0-23.2
kio-5.21.0-23.2
libkde4-32bit-4.14.18-15.2
kdelibs4-core-4.14.18-15.2
kdelibs4-debuginfo-4.14.18-15.2
libkde4-4.14.18-15.2
kdelibs4-4.14.18-15.2
kdelibs4-core-debuginfo-4.14.18-15.2
libkdecore4-debuginfo-4.14.18-15.2
kdelibs4-doc-4.14.18-15.2
libksuseinstall1-4.14.18-15.2
libkde4-debuginfo-32bit-4.14.18-15.2
kio-devel-debuginfo-5.21.0-23.2
kio-devel-5.21.0-23.2
libksuseinstall1-debuginfo-4.14.18-15.2
kio-devel-32bit-5.21.0-23.2
kio-core-debuginfo-5.21.0-23.2
libkdecore4-4.14.18-15.2
libkdecore4-devel-4.14.18-15.2
libksuseinstall1-debuginfo-32bit-4.14.18-15.2
libkdecore4-devel-debuginfo-4.14.18-15.2
kio-core-5.21.0-23.2
kio-debugsource-5.21.0-23.2
kio-core-32bit-5.21.0-23.2
kdelibs4-branding-upstream-4.14.18-15.2
libkdecore4-debuginfo-32bit-4.14.18-15.2
libkde4-debuginfo-4.14.18-15.2
libkde4-devel-4.14.18-15.2
kio-32bit-5.21.0-23.2
kio-devel-debuginfo-32bit-5.21.0-23.2
kio-debuginfo-32bit-5.21.0-23.2
kdelibs4-doc-debuginfo-4.14.18-15.2
libksuseinstall-devel-4.14.18-15.2
libkdecore4-32bit-4.14.18-15.2

i586

kdelibs4-4.14.25-5.2
libkde4-devel-4.14.25-5.2
kdelibs4-core-debuginfo-4.14.25-5.2
kdelibs4-doc-4.14.25-5.2
kio-debugsource-5.26.0-6.2
kdelibs4-debuginfo-4.14.25-5.2
kdelibs4-branding-upstream-4.14.25-5.2
kio-debuginfo-5.26.0-6.2
kdelibs4-debugsource-4.14.25-5.2
libksuseinstall-devel-4.14.25-5.2
libkde4-debuginfo-4.14.25-5.2
kio-5.26.0-6.2
libkdecore4-devel-debuginfo-4.14.25-5.2
libkdecore4-4.14.25-5.2
libkdecore4-debuginfo-4.14.25-5.2
libksuseinstall1-debuginfo-4.14.25-5.2
libkdecore4-devel-4.14.25-5.2
libkde4-4.14.25-5.2
kio-devel-5.26.0-6.2
kdelibs4-core-4.14.25-5.2
kio-core-debuginfo-5.26.0-6.2
kdelibs4-doc-debuginfo-4.14.25-5.2
kio-devel-debuginfo-5.26.0-6.2
libksuseinstall1-4.14.25-5.2
kio-core-5.26.0-6.2

noarch

kdelibs4-apidocs-4.14.25-5.2
kio-lang-5.26.0-6.2

x86_64

kdelibs4-doc-4.14.25-5.2
libkdecore4-devel-4.14.25-5.2
kio-32bit-5.26.0-6.2
libkdecore4-debuginfo-32bit-4.14.25-5.2
libksuseinstall1-debuginfo-32bit-4.14.25-5.2
libkdecore4-devel-debuginfo-4.14.25-5.2
kio-debuginfo-5.26.0-6.2
libksuseinstall1-debuginfo-4.14.25-5.2
kio-devel-32bit-5.26.0-6.2
libkde4-4.14.25-5.2
kio-core-5.26.0-6.2
libksuseinstall-devel-4.14.25-5.2
kio-debugsource-5.26.0-6.2
kdelibs4-doc-debuginfo-4.14.25-5.2
libksuseinstall1-32bit-4.14.25-5.2
kdelibs4-debugsource-4.14.25-5.2
kdelibs4-4.14.25-5.2
libkdecore4-4.14.25-5.2
kio-core-debuginfo-32bit-5.26.0-6.2
libkde4-debuginfo-32bit-4.14.25-5.2
kio-devel-5.26.0-6.2
libksuseinstall1-4.14.25-5.2
kio-5.26.0-6.2
kio-core-debuginfo-5.26.0-6.2
kdelibs4-branding-upstream-4.14.25-5.2
kdelibs4-core-4.14.25-5.2
kio-debuginfo-32bit-5.26.0-6.2
libkdecore4-debuginfo-4.14.25-5.2

libkde4-32bit-4.14.25-5.2
kio-core-32bit-5.26.0-6.2
kdelibs4-debuginfo-4.14.25-5.2
kio-devel-debuginfo-32bit-5.26.0-6.2
libkde4-debuginfo-4.14.25-5.2
kio-devel-debuginfo-5.26.0-6.2
libkde4-devel-4.14.25-5.2
libkdecore4-32bit-4.14.25-5.2
kdelibs4-core-debuginfo-4.14.25-5.2

145528 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2208-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6435, CVE-2017-6436, CVE-2017-6437, CVE-2017-6438, CVE-2017-6439

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2208-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00082.html>

SuSE Linux 42.2

x86_64

libplist++3-1.12-7.6.1
libplist++3-debuginfo-32bit-1.12-7.6.1
libplist++3-debuginfo-1.12-7.6.1
plistutil-1.12-7.6.1
python-plist-1.12-7.6.1
python-plist-debuginfo-1.12-7.6.1
libplist-devel-1.12-7.6.1
libplist++3-32bit-1.12-7.6.1
libplist3-32bit-1.12-7.6.1
libplist-debugsource-1.12-7.6.1
libplist3-1.12-7.6.1
plistutil-debuginfo-1.12-7.6.1
libplist3-debuginfo-32bit-1.12-7.6.1
libplist++-devel-1.12-7.6.1
libplist3-debuginfo-1.12-7.6.1

i586

python-plist-1.12-7.6.1
python-plist-debuginfo-1.12-7.6.1
plistutil-1.12-7.6.1
libplist-debugsource-1.12-7.6.1
libplist++3-1.12-7.6.1
libplist++3-debuginfo-1.12-7.6.1
plistutil-debuginfo-1.12-7.6.1
libplist3-debuginfo-1.12-7.6.1
libplist-devel-1.12-7.6.1
libplist3-1.12-7.6.1
libplist++-devel-1.12-7.6.1

SuSE Linux 42.3

x86_64
libplist3-1.12-11.1
plistutil-debuginfo-1.12-11.1
libplist++3-32bit-1.12-11.1
libplist++3-debuginfo-32bit-1.12-11.1
libplist++3-1.12-11.1
libplist3-32bit-1.12-11.1
libplist++3-debuginfo-1.12-11.1
libplist++-devel-1.12-11.1
libplist-debugsource-1.12-11.1
libplist3-debuginfo-1.12-11.1
libplist-devel-1.12-11.1
plistutil-1.12-11.1
libplist3-debuginfo-32bit-1.12-11.1
python-plist-debuginfo-1.12-11.1
python-plist-1.12-11.1

i586
plistutil-1.12-11.1
libplist-debugsource-1.12-11.1
python-plist-1.12-11.1
libplist++3-debuginfo-1.12-11.1
libplist-devel-1.12-11.1
libplist3-1.12-11.1
plistutil-debuginfo-1.12-11.1
python-plist-debuginfo-1.12-11.1
libplist++3-1.12-11.1
libplist++-devel-1.12-11.1
libplist3-debuginfo-1.12-11.1

145529 - SuSE Linux 42.2 openSUSE-SU-2017:0005-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10013, CVE-2016-10024, CVE-2016-10025, CVE-2016-9932

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0005-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00001.html>

SuSE Linux 42.2

x86_64
xen-libs-32bit-4.7.1_04-6.1
xen-doc-html-4.7.1_04-6.1
xen-tools-4.7.1_04-6.1
xen-tools-domU-debuginfo-4.7.1_04-6.1
xen-4.7.1_04-6.1
xen-libs-4.7.1_04-6.1
xen-debugsource-4.7.1_04-6.1
xen-tools-domU-4.7.1_04-6.1
xen-libs-debuginfo-4.7.1_04-6.1
xen-tools-debuginfo-4.7.1_04-6.1

xen-libs-debuginfo-32bit-4.7.1_04-6.1
xen-devel-4.7.1_04-6.1

i586
xen-tools-domU-debuginfo-4.7.1_04-6.1
xen-libs-4.7.1_04-6.1
xen-debugsource-4.7.1_04-6.1
xen-tools-domU-4.7.1_04-6.1
xen-libs-debuginfo-4.7.1_04-6.1
xen-devel-4.7.1_04-6.1

145542 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1063-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-2775, CVE-2016-6170, CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1063-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00072.html>

SuSE Linux 42.1

i586
bind-debugsource-9.9.9P1-51.1
bind-utils-9.9.9P1-51.1
bind-devel-9.9.9P1-51.1
bind-lwresd-debuginfo-9.9.9P1-51.1
bind-chrootenv-9.9.9P1-51.1
bind-utils-debuginfo-9.9.9P1-51.1
bind-debuginfo-9.9.9P1-51.1
bind-9.9.9P1-51.1
bind-libs-9.9.9P1-51.1
bind-lwresd-9.9.9P1-51.1
bind-libs-debuginfo-9.9.9P1-51.1

noarch
bind-doc-9.9.9P1-51.1

x86_64
bind-libs-9.9.9P1-51.1
bind-devel-9.9.9P1-51.1
bind-9.9.9P1-51.1
bind-utils-debuginfo-9.9.9P1-51.1
bind-lwresd-9.9.9P1-51.1
bind-lwresd-debuginfo-9.9.9P1-51.1
bind-debuginfo-9.9.9P1-51.1
bind-libs-debuginfo-32bit-9.9.9P1-51.1
bind-libs-debuginfo-9.9.9P1-51.1
bind-chrootenv-9.9.9P1-51.1
bind-libs-32bit-9.9.9P1-51.1
bind-debugsource-9.9.9P1-51.1
bind-utils-9.9.9P1-51.1

SuSE Linux 42.2
i586
bind-libs-9.9.9P1-48.3.1
bind-debugsource-9.9.9P1-48.3.1
bind-lwresd-9.9.9P1-48.3.1
bind-9.9.9P1-48.3.1
bind-chrootenv-9.9.9P1-48.3.1
bind-devel-9.9.9P1-48.3.1
bind-utils-debuginfo-9.9.9P1-48.3.1
bind-utils-9.9.9P1-48.3.1
bind-libs-debuginfo-9.9.9P1-48.3.1
bind-debuginfo-9.9.9P1-48.3.1
bind-lwresd-debuginfo-9.9.9P1-48.3.1

noarch
bind-doc-9.9.9P1-48.3.1

x86_64
bind-9.9.9P1-48.3.1
bind-libs-32bit-9.9.9P1-48.3.1
bind-devel-9.9.9P1-48.3.1
bind-lwresd-9.9.9P1-48.3.1
bind-lwresd-debuginfo-9.9.9P1-48.3.1
bind-utils-debuginfo-9.9.9P1-48.3.1
bind-chrootenv-9.9.9P1-48.3.1
bind-utils-9.9.9P1-48.3.1
bind-libs-debuginfo-9.9.9P1-48.3.1
bind-libs-debuginfo-32bit-9.9.9P1-48.3.1
bind-debugsource-9.9.9P1-48.3.1
bind-libs-9.9.9P1-48.3.1
bind-debuginfo-9.9.9P1-48.3.1

145552 - SuSE Linux 42.2 openSUSE-SU-2017:0902-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10163, CVE-2016-10214, CVE-2017-5580, CVE-2017-5937, CVE-2017-5956, CVE-2017-5957, CVE-2017-5993, CVE-2017-5994, CVE-2017-6209, CVE-2017-6210, CVE-2017-6317, CVE-2017-6355, CVE-2017-6386

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:0902-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00119.html>

SuSE Linux 42.2
x86_64
libvirglrenderer0-0.5.0-3.3.1
virglrenderer-test-server-0.5.0-3.3.1
virglrenderer-devel-0.5.0-3.3.1
virglrenderer-test-server-debuginfo-0.5.0-3.3.1
libvirglrenderer0-debuginfo-0.5.0-3.3.1
virglrenderer-debugsource-0.5.0-3.3.1

i586
libvirglrenderer0-0.5.0-3.3.1
virglrenderer-test-server-0.5.0-3.3.1
virglrenderer-devel-0.5.0-3.3.1
virglrenderer-test-server-debuginfo-0.5.0-3.3.1
libvirglrenderer0-debuginfo-0.5.0-3.3.1
virglrenderer-debugsource-0.5.0-3.3.1

145557 - SuSE Linux 42.2 openSUSE-SU-2017:0009-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-1241, CVE-2016-1242

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0009-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00005.html>

SuSE Linux 42.2
noarch
trytond_stock_lot-3.8.1-3.1
trytond_stock-3.8.4-3.1
proteus-3.8.5-3.1
trytond_account_invoice-3.8.4-3.1
trytond_account-3.8.5-3.1
tryton-3.8.12-3.1
trytond-3.8.9-4.1
gnuhealth-3.0.5-3.1

145558 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0821-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6503, CVE-2017-6504

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0821-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00086.html>

SuSE Linux 42.1
x86_64
qbittorrent-nox-3.3.11-6.1
qbittorrent-debugsource-3.3.11-6.1
qbittorrent-debuginfo-3.3.11-6.1

qbittorrent-3.3.11-6.1
qbittorrent-nox-debuginfo-3.3.11-6.1

i586
qbittorrent-nox-3.3.11-6.1
qbittorrent-debugsource-3.3.11-6.1
qbittorrent-debuginfo-3.3.11-6.1
qbittorrent-3.3.11-6.1
qbittorrent-nox-debuginfo-3.3.11-6.1

SuSE Linux 42.2
x86_64
qbittorrent-nox-3.3.11-2.3.1
qbittorrent-debuginfo-3.3.11-2.3.1
qbittorrent-debugsource-3.3.11-2.3.1
qbittorrent-nox-debuginfo-3.3.11-2.3.1
qbittorrent-3.3.11-2.3.1

i586
qbittorrent-nox-3.3.11-2.3.1
qbittorrent-debuginfo-3.3.11-2.3.1
qbittorrent-debugsource-3.3.11-2.3.1
qbittorrent-nox-debuginfo-3.3.11-2.3.1
qbittorrent-3.3.11-2.3.1

145571 - SuSE Linux 42.1 openSUSE-SU-2017:1312-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10155, CVE-2016-9776, CVE-2016-9907, CVE-2016-9911, CVE-2016-9921, CVE-2016-9922, CVE-2017-2615, CVE-2017-2620, CVE-2017-5525, CVE-2017-5526, CVE-2017-5667, CVE-2017-5856, CVE-2017-5898

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1312-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00058.html>

SuSE Linux 42.1
i586
qemu-tools-debuginfo-2.3.1-25.1
qemu-guest-agent-2.3.1-25.1
qemu-block-curl-2.3.1-25.1
qemu-kvm-2.3.1-25.1
qemu-guest-agent-debuginfo-2.3.1-25.1
qemu-extra-2.3.1-25.1
qemu-lang-2.3.1-25.1
qemu-ppc-debuginfo-2.3.1-25.1
qemu-arm-2.3.1-25.1
qemu-s390-2.3.1-25.1
qemu-x86-2.3.1-25.1
qemu-ppc-2.3.1-25.1
qemu-linux-user-debugsource-2.3.1-25.1
qemu-extra-debuginfo-2.3.1-25.1

qemu-2.3.1-25.1
qemu-s390-debuginfo-2.3.1-25.1
qemu-block-curl-debuginfo-2.3.1-25.1
qemu-tools-2.3.1-25.1
qemu-arm-debuginfo-2.3.1-25.1
qemu-x86-debuginfo-2.3.1-25.1
qemu-debugsource-2.3.1-25.1
qemu-linux-user-debuginfo-2.3.1-25.1
qemu-linux-user-2.3.1-25.1

noarch
qemu-vgabios-1.8.1-25.1
qemu-ipxe-1.0.0-25.1
qemu-seabios-1.8.1-25.1
qemu-sgabios-8-25.1

x86_64
qemu-tools-debuginfo-2.3.1-25.1
qemu-guest-agent-2.3.1-25.1
qemu-block-curl-2.3.1-25.1
qemu-kvm-2.3.1-25.1
qemu-guest-agent-debuginfo-2.3.1-25.1
qemu-extra-2.3.1-25.1
qemu-lang-2.3.1-25.1
qemu-ppc-debuginfo-2.3.1-25.1
qemu-testsuite-2.3.1-25.1
qemu-arm-2.3.1-25.1
qemu-block-rbd-2.3.1-25.1
qemu-s390-2.3.1-25.1
qemu-x86-2.3.1-25.1
qemu-ppc-2.3.1-25.1
qemu-linux-user-debugsource-2.3.1-25.1
qemu-extra-debuginfo-2.3.1-25.1
qemu-2.3.1-25.1
qemu-s390-debuginfo-2.3.1-25.1
qemu-block-curl-debuginfo-2.3.1-25.1
qemu-tools-2.3.1-25.1
qemu-arm-debuginfo-2.3.1-25.1
qemu-x86-debuginfo-2.3.1-25.1
qemu-debugsource-2.3.1-25.1
qemu-block-rbd-debuginfo-2.3.1-25.1
qemu-linux-user-debuginfo-2.3.1-25.1
qemu-linux-user-2.3.1-25.1

145586 - SuSE Linux 42.2 openSUSE-SU-2017:1798-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-8350

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:1798-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00028.html>

SuSE Linux 42.2

x86_64

libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.12.3
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.12.3
libGraphicsMagick++-devel-1.3.25-11.12.3
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.12.3
libGraphicsMagick++-Q16-12-1.3.25-11.12.3
GraphicsMagick-devel-1.3.25-11.12.3
perl-GraphicsMagick-1.3.25-11.12.3
perl-GraphicsMagick-debuginfo-1.3.25-11.12.3
libGraphicsMagickWand-Q16-2-1.3.25-11.12.3
GraphicsMagick-debuginfo-1.3.25-11.12.3
libGraphicsMagick3-config-1.3.25-11.12.3
libGraphicsMagick-Q16-3-1.3.25-11.12.3
GraphicsMagick-1.3.25-11.12.3
GraphicsMagick-debugsource-1.3.25-11.12.3

i586

libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.12.3
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.12.3
libGraphicsMagick++-devel-1.3.25-11.12.3
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.12.3
libGraphicsMagick++-Q16-12-1.3.25-11.12.3
GraphicsMagick-devel-1.3.25-11.12.3
perl-GraphicsMagick-1.3.25-11.12.3
perl-GraphicsMagick-debuginfo-1.3.25-11.12.3
libGraphicsMagickWand-Q16-2-1.3.25-11.12.3
GraphicsMagick-debuginfo-1.3.25-11.12.3
libGraphicsMagick3-config-1.3.25-11.12.3
libGraphicsMagick-Q16-3-1.3.25-11.12.3
GraphicsMagick-1.3.25-11.12.3
GraphicsMagick-debugsource-1.3.25-11.12.3

145596 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2119-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-3308, CVE-2017-3309, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2119-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00024.html>

SuSE Linux 42.2

x86_64

mariadb-tools-10.0.31-20.7.1
libmysqlclient18-debuginfo-10.0.31-20.7.1
mariadb-client-debuginfo-10.0.31-20.7.1
libmysqld18-10.0.31-20.7.1
libmysqlclient18-32bit-10.0.31-20.7.1

mariadb-debuginfo-10.0.31-20.7.1
mariadb-debugsource-10.0.31-20.7.1
libmysqlclient18-debuginfo-32bit-10.0.31-20.7.1
mariadb-tools-debuginfo-10.0.31-20.7.1
libmysqlclient18-10.0.31-20.7.1
libmysqlclient_r18-32bit-10.0.31-20.7.1
libmysqld-devel-10.0.31-20.7.1
mariadb-10.0.31-20.7.1
mariadb-bench-debuginfo-10.0.31-20.7.1
mariadb-test-debuginfo-10.0.31-20.7.1
mariadb-bench-10.0.31-20.7.1
libmysqld18-debuginfo-10.0.31-20.7.1
mariadb-test-10.0.31-20.7.1
libmysqlclient_r18-10.0.31-20.7.1
mariadb-client-10.0.31-20.7.1
libmysqlclient-devel-10.0.31-20.7.1
mariadb-errormessages-10.0.31-20.7.1

i586

mariadb-tools-10.0.31-20.7.1
libmysqlclient18-debuginfo-10.0.31-20.7.1
mariadb-client-debuginfo-10.0.31-20.7.1
libmysqld18-10.0.31-20.7.1
mariadb-debuginfo-10.0.31-20.7.1
mariadb-debugsource-10.0.31-20.7.1
mariadb-tools-debuginfo-10.0.31-20.7.1
libmysqlclient18-10.0.31-20.7.1
libmysqld-devel-10.0.31-20.7.1
mariadb-10.0.31-20.7.1
mariadb-bench-debuginfo-10.0.31-20.7.1
mariadb-test-debuginfo-10.0.31-20.7.1
mariadb-bench-10.0.31-20.7.1
libmysqld18-debuginfo-10.0.31-20.7.1
mariadb-test-10.0.31-20.7.1
libmysqlclient_r18-10.0.31-20.7.1
mariadb-client-10.0.31-20.7.1
libmysqlclient-devel-10.0.31-20.7.1
mariadb-errormessages-10.0.31-20.7.1

SuSE Linux 42.3

x86_64

mariadb-errormessages-10.0.31-23.1
mariadb-bench-debuginfo-10.0.31-23.1
mariadb-debugsource-10.0.31-23.1
mariadb-debuginfo-10.0.31-23.1
mariadb-10.0.31-23.1
libmysqlclient_r18-10.0.31-23.1
libmysqlclient18-debuginfo-10.0.31-23.1
libmysqlclient_r18-32bit-10.0.31-23.1
mariadb-test-debuginfo-10.0.31-23.1
libmysqld18-10.0.31-23.1
libmysqld-devel-10.0.31-23.1
libmysqlclient18-debuginfo-32bit-10.0.31-23.1
mariadb-client-10.0.31-23.1
mariadb-bench-10.0.31-23.1
mariadb-client-debuginfo-10.0.31-23.1
libmysqld18-debuginfo-10.0.31-23.1
mariadb-test-10.0.31-23.1
mariadb-tools-10.0.31-23.1
libmysqlclient18-32bit-10.0.31-23.1

mariadb-tools-debuginfo-10.0.31-23.1
libmysqlclient18-10.0.31-23.1
libmysqlclient-devel-10.0.31-23.1

i586

mariadb-errormessages-10.0.31-23.1
mariadb-bench-debuginfo-10.0.31-23.1
mariadb-debugsource-10.0.31-23.1
mariadb-debuginfo-10.0.31-23.1
mariadb-10.0.31-23.1
libmysqlclient_r18-10.0.31-23.1
libmysqlclient18-debuginfo-10.0.31-23.1
mariadb-test-debuginfo-10.0.31-23.1
libmysqld18-10.0.31-23.1
libmysqld-devel-10.0.31-23.1
mariadb-client-10.0.31-23.1
mariadb-bench-10.0.31-23.1
mariadb-client-debuginfo-10.0.31-23.1
libmysqld18-debuginfo-10.0.31-23.1
mariadb-test-10.0.31-23.1
mariadb-tools-10.0.31-23.1
mariadb-tools-debuginfo-10.0.31-23.1
libmysqlclient18-10.0.31-23.1
libmysqlclient-devel-10.0.31-23.1

145598 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1966-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9962

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1966-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-07/msg00093.html>

SuSE Linux 42.1

i586

runc-debugsource-0.1.1+gitr2819_50a19c6-10.1
containerd-debuginfo-0.2.5+gitr569_2a5e70c-10.1
containerd-ctr-0.2.5+gitr569_2a5e70c-10.1
containerd-debugsource-0.2.5+gitr569_2a5e70c-10.1
runc-0.1.1+gitr2819_50a19c6-10.1
containerd-0.2.5+gitr569_2a5e70c-10.1
runc-debuginfo-0.1.1+gitr2819_50a19c6-10.1
containerd-ctr-debuginfo-0.2.5+gitr569_2a5e70c-10.1

noarch

containerd-test-0.2.5+gitr569_2a5e70c-10.1
runc-test-0.1.1+gitr2819_50a19c6-10.1
docker-zsh-completion-1.12.6-27.1
docker-bash-completion-1.12.6-27.1

x86_64
containerd-0.2.5+gitr569_2a5e70c-10.1
containerd-debuginfo-0.2.5+gitr569_2a5e70c-10.1
runc-0.1.1+gitr2819_50a19c6-10.1
containerd-debugsource-0.2.5+gitr569_2a5e70c-10.1
docker-test-1.12.6-27.1
docker-debuginfo-1.12.6-27.1
docker-1.12.6-27.1
docker-test-debuginfo-1.12.6-27.1
containerd-ctr-debuginfo-0.2.5+gitr569_2a5e70c-10.1
containerd-ctr-0.2.5+gitr569_2a5e70c-10.1
runc-debugsource-0.1.1+gitr2819_50a19c6-10.1
docker-debugsource-1.12.6-27.1
runc-debuginfo-0.1.1+gitr2819_50a19c6-10.1

SuSE Linux 42.2

x86_64
docker-debuginfo-1.12.6-25.2
docker-test-1.12.6-25.2
containerd-debuginfo-0.2.5+gitr569_2a5e70c-8.1
docker-1.12.6-25.2
containerd-ctr-0.2.5+gitr569_2a5e70c-8.1
containerd-debugsource-0.2.5+gitr569_2a5e70c-8.1
runc-debugsource-0.1.1+gitr2819_50a19c6-8.1
containerd-ctr-debuginfo-0.2.5+gitr569_2a5e70c-8.1
runc-0.1.1+gitr2819_50a19c6-8.1
containerd-0.2.5+gitr569_2a5e70c-8.1
runc-debuginfo-0.1.1+gitr2819_50a19c6-8.1
docker-debugsource-1.12.6-25.2
docker-test-debuginfo-1.12.6-25.2

noarch

docker-zsh-completion-1.12.6-25.2
runc-test-0.1.1+gitr2819_50a19c6-8.1
containerd-test-0.2.5+gitr569_2a5e70c-8.1
docker-bash-completion-1.12.6-25.2

145619 - SuSE Linux 42.1 openSUSE-SU-2017:0479-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-8318, CVE-2016-8327, CVE-2017-3238, CVE-2017-3244, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-2017-3273, CVE-2017-3291, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0479-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00067.html>

SuSE Linux 42.1

x86_64
mysql-community-server-client-5.6.35-22.1
mysql-community-server-errormessages-5.6.35-22.1

libmysql56client18-debuginfo-32bit-5.6.35-22.1
libmysql56client_r18-32bit-5.6.35-22.1
libmysql56client18-32bit-5.6.35-22.1
libmysql56client18-5.6.35-22.1
mysql-community-server-test-5.6.35-22.1
libmysql56client18-debuginfo-5.6.35-22.1
mysql-community-server-tools-5.6.35-22.1
mysql-community-server-bench-5.6.35-22.1
mysql-community-server-5.6.35-22.1
mysql-community-server-client-debuginfo-5.6.35-22.1
mysql-community-server-tools-debuginfo-5.6.35-22.1
libmysql56client_r18-5.6.35-22.1
mysql-community-server-bench-debuginfo-5.6.35-22.1
mysql-community-server-test-debuginfo-5.6.35-22.1
mysql-community-server-debugsource-5.6.35-22.1
mysql-community-server-debuginfo-5.6.35-22.1

i586

mysql-community-server-client-5.6.35-22.1
mysql-community-server-errormessages-5.6.35-22.1
libmysql56client18-5.6.35-22.1
mysql-community-server-test-5.6.35-22.1
libmysql56client18-debuginfo-5.6.35-22.1
mysql-community-server-tools-5.6.35-22.1
mysql-community-server-bench-5.6.35-22.1
mysql-community-server-5.6.35-22.1
mysql-community-server-client-debuginfo-5.6.35-22.1
mysql-community-server-tools-debuginfo-5.6.35-22.1
libmysql56client_r18-5.6.35-22.1
mysql-community-server-bench-debuginfo-5.6.35-22.1
mysql-community-server-test-debuginfo-5.6.35-22.1
mysql-community-server-debugsource-5.6.35-22.1
mysql-community-server-debuginfo-5.6.35-22.1

145624 - SuSE Linux 42.1 openSUSE-SU-2017:0208-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-8568, CVE-2016-8569

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0208-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00114.html>

SuSE Linux 42.1

x86_64

libgit2-22-debuginfo-32bit-0.22.1-5.1
libgit2-22-32bit-0.22.1-5.1
libgit2-22-0.22.1-5.1
libgit2-devel-0.22.1-5.1
libgit2-debugsource-0.22.1-5.1
libgit2-22-debuginfo-0.22.1-5.1

i586
libgit2-devel-0.22.1-5.1
libgit2-debugsource-0.22.1-5.1
libgit2-22-0.22.1-5.1
libgit2-22-debuginfo-0.22.1-5.1

145626 - SuSE Linux 42.2 openSUSE-SU-2017:1511-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-9142

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1511-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00023.html>

SuSE Linux 42.2

x86_64

libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.9.1
libGraphicsMagick-Q16-3-1.3.25-11.9.1
GraphicsMagick-debugsource-1.3.25-11.9.1
libGraphicsMagick++-Q16-12-1.3.25-11.9.1
libGraphicsMagickWand-Q16-2-1.3.25-11.9.1
perl-GraphicsMagick-1.3.25-11.9.1
perl-GraphicsMagick-debuginfo-1.3.25-11.9.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.9.1
libGraphicsMagick++-devel-1.3.25-11.9.1
GraphicsMagick-debuginfo-1.3.25-11.9.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.9.1
libGraphicsMagick3-config-1.3.25-11.9.1
GraphicsMagick-devel-1.3.25-11.9.1
GraphicsMagick-1.3.25-11.9.1

i586

libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.9.1
libGraphicsMagick-Q16-3-1.3.25-11.9.1
GraphicsMagick-debugsource-1.3.25-11.9.1
libGraphicsMagick++-Q16-12-1.3.25-11.9.1
libGraphicsMagickWand-Q16-2-1.3.25-11.9.1
perl-GraphicsMagick-1.3.25-11.9.1
perl-GraphicsMagick-debuginfo-1.3.25-11.9.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.9.1
libGraphicsMagick++-devel-1.3.25-11.9.1
GraphicsMagick-debuginfo-1.3.25-11.9.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.9.1
libGraphicsMagick3-config-1.3.25-11.9.1
GraphicsMagick-devel-1.3.25-11.9.1
GraphicsMagick-1.3.25-11.9.1

145629 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2123-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-10791, CVE-2017-10792

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:2123-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00028.html>

SuSE Linux 42.2

x86_64

pspp-0.10.2-2.3.1

pspp-debugsource-0.10.2-2.3.1

pspp-debuginfo-0.10.2-2.3.1

pspp-devel-0.10.2-2.3.1

SuSE Linux 42.3

x86_64

pspp-0.10.2-5.1

pspp-devel-0.10.2-5.1

pspp-debugsource-0.10.2-5.1

pspp-debuginfo-0.10.2-5.1

145630 - SuSE Linux 42.2 openSUSE-SU-2017:0894-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6335

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:0894-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00116.html>

SuSE Linux 42.2

x86_64

libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.3.1

GraphicsMagick-debugsource-1.3.25-11.3.1

libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.3.1

libGraphicsMagick-Q16-3-1.3.25-11.3.1

GraphicsMagick-devel-1.3.25-11.3.1

libGraphicsMagickWand-Q16-2-1.3.25-11.3.1

libGraphicsMagick3-config-1.3.25-11.3.1

perl-GraphicsMagick-debuginfo-1.3.25-11.3.1

perl-GraphicsMagick-1.3.25-11.3.1

libGraphicsMagick++-devel-1.3.25-11.3.1

GraphicsMagick-1.3.25-11.3.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.3.1
libGraphicsMagick++-Q16-12-1.3.25-11.3.1
GraphicsMagick-debuginfo-1.3.25-11.3.1

i586

libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.3.1
GraphicsMagick-debugsource-1.3.25-11.3.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.3.1
libGraphicsMagick-Q16-3-1.3.25-11.3.1
GraphicsMagick-devel-1.3.25-11.3.1
libGraphicsMagickWand-Q16-2-1.3.25-11.3.1
libGraphicsMagick3-config-1.3.25-11.3.1
perl-GraphicsMagick-debuginfo-1.3.25-11.3.1
perl-GraphicsMagick-1.3.25-11.3.1
libGraphicsMagick++-devel-1.3.25-11.3.1
GraphicsMagick-1.3.25-11.3.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.3.1
libGraphicsMagick++-Q16-12-1.3.25-11.3.1
GraphicsMagick-debuginfo-1.3.25-11.3.1

145633 - SuSE Linux 42.1 openSUSE-SU-2017:0891-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6335

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0891-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00114.html>

SuSE Linux 42.1

x86_64

perl-GraphicsMagick-debuginfo-1.3.21-29.1
libGraphicsMagick-Q16-3-debuginfo-1.3.21-29.1
perl-GraphicsMagick-1.3.21-29.1
libGraphicsMagickWand-Q16-2-1.3.21-29.1
GraphicsMagick-1.3.21-29.1
libGraphicsMagick++-Q16-11-1.3.21-29.1
libGraphicsMagick++-devel-1.3.21-29.1
GraphicsMagick-devel-1.3.21-29.1
GraphicsMagick-debugsource-1.3.21-29.1
libGraphicsMagick++-Q16-11-debuginfo-1.3.21-29.1
libGraphicsMagick3-config-1.3.21-29.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.21-29.1
libGraphicsMagick-Q16-3-1.3.21-29.1
GraphicsMagick-debuginfo-1.3.21-29.1

i586

perl-GraphicsMagick-debuginfo-1.3.21-29.1
libGraphicsMagick-Q16-3-debuginfo-1.3.21-29.1
perl-GraphicsMagick-1.3.21-29.1

libGraphicsMagickWand-Q16-2-1.3.21-29.1
GraphicsMagick-1.3.21-29.1
libGraphicsMagick++-Q16-11-1.3.21-29.1
libGraphicsMagick++-devel-1.3.21-29.1
GraphicsMagick-devel-1.3.21-29.1
GraphicsMagick-debugsource-1.3.21-29.1
libGraphicsMagick++-Q16-11-debuginfo-1.3.21-29.1
libGraphicsMagick3-config-1.3.21-29.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.21-29.1
libGraphicsMagick-Q16-3-1.3.21-29.1
GraphicsMagick-debuginfo-1.3.21-29.1

145634 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0890-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6508

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0890-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00113.html>

SuSE Linux 42.1

x86_64

wget-debuginfo-1.14-11.1

wget-debugsource-1.14-11.1

wget-1.14-11.1

i586

wget-debuginfo-1.14-11.1

wget-debugsource-1.14-11.1

wget-1.14-11.1

SuSE Linux 42.2

x86_64

wget-debugsource-1.14-8.3.1

wget-debuginfo-1.14-8.3.1

wget-1.14-8.3.1

i586

wget-debugsource-1.14-8.3.1

wget-debuginfo-1.14-8.3.1

wget-1.14-8.3.1

145649 - SuSE Linux 42.1 openSUSE-SU-2017:0325-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9811

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0325-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00169.html>

SuSE Linux 42.1

i586

libgstapp-0_10-0-0.10.36-14.1
libgstapp-0_10-0-debuginfo-0.10.36-14.1
gststreamer-0_10-plugins-base-devel-0.10.36-14.1
gststreamer-0_10-plugin-gnomevfs-debuginfo-0.10.36-14.1
libgstinterfaces-0_10-0-0.10.36-14.1
gststreamer-0_10-plugin-gnomevfs-0.10.36-14.1
typelib-1_0-GstInterfaces-0_10-0.10.36-14.1
gststreamer-0_10-plugins-base-0.10.36-14.1
gststreamer-0_10-plugins-base-debuginfo-0.10.36-14.1
gststreamer-0_10-plugins-base-debugsource-0.10.36-14.1
typelib-1_0-GstApp-0_10-0.10.36-14.1
libgstinterfaces-0_10-0-debuginfo-0.10.36-14.1
gststreamer-0_10-plugins-base-doc-0.10.36-14.1

noarch

gststreamer-0_10-plugins-base-lang-0.10.36-14.1

x86_64

libgstapp-0_10-0-0.10.36-14.1
libgstapp-0_10-0-debuginfo-0.10.36-14.1
gststreamer-0_10-plugins-base-devel-0.10.36-14.1
libgstapp-0_10-0-debuginfo-32bit-0.10.36-14.1
gststreamer-0_10-plugin-gnomevfs-debuginfo-0.10.36-14.1
libgstinterfaces-0_10-0-debuginfo-32bit-0.10.36-14.1
libgstinterfaces-0_10-0-0.10.36-14.1
gststreamer-0_10-plugin-gnomevfs-0.10.36-14.1
typelib-1_0-GstInterfaces-0_10-0.10.36-14.1
gststreamer-0_10-plugins-base-debuginfo-32bit-0.10.36-14.1
gststreamer-0_10-plugins-base-0.10.36-14.1
gststreamer-0_10-plugins-base-debuginfo-0.10.36-14.1
gststreamer-0_10-plugins-base-32bit-0.10.36-14.1
gststreamer-0_10-plugins-base-debugsource-0.10.36-14.1
typelib-1_0-GstApp-0_10-0.10.36-14.1
libgstinterfaces-0_10-0-debuginfo-0.10.36-14.1
libgstapp-0_10-0-32bit-0.10.36-14.1
gststreamer-0_10-plugins-base-doc-0.10.36-14.1
libgstinterfaces-0_10-0-32bit-0.10.36-14.1

145669 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0389-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-2037

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0389-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00026.html>

SuSE Linux 42.1

i586

cpio-debugsource-2.11-32.1

cpio-2.11-32.1

cpio-debuginfo-2.11-32.1

noarch

cpio-lang-2.11-32.1

x86_64

cpio-debugsource-2.11-32.1

cpio-2.11-32.1

cpio-debuginfo-2.11-32.1

SuSE Linux 42.2

i586

cpio-2.11-33.1

cpio-debuginfo-2.11-33.1

cpio-debugsource-2.11-33.1

noarch

cpio-lang-2.11-33.1

x86_64

cpio-2.11-33.1

cpio-debuginfo-2.11-33.1

cpio-debugsource-2.11-33.1

145673 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2367-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-12927, CVE-2017-12978

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:2367-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-09/msg00017.html>

SuSE Linux 42.2

i586

cacti-spine-1.1.19-7.6.1

cacti-spine-debugsource-1.1.19-7.6.1

cacti-spine-debuginfo-1.1.19-7.6.1

noarch

cacti-1.1.19-16.6.1
cacti-doc-1.1.19-16.6.1

x86_64
cacti-spine-1.1.19-7.6.1
cacti-spine-debugsource-1.1.19-7.6.1
cacti-spine-debuginfo-1.1.19-7.6.1

SuSE Linux 42.3
i586
cacti-spine-debuginfo-1.1.19-13.1
cacti-spine-debugsource-1.1.19-13.1
cacti-spine-1.1.19-13.1

noarch
cacti-doc-1.1.19-22.1
cacti-1.1.19-22.1

x86_64
cacti-spine-debuginfo-1.1.19-13.1
cacti-spine-debugsource-1.1.19-13.1
cacti-spine-1.1.19-13.1

145677 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1107-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-7585, CVE-2017-7586, CVE-2017-7741, CVE-2017-7742

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1107-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00096.html>

SuSE Linux 42.1
x86_64
libsndfile-debugsource-1.0.25-27.1
libsndfile1-debuginfo-1.0.25-27.1
libsndfile-progs-1.0.25-27.1
libsndfile-devel-1.0.25-27.1
libsndfile1-debuginfo-32bit-1.0.25-27.1
libsndfile-progs-debugsource-1.0.25-27.1
libsndfile1-1.0.25-27.1
libsndfile-progs-debuginfo-1.0.25-27.1
libsndfile1-32bit-1.0.25-27.1

i586
libsndfile-debugsource-1.0.25-27.1
libsndfile1-debuginfo-1.0.25-27.1
libsndfile-progs-1.0.25-27.1
libsndfile-devel-1.0.25-27.1
libsndfile-progs-debugsource-1.0.25-27.1
libsndfile1-1.0.25-27.1

libsndfile-progs-debuginfo-1.0.25-27.1

SuSE Linux 42.2

x86_64

libsndfile-devel-1.0.25-26.3.1

libsndfile-progs-debuginfo-1.0.25-26.3.1

libsndfile-progs-debugsource-1.0.25-26.3.1

libsndfile1-1.0.25-26.3.1

libsndfile-progs-1.0.25-26.3.1

libsndfile1-32bit-1.0.25-26.3.1

libsndfile1-debuginfo-32bit-1.0.25-26.3.1

libsndfile1-debuginfo-1.0.25-26.3.1

libsndfile-debugsource-1.0.25-26.3.1

i586

libsndfile-devel-1.0.25-26.3.1

libsndfile-progs-debuginfo-1.0.25-26.3.1

libsndfile-progs-debugsource-1.0.25-26.3.1

libsndfile1-1.0.25-26.3.1

libsndfile-progs-1.0.25-26.3.1

libsndfile1-debuginfo-1.0.25-26.3.1

libsndfile-debugsource-1.0.25-26.3.1

145686 - SuSE Linux 42.1 openSUSE-SU-2017:1177-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-7941

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:1177-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00008.html>

SuSE Linux 42.1

x86_64

libGraphicsMagick++-Q16-11-debuginfo-1.3.21-32.1

perl-GraphicsMagick-1.3.21-32.1

GraphicsMagick-debuginfo-1.3.21-32.1

libGraphicsMagick++-devel-1.3.21-32.1

libGraphicsMagick3-config-1.3.21-32.1

libGraphicsMagick++-Q16-11-1.3.21-32.1

GraphicsMagick-devel-1.3.21-32.1

perl-GraphicsMagick-debuginfo-1.3.21-32.1

libGraphicsMagickWand-Q16-2-1.3.21-32.1

libGraphicsMagick-Q16-3-debuginfo-1.3.21-32.1

libGraphicsMagickWand-Q16-2-debuginfo-1.3.21-32.1

libGraphicsMagick-Q16-3-1.3.21-32.1

GraphicsMagick-1.3.21-32.1

GraphicsMagick-debugsource-1.3.21-32.1

i586

libGraphicsMagick++-Q16-11-debuginfo-1.3.21-32.1

perl-GraphicsMagick-1.3.21-32.1
GraphicsMagick-debuginfo-1.3.21-32.1
libGraphicsMagick++-devel-1.3.21-32.1
libGraphicsMagick3-config-1.3.21-32.1
libGraphicsMagick++-Q16-11-1.3.21-32.1
GraphicsMagick-devel-1.3.21-32.1
perl-GraphicsMagick-debuginfo-1.3.21-32.1
libGraphicsMagickWand-Q16-2-1.3.21-32.1
libGraphicsMagick-Q16-3-debuginfo-1.3.21-32.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.21-32.1
libGraphicsMagick-Q16-3-1.3.21-32.1
GraphicsMagick-1.3.21-32.1
GraphicsMagick-debugsource-1.3.21-32.1

145703 - SuSE Linux 42.2 openSUSE-SU-2017:1650-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-8932

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1650-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00080.html>

SuSE Linux 42.2

x86_64

go-debugsource-1.6.2-23.3.3

go-1.6.2-23.3.3

go-debuginfo-1.6.2-23.3.3

go-doc-1.6.2-23.3.3

i586

go-debugsource-1.6.2-23.3.3

go-1.6.2-23.3.3

go-debuginfo-1.6.2-23.3.3

go-doc-1.6.2-23.3.3

145710 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0969-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6507

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0969-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00037.html>

SuSE Linux 42.1

i586

pam_apparmor-2.10.2-12.1
apparmor-parser-2.10.2-12.1
apache2-mod_apparmor-2.10.2-12.1
ruby-apparmor-debuginfo-2.10.2-12.1
apparmor-parser-debuginfo-2.10.2-12.1
libapparmor-devel-2.10.2-12.1
perl-apparmor-debuginfo-2.10.2-12.1
apparmor-debugsource-2.10.2-12.1
libapparmor1-2.10.2-12.1
libapparmor1-debuginfo-2.10.2-12.1
ruby-apparmor-2.10.2-12.1
perl-apparmor-2.10.2-12.1
python3-apparmor-2.10.2-12.1
python3-apparmor-debuginfo-2.10.2-12.1
apache2-mod_apparmor-debuginfo-2.10.2-12.1
pam_apparmor-debuginfo-2.10.2-12.1

noarch

apparmor-abstractions-2.10.2-12.1
apparmor-parser-lang-2.10.2-12.1
apparmor-profiles-2.10.2-12.1
apparmor-utils-2.10.2-12.1
apparmor-utils-lang-2.10.2-12.1
apparmor-docs-2.10.2-12.1

x86_64

libapparmor1-32bit-2.10.2-12.1
pam_apparmor-2.10.2-12.1
apparmor-parser-2.10.2-12.1
apache2-mod_apparmor-2.10.2-12.1
pam_apparmor-debuginfo-32bit-2.10.2-12.1
ruby-apparmor-debuginfo-2.10.2-12.1
apparmor-parser-debuginfo-2.10.2-12.1
libapparmor-devel-2.10.2-12.1
perl-apparmor-debuginfo-2.10.2-12.1
apparmor-debugsource-2.10.2-12.1
libapparmor1-debuginfo-32bit-2.10.2-12.1
libapparmor1-2.10.2-12.1
libapparmor1-debuginfo-2.10.2-12.1
ruby-apparmor-2.10.2-12.1
perl-apparmor-2.10.2-12.1
python3-apparmor-2.10.2-12.1
python3-apparmor-debuginfo-2.10.2-12.1
pam_apparmor-32bit-2.10.2-12.1
apache2-mod_apparmor-debuginfo-2.10.2-12.1
pam_apparmor-debuginfo-2.10.2-12.1

SuSE Linux 42.2

i586

apache2-mod_apparmor-debuginfo-2.10.2-12.3.1
perl-apparmor-2.10.2-12.3.1
python3-apparmor-debuginfo-2.10.2-12.3.1
pam_apparmor-2.10.2-12.3.1
apparmor-debugsource-2.10.2-12.3.1
ruby-apparmor-2.10.2-12.3.1
apparmor-parser-2.10.2-12.3.1

perl-apparmor-debuginfo-2.10.2-12.3.1
libapparmor1-2.10.2-12.3.1
ruby-apparmor-debuginfo-2.10.2-12.3.1
libapparmor-devel-2.10.2-12.3.1
apparmor-parser-debuginfo-2.10.2-12.3.1
python3-apparmor-2.10.2-12.3.1
libapparmor1-debuginfo-2.10.2-12.3.1
apache2-mod_apparmor-2.10.2-12.3.1
pam_apparmor-debuginfo-2.10.2-12.3.1

noarch

apparmor-profiles-2.10.2-12.3.1
apparmor-utils-lang-2.10.2-12.3.1
apparmor-docs-2.10.2-12.3.1
apparmor-utils-2.10.2-12.3.1
apparmor-abstractions-2.10.2-12.3.1
apparmor-parser-lang-2.10.2-12.3.1

x86_64

apache2-mod_apparmor-debuginfo-2.10.2-12.3.1
perl-apparmor-2.10.2-12.3.1
python3-apparmor-debuginfo-2.10.2-12.3.1
libapparmor1-32bit-2.10.2-12.3.1
pam_apparmor-2.10.2-12.3.1
apparmor-debugsource-2.10.2-12.3.1
ruby-apparmor-2.10.2-12.3.1
apparmor-parser-2.10.2-12.3.1
pam_apparmor-32bit-2.10.2-12.3.1
perl-apparmor-debuginfo-2.10.2-12.3.1
libapparmor1-2.10.2-12.3.1
libapparmor1-debuginfo-32bit-2.10.2-12.3.1
ruby-apparmor-debuginfo-2.10.2-12.3.1
libapparmor-devel-2.10.2-12.3.1
apparmor-parser-debuginfo-2.10.2-12.3.1
python3-apparmor-2.10.2-12.3.1
libapparmor1-debuginfo-2.10.2-12.3.1
pam_apparmor-debuginfo-32bit-2.10.2-12.3.1
apache2-mod_apparmor-2.10.2-12.3.1
pam_apparmor-debuginfo-2.10.2-12.3.1

145717 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2053-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6009, CVE-2017-6010, CVE-2017-6011

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:2053-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00012.html>

SuSE Linux 42.2

x86_64

icoutils-debugsource-0.31.3-10.3.1
icoutils-debuginfo-0.31.3-10.3.1
icoutils-0.31.3-10.3.1

i586
icoutils-debugsource-0.31.3-10.3.1
icoutils-debuginfo-0.31.3-10.3.1
icoutils-0.31.3-10.3.1

SuSE Linux 42.3
x86_64
icoutils-0.31.3-13.1
icoutils-debuginfo-0.31.3-13.1
icoutils-debugsource-0.31.3-13.1

i586
icoutils-0.31.3-13.1
icoutils-debuginfo-0.31.3-13.1
icoutils-debugsource-0.31.3-13.1

145738 - SuSE Linux 42.2 openSUSE-SU-2017:0021-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-2123, CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0021-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00010.html>

SuSE Linux 42.2
i586
libsmbclient0-debuginfo-4.4.2-9.1
samba-python-debuginfo-4.4.2-9.1
libdcerpc-samr-devel-4.4.2-9.1
libsmbclient0-4.4.2-9.1
libsamba-policy-devel-4.4.2-9.1
samba-debugsource-4.4.2-9.1
libsamba-policy0-debuginfo-4.4.2-9.1
libndr-devel-4.4.2-9.1
libsmbconf0-4.4.2-9.1
samba-test-4.4.2-9.1
libsamba-util0-4.4.2-9.1
libndr-standard0-4.4.2-9.1
samba-core-devel-4.4.2-9.1
ctdb-tests-4.4.2-9.1
samba-client-4.4.2-9.1
libsamba-errors0-4.4.2-9.1
libtevent-util0-4.4.2-9.1
samba-client-debuginfo-4.4.2-9.1
libtevent-util0-debuginfo-4.4.2-9.1
samba-pidl-4.4.2-9.1

libndr-standard-devel-4.4.2-9.1
libdcerpc-binding0-debuginfo-4.4.2-9.1
libdcerpc-samr0-debuginfo-4.4.2-9.1
libsamdb0-4.4.2-9.1
ctdb-4.4.2-9.1
libsmbldap0-debuginfo-4.4.2-9.1
libsamba-hostconfig0-4.4.2-9.1
libdcerpc-binding0-4.4.2-9.1
samba-test-debuginfo-4.4.2-9.1
ctdb-debuginfo-4.4.2-9.1
libnetapi0-debuginfo-4.4.2-9.1
libwbclient0-debuginfo-4.4.2-9.1
libtevent-util-devel-4.4.2-9.1
libsamba-credentials0-4.4.2-9.1
libndr-nbt0-debuginfo-4.4.2-9.1
libsmbclient-devel-4.4.2-9.1
libsamba-errors-devel-4.4.2-9.1
libwbclient0-4.4.2-9.1
samba-winbind-4.4.2-9.1
libsamba-passdb-devel-4.4.2-9.1
libsamba-credentials-devel-4.4.2-9.1
libsmbconf-devel-4.4.2-9.1
libndr-nbt0-4.4.2-9.1
libndr0-4.4.2-9.1
libdcerpc-samr0-4.4.2-9.1
libsmbldap0-4.4.2-9.1
libndr-krb5pac0-debuginfo-4.4.2-9.1
libsamba-passdb0-debuginfo-4.4.2-9.1
libsamba-util-devel-4.4.2-9.1
samba-debuginfo-4.4.2-9.1
libnetapi0-4.4.2-9.1
libsmbldap-devel-4.4.2-9.1
libdcerpc0-debuginfo-4.4.2-9.1
libndr-krb5pac0-4.4.2-9.1
samba-python-4.4.2-9.1
samba-winbind-debuginfo-4.4.2-9.1
libsamdb-devel-4.4.2-9.1
libndr-krb5pac-devel-4.4.2-9.1
libsamdb0-debuginfo-4.4.2-9.1
libwbclient-devel-4.4.2-9.1
libndr-standard0-debuginfo-4.4.2-9.1
libsamba-errors0-debuginfo-4.4.2-9.1
libndr-nbt-devel-4.4.2-9.1
samba-libs-4.4.2-9.1
libsmbconf0-debuginfo-4.4.2-9.1
libsamba-hostconfig0-debuginfo-4.4.2-9.1
samba-4.4.2-9.1
libsamba-hostconfig-devel-4.4.2-9.1
libndr0-debuginfo-4.4.2-9.1
libdcerpc-devel-4.4.2-9.1
libsamba-passdb0-4.4.2-9.1
libsamba-policy0-4.4.2-9.1
libnetapi-devel-4.4.2-9.1
ctdb-tests-debuginfo-4.4.2-9.1
libdcerpc0-4.4.2-9.1
libsamba-credentials0-debuginfo-4.4.2-9.1
libsamba-util0-debuginfo-4.4.2-9.1
samba-libs-debuginfo-4.4.2-9.1

noarch

samba-doc-4.4.2-9.1

x86_64

libsmbclient0-debuginfo-4.4.2-9.1

samba-python-debuginfo-4.4.2-9.1

libsmbconf0-32bit-4.4.2-9.1

libdcerpc-samr-devel-4.4.2-9.1

libsmbclient0-4.4.2-9.1

libsamba-policy-devel-4.4.2-9.1

samba-debugsource-4.4.2-9.1

libsamba-policy0-debuginfo-4.4.2-9.1

samba-client-debuginfo-32bit-4.4.2-9.1

libndr0-32bit-4.4.2-9.1

libndr-devel-4.4.2-9.1

libnetapi0-debuginfo-32bit-4.4.2-9.1

libndr-nbt0-32bit-4.4.2-9.1

libsmbconf0-4.4.2-9.1

samba-test-4.4.2-9.1

libsamba-util0-4.4.2-9.1

libndr-standard0-4.4.2-9.1

samba-core-devel-4.4.2-9.1

ctdb-tests-4.4.2-9.1

libwbclient0-debuginfo-32bit-4.4.2-9.1

samba-client-4.4.2-9.1

libsamba-errors0-4.4.2-9.1

libtevent-util0-4.4.2-9.1

samba-client-32bit-4.4.2-9.1

samba-client-debuginfo-4.4.2-9.1

libtevent-util0-debuginfo-4.4.2-9.1

libsamba-util0-debuginfo-32bit-4.4.2-9.1

samba-pidl-4.4.2-9.1

libsamba-credentials0-debuginfo-32bit-4.4.2-9.1

libndr-standard-devel-4.4.2-9.1

libdcerpc-binding0-debuginfo-4.4.2-9.1

libdcerpc-samr0-debuginfo-4.4.2-9.1

libsamdb0-4.4.2-9.1

ctdb-4.4.2-9.1

libsamba-hostconfig0-32bit-4.4.2-9.1

samba-libs-debuginfo-32bit-4.4.2-9.1

libsmbldap0-debuginfo-4.4.2-9.1

libsamba-hostconfig0-4.4.2-9.1

libdcerpc-binding0-4.4.2-9.1

samba-test-debuginfo-4.4.2-9.1

ctdb-debuginfo-4.4.2-9.1

samba-libs-32bit-4.4.2-9.1

libwbclient0-32bit-4.4.2-9.1

libsmbconf0-debuginfo-32bit-4.4.2-9.1

libdcerpc-binding0-32bit-4.4.2-9.1

samba-winbind-32bit-4.4.2-9.1

libsamba-util0-32bit-4.4.2-9.1

libndr-standard0-debuginfo-32bit-4.4.2-9.1

libnetapi0-debuginfo-4.4.2-9.1

libwbclient0-debuginfo-4.4.2-9.1

libtevent-util-devel-4.4.2-9.1

libsamba-credentials0-4.4.2-9.1

libndr-nbt0-debuginfo-4.4.2-9.1

libsmbclient-devel-4.4.2-9.1

libsamba-hostconfig0-debuginfo-32bit-4.4.2-9.1

libsamba-errors-devel-4.4.2-9.1

libdcerpc0-debuginfo-32bit-4.4.2-9.1

libnetapi0-32bit-4.4.2-9.1
libsamba-passdb0-32bit-4.4.2-9.1
libwbclient0-4.4.2-9.1
libndr-krb5pac0-debuginfo-32bit-4.4.2-9.1
libdcerpc0-32bit-4.4.2-9.1
samba-winbind-4.4.2-9.1
libsamba-policy0-debuginfo-32bit-4.4.2-9.1
libsamba-passdb-devel-4.4.2-9.1
libsmbldap0-32bit-4.4.2-9.1
libsamba-credentials-devel-4.4.2-9.1
libsmbconf-devel-4.4.2-9.1
libndr-nbt0-4.4.2-9.1
libsmbldap0-debuginfo-32bit-4.4.2-9.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-9.1
libndr0-4.4.2-9.1
libdcerpc-samr0-4.4.2-9.1
libsamba-passdb0-debuginfo-32bit-4.4.2-9.1
libsmbldap0-4.4.2-9.1
libndr-krb5pac0-debuginfo-4.4.2-9.1
libsamba-credentials0-32bit-4.4.2-9.1
libtevent-util0-32bit-4.4.2-9.1
libsamba-passdb0-debuginfo-4.4.2-9.1
libsamba-util-devel-4.4.2-9.1
libndr-nbt0-debuginfo-32bit-4.4.2-9.1
libdcerpc-samr0-32bit-4.4.2-9.1
libsamdb0-debuginfo-32bit-4.4.2-9.1
samba-debuginfo-4.4.2-9.1
libsamba-errors0-32bit-4.4.2-9.1
libnetapi0-4.4.2-9.1
libsmbldap-devel-4.4.2-9.1
libdcerpc0-debuginfo-4.4.2-9.1
libdcerpc-samr0-debuginfo-32bit-4.4.2-9.1
libndr-krb5pac0-4.4.2-9.1
libndr-standard0-32bit-4.4.2-9.1
samba-python-4.4.2-9.1
libsmbclient0-debuginfo-32bit-4.4.2-9.1
samba-winbind-debuginfo-4.4.2-9.1
libsamdb-devel-4.4.2-9.1
libndr-krb5pac-devel-4.4.2-9.1
libsamdb0-debuginfo-4.4.2-9.1
libwbclient-devel-4.4.2-9.1
libndr-standard0-debuginfo-4.4.2-9.1
libsamba-errors0-debuginfo-4.4.2-9.1
libndr-nbt-devel-4.4.2-9.1
libtevent-util0-debuginfo-32bit-4.4.2-9.1
samba-libs-4.4.2-9.1
libsmbconf0-debuginfo-4.4.2-9.1
libsamdb0-32bit-4.4.2-9.1
libndr-krb5pac0-32bit-4.4.2-9.1
libsamba-policy0-32bit-4.4.2-9.1
libsamba-hostconfig0-debuginfo-4.4.2-9.1
samba-4.4.2-9.1
libsamba-errors0-debuginfo-32bit-4.4.2-9.1
libsamba-hostconfig-devel-4.4.2-9.1
samba-winbind-debuginfo-32bit-4.4.2-9.1
libndr0-debuginfo-32bit-4.4.2-9.1
libndr0-debuginfo-4.4.2-9.1
libdcerpc-devel-4.4.2-9.1
libsmbclient0-32bit-4.4.2-9.1
libsamba-passdb0-4.4.2-9.1

libsamba-policy0-4.4.2-9.1
libnetapi-devel-4.4.2-9.1
ctdb-tests-debuginfo-4.4.2-9.1
libdcerpc0-4.4.2-9.1
libsamba-credentials0-debuginfo-4.4.2-9.1
libsamba-util0-debuginfo-4.4.2-9.1
samba-libs-debuginfo-4.4.2-9.1

145742 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0531-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5592

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0531-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00097.html>

SuSE Linux 42.1
x86_64
profanity-0.4.7-3.1
profanity-debugsource-0.4.7-3.1
profanity-debuginfo-0.4.7-3.1

i586
profanity-0.4.7-3.1
profanity-debugsource-0.4.7-3.1
profanity-debuginfo-0.4.7-3.1

SuSE Linux 42.2
x86_64
profanity-standard-debuginfo-0.5.0-4.1
profanity-mini-0.5.0-4.1
profanity-debuginfo-0.5.0-4.1
profanity-debugsource-0.5.0-4.1
profanity-0.5.0-4.1
profanity-mini-debuginfo-0.5.0-4.1
profanity-standard-0.5.0-4.1

145752 - SuSE Linux 42.2 openSUSE-SU-2017:1427-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-7585, CVE-2017-7741, CVE-2017-7742, CVE-2017-8361, CVE-2017-8362, CVE-2017-8363, CVE-2017-8365

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1427-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00095.html>

SuSE Linux 42.2

x86_64

libsndfile-progs-1.0.25-26.6.1
libsndfile-progs-debugsource-1.0.25-26.6.1
libsndfile1-debuginfo-32bit-1.0.25-26.6.1
libsndfile-devel-1.0.25-26.6.1
libsndfile-debugsource-1.0.25-26.6.1
libsndfile-progs-debuginfo-1.0.25-26.6.1
libsndfile1-debuginfo-1.0.25-26.6.1
libsndfile1-32bit-1.0.25-26.6.1
libsndfile1-1.0.25-26.6.1

i586

libsndfile-progs-1.0.25-26.6.1
libsndfile-progs-debugsource-1.0.25-26.6.1
libsndfile-devel-1.0.25-26.6.1
libsndfile-debugsource-1.0.25-26.6.1
libsndfile-progs-debuginfo-1.0.25-26.6.1
libsndfile1-debuginfo-1.0.25-26.6.1
libsndfile1-1.0.25-26.6.1

145755 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1210-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5974, CVE-2017-5975, CVE-2017-5976, CVE-2017-5977, CVE-2017-5978, CVE-2017-5979, CVE-2017-5980, CVE-2017-5981

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1210-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00025.html>

SuSE Linux 42.1

x86_64

zzip-devel-debuginfo-32bit-0.13.62-10.1
libzip-0-13-debuginfo-0.13.62-10.1
zzip-devel-32bit-0.13.62-10.1
libzip-0-13-0.13.62-10.1
libzip-0-13-debuginfo-32bit-0.13.62-10.1
libzip-0-13-32bit-0.13.62-10.1
zzip-debugsource-0.13.62-10.1
zzip-devel-debuginfo-0.13.62-10.1
zzip-devel-0.13.62-10.1

i586

zzip-devel-debuginfo-0.13.62-10.1
zzip-devel-0.13.62-10.1

libzip-0-13-debuginfo-0.13.62-10.1
libzip-0-13-0.13.62-10.1
zziplib-debugsource-0.13.62-10.1

SuSE Linux 42.2

x86_64

libzip-0-13-32bit-0.13.62-10.3.1
libzip-0-13-debuginfo-32bit-0.13.62-10.3.1
zziplib-devel-debuginfo-0.13.62-10.3.1
zziplib-devel-0.13.62-10.3.1
zziplib-debugsource-0.13.62-10.3.1
zziplib-devel-32bit-0.13.62-10.3.1
libzip-0-13-0.13.62-10.3.1
libzip-0-13-debuginfo-0.13.62-10.3.1
zziplib-devel-debuginfo-32bit-0.13.62-10.3.1

i586

libzip-0-13-0.13.62-10.3.1
zziplib-devel-debuginfo-0.13.62-10.3.1
zziplib-devel-0.13.62-10.3.1
zziplib-debugsource-0.13.62-10.3.1
libzip-0-13-debuginfo-0.13.62-10.3.1

145756 - SuSE Linux 42.1 openSUSE-SU-2017:0020-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-2123, CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0020-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00009.html>

SuSE Linux 42.1

i586

samba-test-debuginfo-4.2.4-24.1
samba-pidl-4.2.4-24.1
libsmbclient0-4.2.4-24.1
libsmbconf-devel-4.2.4-24.1
libdcerpc-atsvc-devel-4.2.4-24.1
libtevent-util-devel-4.2.4-24.1
libwbclient0-4.2.4-24.1
libndr-krb5pac-devel-4.2.4-24.1
libsmbldap0-4.2.4-24.1
libregistry0-debuginfo-4.2.4-24.1
libndr-nbt0-4.2.4-24.1
libdcerpc-samr-devel-4.2.4-24.1
libdcerpc-samr0-debuginfo-4.2.4-24.1
libsmbclient-raw0-4.2.4-24.1
libsamba-passdb0-debuginfo-4.2.4-24.1
libdcerpc-atsvc0-4.2.4-24.1
libwbclient-devel-4.2.4-24.1

libdcerpc-samr0-4.2.4-24.1
samba-debugsource-4.2.4-24.1
libdcerpc0-4.2.4-24.1
libsmbclient-devel-4.2.4-24.1
libsamba-credentials0-4.2.4-24.1
libndr0-4.2.4-24.1
samba-winbind-4.2.4-24.1
samba-4.2.4-24.1
libndr-standard0-debuginfo-4.2.4-24.1
samba-client-4.2.4-24.1
libndr0-debuginfo-4.2.4-24.1
libsamba-policy0-debuginfo-4.2.4-24.1
samba-libs-4.2.4-24.1
libndr-nbt-devel-4.2.4-24.1
libregistry0-4.2.4-24.1
ctdb-4.2.4-24.1
libsamba-passsdb0-4.2.4-24.1
libndr-nbt0-debuginfo-4.2.4-24.1
libregistry-devel-4.2.4-24.1
libdcerpc-binding0-4.2.4-24.1
samba-test-4.2.4-24.1
libgensec-devel-4.2.4-24.1
libsmbconf0-4.2.4-24.1
samba-test-devel-4.2.4-24.1
libsamdb-devel-4.2.4-24.1
libgensec0-debuginfo-4.2.4-24.1
libndr-krb5pac0-debuginfo-4.2.4-24.1
libsamdb0-debuginfo-4.2.4-24.1
libnetapi-devel-4.2.4-24.1
libtevent-util0-debuginfo-4.2.4-24.1
libdcerpc0-debuginfo-4.2.4-24.1
ctdb-tests-debuginfo-4.2.4-24.1
libdcerpc-devel-4.2.4-24.1
samba-client-debuginfo-4.2.4-24.1
libnetapi0-debuginfo-4.2.4-24.1
libsamba-policy-devel-4.2.4-24.1
libsamba-util0-debuginfo-4.2.4-24.1
libtevent-util0-4.2.4-24.1
libnetapi0-4.2.4-24.1
libdcerpc-binding0-debuginfo-4.2.4-24.1
libsamba-hostconfig0-4.2.4-24.1
libsamba-policy0-4.2.4-24.1
libsamdb0-4.2.4-24.1
libwbclient0-debuginfo-4.2.4-24.1
libsamba-hostconfig0-debuginfo-4.2.4-24.1
libsmbldap-devel-4.2.4-24.1
libsamba-hostconfig-devel-4.2.4-24.1
libgensec0-4.2.4-24.1
samba-debuginfo-4.2.4-24.1
libsmbconf0-debuginfo-4.2.4-24.1
libsamba-credentials-devel-4.2.4-24.1
libsamba-passsdb-devel-4.2.4-24.1
libsmbldap0-debuginfo-4.2.4-24.1
libndr-krb5pac0-4.2.4-24.1
libdcerpc-atvc0-debuginfo-4.2.4-24.1
libsmbclient0-debuginfo-4.2.4-24.1
libsamba-credentials0-debuginfo-4.2.4-24.1
libndr-devel-4.2.4-24.1
libndr-standard-devel-4.2.4-24.1
samba-python-debuginfo-4.2.4-24.1

ctdb-debuginfo-4.2.4-24.1
libsamba-util0-4.2.4-24.1
ctdb-devel-4.2.4-24.1
samba-core-devel-4.2.4-24.1
samba-libs-debuginfo-4.2.4-24.1
libsamba-util-devel-4.2.4-24.1
libndr-standard0-4.2.4-24.1
ctdb-tests-4.2.4-24.1
samba-winbind-debuginfo-4.2.4-24.1
libsmbclient-raw-devel-4.2.4-24.1
samba-python-4.2.4-24.1
libsmbclient-raw0-debuginfo-4.2.4-24.1

noarch
samba-doc-4.2.4-24.1

x86_64
libsamdb0-4.2.4-24.1
samba-python-4.2.4-24.1
libregistry0-32bit-4.2.4-24.1
libsmbclient-raw0-debuginfo-32bit-4.2.4-24.1
libndr-krb5pac0-4.2.4-24.1
ctdb-devel-4.2.4-24.1
libdcerpc-binding0-32bit-4.2.4-24.1
libregistry0-debuginfo-32bit-4.2.4-24.1
libsamba-util-devel-4.2.4-24.1
libndr-nbt0-32bit-4.2.4-24.1
libgensec0-32bit-4.2.4-24.1
libwbclient0-debuginfo-32bit-4.2.4-24.1
samba-debuginfo-32bit-4.2.4-24.1
libndr0-32bit-4.2.4-24.1
samba-core-devel-4.2.4-24.1
samba-4.2.4-24.1
libnetapi0-4.2.4-24.1
libsamba-policy0-debuginfo-32bit-4.2.4-24.1
libsmbldap0-debuginfo-32bit-4.2.4-24.1
libsamba-passdb-devel-4.2.4-24.1
libnetapi0-32bit-4.2.4-24.1
libregistry-devel-4.2.4-24.1
ctdb-tests-debuginfo-4.2.4-24.1
samba-client-debuginfo-4.2.4-24.1
libsamba-credentials0-32bit-4.2.4-24.1
libndr-nbt0-debuginfo-32bit-4.2.4-24.1
libndr-nbt-devel-4.2.4-24.1
libwbclient0-debuginfo-4.2.4-24.1
libndr-nbt0-debuginfo-4.2.4-24.1
ctdb-debuginfo-4.2.4-24.1
libsamba-passdb0-32bit-4.2.4-24.1
samba-debuginfo-4.2.4-24.1
libdcerpc-binding0-debuginfo-32bit-4.2.4-24.1
libnetapi0-debuginfo-4.2.4-24.1
libdcerpc-samr0-debuginfo-4.2.4-24.1
libndr-standard0-debuginfo-32bit-4.2.4-24.1
samba-test-debuginfo-4.2.4-24.1
libsmbldap0-32bit-4.2.4-24.1
libsamba-policy0-32bit-4.2.4-24.1
libsmbconf-devel-4.2.4-24.1
samba-winbind-debuginfo-32bit-4.2.4-24.1
libsmbclient0-4.2.4-24.1
samba-client-4.2.4-24.1

libdcerpc-devel-4.2.4-24.1
libsamba-hostconfig0-4.2.4-24.1
samba-32bit-4.2.4-24.1
libndr-krb5pac0-debuginfo-4.2.4-24.1
libndr0-debuginfo-4.2.4-24.1
libndr-devel-4.2.4-24.1
samba-winbind-debuginfo-4.2.4-24.1
samba-winbind-4.2.4-24.1
libdcerpc-atvc0-debuginfo-4.2.4-24.1
libsamba-util0-4.2.4-24.1
libsamba-hostconfig0-32bit-4.2.4-24.1
samba-test-4.2.4-24.1
samba-libs-debuginfo-4.2.4-24.1
libsamba-policy-devel-4.2.4-24.1
libndr-standard0-4.2.4-24.1
samba-libs-32bit-4.2.4-24.1
libndr-standard-devel-4.2.4-24.1
samba-libs-debuginfo-32bit-4.2.4-24.1
libdcerpc0-4.2.4-24.1
libdcerpc0-32bit-4.2.4-24.1
libdcerpc-samr-devel-4.2.4-24.1
libdcerpc-atvc0-debuginfo-32bit-4.2.4-24.1
samba-test-devel-4.2.4-24.1
libtevent-util-devel-4.2.4-24.1
libregistry0-4.2.4-24.1
libsmbldap0-debuginfo-4.2.4-24.1
samba-pidl-4.2.4-24.1
libwbclient0-4.2.4-24.1
libsmbclient0-32bit-4.2.4-24.1
libsmbclient-raw0-debuginfo-4.2.4-24.1
libsamba-passdb0-debuginfo-32bit-4.2.4-24.1
libsamba-passdb0-4.2.4-24.1
libsmbclient0-debuginfo-4.2.4-24.1
libwbclient-devel-4.2.4-24.1
libsamdb-devel-4.2.4-24.1
libdcerpc-atvc-devel-4.2.4-24.1
libndr-standard0-32bit-4.2.4-24.1
libsmbldap0-4.2.4-24.1
libsmbconf0-4.2.4-24.1
libwbclient0-32bit-4.2.4-24.1
libgensec-devel-4.2.4-24.1
libsamba-credentials0-debuginfo-4.2.4-24.1
libtevent-util0-4.2.4-24.1
libgensec0-debuginfo-4.2.4-24.1
libsmbclient-devel-4.2.4-24.1
libsmbclient0-debuginfo-32bit-4.2.4-24.1
samba-libs-4.2.4-24.1
libsamba-policy0-debuginfo-4.2.4-24.1
libdcerpc0-debuginfo-32bit-4.2.4-24.1
libsamba-credentials0-4.2.4-24.1
ctdb-tests-4.2.4-24.1
libndr0-4.2.4-24.1
samba-client-32bit-4.2.4-24.1
libsamba-credentials0-debuginfo-32bit-4.2.4-24.1
libdcerpc0-debuginfo-4.2.4-24.1
libsamba-util0-debuginfo-4.2.4-24.1
libsamba-util0-32bit-4.2.4-24.1
libtevent-util0-debuginfo-32bit-4.2.4-24.1
libsmbconf0-32bit-4.2.4-24.1
libsmbconf0-debuginfo-32bit-4.2.4-24.1

libndr-nbt0-4.2.4-24.1
libnetapi0-debuginfo-32bit-4.2.4-24.1
libsamba-passdb0-debuginfo-4.2.4-24.1
libsamba-policy0-4.2.4-24.1
libdcerpc-atvc0-4.2.4-24.1
libndr-krb5pac0-32bit-4.2.4-24.1
libsmbldap-devel-4.2.4-24.1
samba-python-debuginfo-4.2.4-24.1
libtevent-util0-32bit-4.2.4-24.1
libsmbconf0-debuginfo-4.2.4-24.1
libsamdb0-debuginfo-32bit-4.2.4-24.1
samba-client-debuginfo-32bit-4.2.4-24.1
libsamdb0-debuginfo-4.2.4-24.1
libsmbclient-raw-devel-4.2.4-24.1
libsmbclient-raw0-32bit-4.2.4-24.1
libndr-krb5pac-devel-4.2.4-24.1
libdcerpc-binding0-4.2.4-24.1
libndr-krb5pac0-debuginfo-32bit-4.2.4-24.1
libsamba-hostconfig0-debuginfo-4.2.4-24.1
libsmbclient-raw0-4.2.4-24.1
libgensec0-debuginfo-32bit-4.2.4-24.1
libndr-standard0-debuginfo-4.2.4-24.1
ctdb-4.2.4-24.1
libsamba-hostconfig-devel-4.2.4-24.1
libtevent-util0-debuginfo-4.2.4-24.1
libsamba-credentials-devel-4.2.4-24.1

145769 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0980-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3566

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0980-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00040.html>

SuSE Linux 42.1

i586
slrn-debugsource-1.0.3-4.1
slrn-debuginfo-1.0.3-4.1
slrn-1.0.3-4.1

noarch
slrn-lang-1.0.3-4.1

x86_64
slrn-debugsource-1.0.3-4.1
slrn-debuginfo-1.0.3-4.1
slrn-1.0.3-4.1

SuSE Linux 42.2

x86_64
slrn-debuginfo-1.0.3-4.3.1
slrn-debugsource-1.0.3-4.3.1
slrn-1.0.3-4.3.1

noarch
slrn-lang-1.0.3-4.3.1

145770 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0820-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6596

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0820-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00085.html>

SuSE Linux 42.1
i586
partclone-debugsource-0.3.5a-7.1
partclone-debuginfo-0.3.5a-7.1
partclone-0.3.5a-7.1

noarch
partclone-lang-0.3.5a-7.1

x86_64
partclone-debugsource-0.3.5a-7.1
partclone-debuginfo-0.3.5a-7.1
partclone-0.3.5a-7.1

SuSE Linux 42.2
x86_64
partclone-0.3.5a-2.3.1
partclone-debugsource-0.3.5a-2.3.1
partclone-debuginfo-0.3.5a-2.3.1

noarch
partclone-lang-0.3.5a-2.3.1

145771 - SuSE Linux 42.1 openSUSE-SU-2017:0148-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9811

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0148-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00080.html>

SuSE Linux 42.1

i586

typelib-1_0-GstPbutils-1_0-1.4.5-5.1
typelib-1_0-GstVideo-1_0-1.4.5-5.1
libgstfft-1_0-0-1.4.5-5.1
libgstsd-1_0-0-debuginfo-1.4.5-5.1
libgstrtp-1_0-0-debuginfo-1.4.5-5.1
typelib-1_0-GstAllocators-1_0-1.4.5-5.1
typelib-1_0-GstApp-1_0-1.4.5-5.1
typelib-1_0-GstRtp-1_0-1.4.5-5.1
libgstaudio-1_0-0-1.4.5-5.1
libgstpbutils-1_0-0-1.4.5-5.1
libgstrtp-1_0-0-1.4.5-5.1
libgstvideo-1_0-0-debuginfo-1.4.5-5.1
libgstrtp-1_0-0-debuginfo-1.4.5-5.1
gstreamer-plugins-base-devel-1.4.5-5.1
typelib-1_0-GstTag-1_0-1.4.5-5.1
typelib-1_0-GstSdp-1_0-1.4.5-5.1
libgstallocators-1_0-0-1.4.5-5.1
libgstpbutils-1_0-0-debuginfo-1.4.5-5.1
libgstsd-1_0-0-1.4.5-5.1
typelib-1_0-GstRtsp-1_0-1.4.5-5.1
typelib-1_0-GstFft-1_0-1.4.5-5.1
gstreamer-plugins-base-1.4.5-5.1
libgsttag-1_0-0-debuginfo-1.4.5-5.1
typelib-1_0-GstAudio-1_0-1.4.5-5.1
gstreamer-plugins-base-debugsource-1.4.5-5.1
libgstvideo-1_0-0-1.4.5-5.1
typelib-1_0-GstRiff-1_0-1.4.5-5.1
libgstapp-1_0-0-1.4.5-5.1
gstreamer-plugins-base-debuginfo-1.4.5-5.1
libgstaudio-1_0-0-debuginfo-1.4.5-5.1
gstreamer-plugins-base-doc-1.4.5-5.1
libgsttriff-1_0-0-debuginfo-1.4.5-5.1
libgsttriff-1_0-0-1.4.5-5.1
libgstfft-1_0-0-debuginfo-1.4.5-5.1
libgsttag-1_0-0-1.4.5-5.1
libgstallocators-1_0-0-debuginfo-1.4.5-5.1
libgstapp-1_0-0-debuginfo-1.4.5-5.1
libgstrtp-1_0-0-1.4.5-5.1

noarch

gstreamer-plugins-base-lang-1.4.5-5.1

x86_64

libgstsd-1_0-0-debuginfo-32bit-1.4.5-5.1
libgstvideo-1_0-0-debuginfo-32bit-1.4.5-5.1
typelib-1_0-GstPbutils-1_0-1.4.5-5.1
libgstfft-1_0-0-debuginfo-32bit-1.4.5-5.1
typelib-1_0-GstVideo-1_0-1.4.5-5.1
libgstfft-1_0-0-1.4.5-5.1
libgsttag-1_0-0-32bit-1.4.5-5.1
libgstsd-1_0-0-debuginfo-1.4.5-5.1
libgstpbutils-1_0-0-debuginfo-32bit-1.4.5-5.1

libgstrtp-1_0-0-debuginfo-1.4.5-5.1
libgstriff-1_0-0-debuginfo-32bit-1.4.5-5.1
typelib-1_0-GstAllocators-1_0-1.4.5-5.1
typelib-1_0-GstApp-1_0-1.4.5-5.1
gstreamer-plugins-base-debuginfo-32bit-1.4.5-5.1
typelib-1_0-GstRtp-1_0-1.4.5-5.1
libgstaudio-1_0-0-1.4.5-5.1
libgstpbutils-1_0-0-1.4.5-5.1
libgsttag-1_0-0-debuginfo-32bit-1.4.5-5.1
libgstallocators-1_0-0-32bit-1.4.5-5.1
libgstrtp-1_0-0-debuginfo-32bit-1.4.5-5.1
libgstrtsp-1_0-0-1.4.5-5.1
libgstvideo-1_0-0-32bit-1.4.5-5.1
libgstapp-1_0-0-debuginfo-32bit-1.4.5-5.1
libgstrtsp-1_0-0-debuginfo-32bit-1.4.5-5.1
libgstrtsp-1_0-0-32bit-1.4.5-5.1
libgstvideo-1_0-0-debuginfo-1.4.5-5.1
libgstrtsp-1_0-0-debuginfo-1.4.5-5.1
gstreamer-plugins-base-devel-1.4.5-5.1
typelib-1_0-GstTag-1_0-1.4.5-5.1
typelib-1_0-GstSdp-1_0-1.4.5-5.1
libgstallocators-1_0-0-1.4.5-5.1
libgstsdp-1_0-0-32bit-1.4.5-5.1
libgstpbutils-1_0-0-debuginfo-1.4.5-5.1
libgstsdp-1_0-0-1.4.5-5.1
libgstrtp-1_0-0-32bit-1.4.5-5.1
libgstallocators-1_0-0-debuginfo-32bit-1.4.5-5.1
typelib-1_0-GstRtsp-1_0-1.4.5-5.1
typelib-1_0-GstFft-1_0-1.4.5-5.1
gstreamer-plugins-base-1.4.5-5.1
libgsttag-1_0-0-debuginfo-1.4.5-5.1
libgstaudio-1_0-0-32bit-1.4.5-5.1
libgstfft-1_0-0-32bit-1.4.5-5.1
typelib-1_0-GstAudio-1_0-1.4.5-5.1
gstreamer-plugins-base-debugsource-1.4.5-5.1
libgstaudio-1_0-0-debuginfo-32bit-1.4.5-5.1
libgstvideo-1_0-0-1.4.5-5.1
typelib-1_0-GstRiff-1_0-1.4.5-5.1
libgstpbutils-1_0-0-32bit-1.4.5-5.1
libgstapp-1_0-0-1.4.5-5.1
gstreamer-plugins-base-32bit-1.4.5-5.1
gstreamer-plugins-base-debuginfo-1.4.5-5.1
libgstaudio-1_0-0-debuginfo-1.4.5-5.1
gstreamer-plugins-base-doc-1.4.5-5.1
libgstapp-1_0-0-32bit-1.4.5-5.1
libgstriff-1_0-0-debuginfo-1.4.5-5.1
libgstriff-1_0-0-1.4.5-5.1
libgstriff-1_0-0-32bit-1.4.5-5.1
libgstfft-1_0-0-debuginfo-1.4.5-5.1
libgsttag-1_0-0-1.4.5-5.1
libgstallocators-1_0-0-debuginfo-1.4.5-5.1
libgstapp-1_0-0-debuginfo-1.4.5-5.1
libgstrtp-1_0-0-1.4.5-5.1

145780 - SuSE Linux 42.2 openSUSE-SU-2017:0618-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-8318, CVE-2016-8327, CVE-2017-3238, CVE-2017-3244, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-

2017-3273, CVE-2017-3291, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0618-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00010.html>

SuSE Linux 42.2

x86_64

mysql-community-server-client-5.6.35-22.1
mysql-community-server-errormessages-5.6.35-22.1
libmysql56client18-debuginfo-32bit-5.6.35-22.1
libmysql56client_r18-32bit-5.6.35-22.1
libmysql56client18-32bit-5.6.35-22.1
libmysql56client18-5.6.35-22.1
mysql-community-server-test-5.6.35-22.1
libmysql56client18-debuginfo-5.6.35-22.1
mysql-community-server-tools-5.6.35-22.1
mysql-community-server-bench-5.6.35-22.1
mysql-community-server-5.6.35-22.1
mysql-community-server-client-debuginfo-5.6.35-22.1
mysql-community-server-tools-debuginfo-5.6.35-22.1
libmysql56client_r18-5.6.35-22.1
mysql-community-server-bench-debuginfo-5.6.35-22.1
mysql-community-server-test-debuginfo-5.6.35-22.1
mysql-community-server-debugsource-5.6.35-22.1
mysql-community-server-debuginfo-5.6.35-22.1

i586

mysql-community-server-client-5.6.35-22.1
mysql-community-server-errormessages-5.6.35-22.1
libmysql56client18-5.6.35-22.1
mysql-community-server-test-5.6.35-22.1
libmysql56client18-debuginfo-5.6.35-22.1
mysql-community-server-tools-5.6.35-22.1
mysql-community-server-bench-5.6.35-22.1
mysql-community-server-5.6.35-22.1
mysql-community-server-client-debuginfo-5.6.35-22.1
mysql-community-server-tools-debuginfo-5.6.35-22.1
libmysql56client_r18-5.6.35-22.1
mysql-community-server-bench-debuginfo-5.6.35-22.1
mysql-community-server-test-debuginfo-5.6.35-22.1
mysql-community-server-debugsource-5.6.35-22.1
mysql-community-server-debuginfo-5.6.35-22.1

145785 - SuSE Linux 42.2 openSUSE-SU-2017:1700-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-9526

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1700-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00104.html>

SuSE Linux 42.2

x86_64

libgrypt-devel-32bit-1.6.1-34.3.1

libgrypt20-32bit-1.6.1-34.3.1

libgrypt-devel-debuginfo-32bit-1.6.1-34.3.1

libgrypt-cavs-debuginfo-1.6.1-34.3.1

libgrypt-debugsource-1.6.1-34.3.1

libgrypt-devel-1.6.1-34.3.1

libgrypt-devel-debuginfo-1.6.1-34.3.1

libgrypt20-1.6.1-34.3.1

libgrypt20-debuginfo-32bit-1.6.1-34.3.1

libgrypt20-debuginfo-1.6.1-34.3.1

libgrypt-cavs-1.6.1-34.3.1

libgrypt20-hmac-32bit-1.6.1-34.3.1

libgrypt20-hmac-1.6.1-34.3.1

i586

libgrypt-devel-debuginfo-1.6.1-34.3.1

libgrypt20-hmac-1.6.1-34.3.1

libgrypt20-debuginfo-1.6.1-34.3.1

libgrypt-debugsource-1.6.1-34.3.1

libgrypt-cavs-debuginfo-1.6.1-34.3.1

libgrypt20-1.6.1-34.3.1

libgrypt-devel-1.6.1-34.3.1

libgrypt-cavs-1.6.1-34.3.1

145793 - SuSE Linux 42.2 openSUSE-SU-2017:1413-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-8350, CVE-2017-8351, CVE-2017-8353, CVE-2017-8355

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1413-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00085.html>

SuSE Linux 42.2

x86_64

GraphicsMagick-debuginfo-1.3.25-11.6.1

GraphicsMagick-devel-1.3.25-11.6.1

libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.6.1

GraphicsMagick-debugsource-1.3.25-11.6.1

libGraphicsMagick3-config-1.3.25-11.6.1
libGraphicsMagick++-devel-1.3.25-11.6.1
perl-GraphicsMagick-debuginfo-1.3.25-11.6.1
perl-GraphicsMagick-1.3.25-11.6.1
GraphicsMagick-1.3.25-11.6.1
libGraphicsMagickWand-Q16-2-1.3.25-11.6.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.6.1
libGraphicsMagick-Q16-3-1.3.25-11.6.1
libGraphicsMagick++-Q16-12-1.3.25-11.6.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.6.1

i586

GraphicsMagick-debuginfo-1.3.25-11.6.1
GraphicsMagick-devel-1.3.25-11.6.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.6.1
GraphicsMagick-debugsource-1.3.25-11.6.1
libGraphicsMagick3-config-1.3.25-11.6.1
libGraphicsMagick++-devel-1.3.25-11.6.1
perl-GraphicsMagick-debuginfo-1.3.25-11.6.1
perl-GraphicsMagick-1.3.25-11.6.1
GraphicsMagick-1.3.25-11.6.1
libGraphicsMagickWand-Q16-2-1.3.25-11.6.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.6.1
libGraphicsMagick-Q16-3-1.3.25-11.6.1
libGraphicsMagick++-Q16-12-1.3.25-11.6.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.6.1

145799 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0501-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5938

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:0501-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00082.html>

SuSE Linux 42.1

noarch

viewvc-1.1.26-5.1

SuSE Linux 42.2

noarch

viewvc-1.1.26-6.1

145812 - SuSE Linux 42.2 openSUSE-SU-2017:0707-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10028, CVE-2016-10029, CVE-2016-10155, CVE-2016-9921, CVE-2016-9922, CVE-2017-2615, CVE-2017-2620, CVE-2017-5525, CVE-2017-5526, CVE-2017-5552, CVE-2017-5578, CVE-2017-5667, CVE-2017-5856, CVE-2017-5857, CVE-2017-

5898

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0707-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00046.html>

SuSE Linux 42.2

i586

qemu-tools-2.6.2-29.4
qemu-guest-agent-2.6.2-29.4
qemu-block-dmg-2.6.2-29.4
qemu-testsuite-2.6.2-29.8
qemu-debugsource-2.6.2-29.4
qemu-linux-user-debugsource-2.6.2-29.1
qemu-linux-user-2.6.2-29.1
qemu-block-ssh-debuginfo-2.6.2-29.4
qemu-kvm-2.6.2-29.4
qemu-lang-2.6.2-29.4
qemu-s390-2.6.2-29.4
qemu-extra-2.6.2-29.4
qemu-arm-2.6.2-29.4
qemu-x86-debuginfo-2.6.2-29.4
qemu-linux-user-debuginfo-2.6.2-29.1
qemu-ppc-debuginfo-2.6.2-29.4
qemu-block-ssh-2.6.2-29.4
qemu-extra-debuginfo-2.6.2-29.4
qemu-2.6.2-29.4
qemu-x86-2.6.2-29.4
qemu-arm-debuginfo-2.6.2-29.4
qemu-block-iscsi-debuginfo-2.6.2-29.4
qemu-guest-agent-debuginfo-2.6.2-29.4
qemu-block-dmg-debuginfo-2.6.2-29.4
qemu-s390-debuginfo-2.6.2-29.4
qemu-block-curl-debuginfo-2.6.2-29.4
qemu-block-iscsi-2.6.2-29.4
qemu-block-curl-2.6.2-29.4
qemu-tools-debuginfo-2.6.2-29.4
qemu-ppc-2.6.2-29.4

noarch

qemu-ipxe-1.0.0-29.4
qemu-vgabios-1.9.1-29.4
qemu-sgabios-8-29.4
qemu-seabios-1.9.1-29.4

x86_64

qemu-tools-2.6.2-29.4
qemu-guest-agent-2.6.2-29.4
qemu-block-dmg-2.6.2-29.4
qemu-block-rbd-debuginfo-2.6.2-29.4
qemu-testsuite-2.6.2-29.8
qemu-debugsource-2.6.2-29.4
qemu-linux-user-debugsource-2.6.2-29.1

qemu-linux-user-2.6.2-29.1
qemu-block-ssh-debuginfo-2.6.2-29.4
qemu-block-rbd-2.6.2-29.4
qemu-kvm-2.6.2-29.4
qemu-lang-2.6.2-29.4
qemu-s390-2.6.2-29.4
qemu-extra-2.6.2-29.4
qemu-arm-2.6.2-29.4
qemu-x86-debuginfo-2.6.2-29.4
qemu-linux-user-debuginfo-2.6.2-29.1
qemu-ppc-debuginfo-2.6.2-29.4
qemu-block-ssh-2.6.2-29.4
qemu-extra-debuginfo-2.6.2-29.4
qemu-2.6.2-29.4
qemu-x86-2.6.2-29.4
qemu-arm-debuginfo-2.6.2-29.4
qemu-block-iscsi-debuginfo-2.6.2-29.4
qemu-guest-agent-debuginfo-2.6.2-29.4
qemu-block-dmg-debuginfo-2.6.2-29.4
qemu-s390-debuginfo-2.6.2-29.4
qemu-block-curl-debuginfo-2.6.2-29.4
qemu-block-iscsi-2.6.2-29.4
qemu-block-curl-2.6.2-29.4
qemu-tools-debuginfo-2.6.2-29.4
qemu-ppc-2.6.2-29.4

145819 - SuSE Linux 42.2 openSUSE-SU-2017:1595-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-8108

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1595-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00062.html>

SuSE Linux 42.2

noarch

lynis-2.5.1-2.3.1

145823 - SuSE Linux 42.2 openSUSE-SU-2017:0311-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9811

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0311-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00155.html>

SuSE Linux 42.2

i586

libgstpbutils-1_0-0-1.8.3-3.1
libgstvideo-1_0-0-1.8.3-3.1
gstreamer-plugins-base-devel-1.8.3-3.1
typelib-1_0-GstSdp-1_0-1.8.3-3.1
gstreamer-plugins-base-1.8.3-3.1
typelib-1_0-GstRtsp-1_0-1.8.3-3.1
libgstapp-1_0-0-1.8.3-3.1
libgstfft-1_0-0-debuginfo-1.8.3-3.1
typelib-1_0-GstFft-1_0-1.8.3-3.1
libgstapp-1_0-0-debuginfo-1.8.3-3.1
libgstvideo-1_0-0-debuginfo-1.8.3-3.1
gstreamer-plugins-base-debuginfo-1.8.3-3.1
libgstrtp-1_0-0-debuginfo-1.8.3-3.1
typelib-1_0-GstAudio-1_0-1.8.3-3.1
libgsttriff-1_0-0-debuginfo-1.8.3-3.1
typelib-1_0-GstApp-1_0-1.8.3-3.1
libgsttriff-1_0-0-1.8.3-3.1
libgsttag-1_0-0-debuginfo-1.8.3-3.1
libgstaudio-1_0-0-1.8.3-3.1
libgstallocators-1_0-0-debuginfo-1.8.3-3.1
libgstpbutils-1_0-0-debuginfo-1.8.3-3.1
typelib-1_0-GstPbutils-1_0-1.8.3-3.1
typelib-1_0-GstVideo-1_0-1.8.3-3.1
typelib-1_0-GstTag-1_0-1.8.3-3.1
typelib-1_0-GstRtp-1_0-1.8.3-3.1
libgstsdp-1_0-0-debuginfo-1.8.3-3.1
libgstsdp-1_0-0-1.8.3-3.1
libgsttag-1_0-0-1.8.3-3.1
libgstrtp-1_0-0-1.8.3-3.1
libgstrtp-1_0-0-debuginfo-1.8.3-3.1
libgstfft-1_0-0-1.8.3-3.1
gstreamer-plugins-base-doc-1.8.3-3.1
typelib-1_0-GstAllocators-1_0-1.8.3-3.1
gstreamer-plugins-base-debugsource-1.8.3-3.1
libgstrtp-1_0-0-1.8.3-3.1
libgstaudio-1_0-0-debuginfo-1.8.3-3.1
libgstallocators-1_0-0-1.8.3-3.1

noarch

gstreamer-plugins-base-lang-1.8.3-3.1

x86_64

libgstrtp-1_0-0-32bit-1.8.3-3.1
libgstpbutils-1_0-0-1.8.3-3.1
libgstvideo-1_0-0-1.8.3-3.1
gstreamer-plugins-base-devel-1.8.3-3.1
typelib-1_0-GstSdp-1_0-1.8.3-3.1
gstreamer-plugins-base-1.8.3-3.1
libgstallocators-1_0-0-debuginfo-32bit-1.8.3-3.1
typelib-1_0-GstRtsp-1_0-1.8.3-3.1
libgstallocators-1_0-0-32bit-1.8.3-3.1
libgstapp-1_0-0-1.8.3-3.1

libgstrtp-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstfft-1_0-0-debuginfo-1.8.3-3.1
typelib-1_0-GstFft-1_0-1.8.3-3.1
libgstapp-1_0-0-debuginfo-1.8.3-3.1
libgstvideo-1_0-0-debuginfo-1.8.3-3.1
gstreamer-plugins-base-debuginfo-1.8.3-3.1
libgstrtp-1_0-0-debuginfo-1.8.3-3.1
gstreamer-plugins-base-32bit-1.8.3-3.1
typelib-1_0-GstAudio-1_0-1.8.3-3.1
libgstriff-1_0-0-debuginfo-1.8.3-3.1
typelib-1_0-GstApp-1_0-1.8.3-3.1
libgstriff-1_0-0-1.8.3-3.1
libgsttag-1_0-0-debuginfo-1.8.3-3.1
libgstaudio-1_0-0-1.8.3-3.1
libgstallocators-1_0-0-debuginfo-1.8.3-3.1
libgstpbutils-1_0-0-debuginfo-1.8.3-3.1
gstreamer-plugins-base-devel-32bit-1.8.3-3.1
libgstfft-1_0-0-debuginfo-32bit-1.8.3-3.1
typelib-1_0-GstPbutils-1_0-1.8.3-3.1
libgstaudio-1_0-0-debuginfo-32bit-1.8.3-3.1
typelib-1_0-GstVideo-1_0-1.8.3-3.1
libgstaudio-1_0-0-32bit-1.8.3-3.1
libgstvideo-1_0-0-debuginfo-32bit-1.8.3-3.1
typelib-1_0-GstTag-1_0-1.8.3-3.1
typelib-1_0-GstRtp-1_0-1.8.3-3.1
libgstsdp-1_0-0-debuginfo-1.8.3-3.1
libgstriff-1_0-0-32bit-1.8.3-3.1
libgstvideo-1_0-0-32bit-1.8.3-3.1
libgsttag-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstsdp-1_0-0-1.8.3-3.1
libgsttag-1_0-0-1.8.3-3.1
libgstriff-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstrtp-1_0-0-32bit-1.8.3-3.1
libgstrtp-1_0-0-1.8.3-3.1
gstreamer-plugins-base-debuginfo-32bit-1.8.3-3.1
libgstapp-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstapp-1_0-0-32bit-1.8.3-3.1
libgstrtp-1_0-0-debuginfo-1.8.3-3.1
libgstfft-1_0-0-1.8.3-3.1
gstreamer-plugins-base-doc-1.8.3-3.1
typelib-1_0-GstAllocators-1_0-1.8.3-3.1
libgstpbutils-1_0-0-32bit-1.8.3-3.1
gstreamer-plugins-base-debugsource-1.8.3-3.1
libgstrtp-1_0-0-1.8.3-3.1
libgstfft-1_0-0-32bit-1.8.3-3.1
libgstsdp-1_0-0-32bit-1.8.3-3.1
libgstrtp-1_0-0-debuginfo-32bit-1.8.3-3.1
libgsttag-1_0-0-32bit-1.8.3-3.1
libgstpbutils-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstsdp-1_0-0-debuginfo-32bit-1.8.3-3.1
libgstaudio-1_0-0-debuginfo-1.8.3-3.1
libgstallocators-1_0-0-1.8.3-3.1

145824 - SuSE Linux 42.1 openSUSE-SU-2017:1079-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5837, CVE-2017-5844

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1079-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00084.html>

SuSE Linux 42.1

i586

libgstapp-0_10-0-0.10.36-17.1

typelib-1_0-GstInterfaces-0_10-0.10.36-17.1

gststreamer-0_10-plugins-base-debugsource-0.10.36-17.1

gststreamer-0_10-plugins-base-doc-0.10.36-17.1

gststreamer-0_10-plugins-base-0.10.36-17.1

gststreamer-0_10-plugins-base-debuginfo-0.10.36-17.1

gststreamer-0_10-plugins-base-devel-0.10.36-17.1

typelib-1_0-GstApp-0_10-0.10.36-17.1

gststreamer-0_10-plugin-gnomevfs-debuginfo-0.10.36-17.1

libgstinterfaces-0_10-0-debuginfo-0.10.36-17.1

gststreamer-0_10-plugin-gnomevfs-0.10.36-17.1

libgstinterfaces-0_10-0-0.10.36-17.1

libgstapp-0_10-0-debuginfo-0.10.36-17.1

noarch

gststreamer-0_10-plugins-base-lang-0.10.36-17.1

x86_64

gststreamer-0_10-plugins-base-debuginfo-32bit-0.10.36-17.1

libgstapp-0_10-0-0.10.36-17.1

libgstinterfaces-0_10-0-debuginfo-32bit-0.10.36-17.1

typelib-1_0-GstInterfaces-0_10-0.10.36-17.1

libgstinterfaces-0_10-0-32bit-0.10.36-17.1

gststreamer-0_10-plugins-base-debugsource-0.10.36-17.1

libgstapp-0_10-0-debuginfo-32bit-0.10.36-17.1

gststreamer-0_10-plugins-base-32bit-0.10.36-17.1

gststreamer-0_10-plugins-base-doc-0.10.36-17.1

gststreamer-0_10-plugins-base-0.10.36-17.1

gststreamer-0_10-plugins-base-debuginfo-0.10.36-17.1

gststreamer-0_10-plugins-base-devel-0.10.36-17.1

typelib-1_0-GstApp-0_10-0.10.36-17.1

gststreamer-0_10-plugin-gnomevfs-debuginfo-0.10.36-17.1

libgstinterfaces-0_10-0-debuginfo-0.10.36-17.1

gststreamer-0_10-plugin-gnomevfs-0.10.36-17.1

libgstinterfaces-0_10-0-0.10.36-17.1

libgstapp-0_10-0-debuginfo-0.10.36-17.1

libgstapp-0_10-0-32bit-0.10.36-17.1

145849 - SuSE Linux 42.2 openSUSE-SU-2017:0251-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6225

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:0251-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00126.html>

SuSE Linux 42.2
x86_64
xtrabackup-debuginfo-2.3.6-3.1
xtrabackup-test-2.3.6-3.1
xtrabackup-2.3.6-3.1
xtrabackup-debugsource-2.3.6-3.1

145853 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0742-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6820

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0742-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00056.html>

SuSE Linux 42.1
noarch
roundcubemail-1.1.8-18.1

SuSE Linux 42.2
noarch
roundcubemail-1.1.8-18.1

145854 - SuSE Linux 42.2 openSUSE-SU-2017:0515-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5589

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0515-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00094.html>

SuSE Linux 42.2
x86_64
mcabber-1.0.5-6.1
mcabber-debuginfo-1.0.5-6.1
mcabber-devel-1.0.5-6.1
mcabber-debugsource-1.0.5-6.1

145856 - SuSE Linux 42.3 openSUSE-SU-2017:2181-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-9287

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:2181-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-08/msg00063.html>

SuSE Linux 42.3

i586

openldap2-back-sql-debuginfo-2.4.44-18.1
openldap2-client-2.4.44-18.1
openldap2-ppolicy-check-password-1.2-18.1
openldap2-devel-2.4.44-18.1
openldap2-back-meta-2.4.44-18.1
openldap2-back-sql-2.4.44-18.1
openldap2-back-sock-debuginfo-2.4.44-18.1
openldap2-back-meta-debuginfo-2.4.44-18.1
openldap2-back-sock-2.4.44-18.1
openldap2-ppolicy-check-password-debuginfo-1.2-18.1
libldap-2_4-2-debuginfo-2.4.44-18.1
openldap2-debuginfo-2.4.44-18.1
openldap2-debugsource-2.4.44-18.1
openldap2-back-perl-debuginfo-2.4.44-18.1
openldap2-back-perl-2.4.44-18.1
openldap2-client-debuginfo-2.4.44-18.1
openldap2-devel-static-2.4.44-18.1
openldap2-2.4.44-18.1
openldap2-contrib-2.4.44-18.1
openldap2-contrib-debuginfo-2.4.44-18.1
libldap-2_4-2-2.4.44-18.1

noarch

openldap2-doc-2.4.44-18.1
libldap-data-2.4.44-18.1

x86_64

libldap-2_4-2-32bit-2.4.44-18.1
openldap2-back-sql-debuginfo-2.4.44-18.1
openldap2-client-2.4.44-18.1
openldap2-ppolicy-check-password-1.2-18.1
openldap2-devel-2.4.44-18.1
openldap2-back-meta-2.4.44-18.1

openldap2-back-sql-2.4.44-18.1
openldap2-back-sock-debuginfo-2.4.44-18.1
openldap2-back-meta-debuginfo-2.4.44-18.1
openldap2-back-sock-2.4.44-18.1
openldap2-ppolicy-check-password-debuginfo-1.2-18.1
libldap-2_4-2-debuginfo-2.4.44-18.1
openldap2-debuginfo-2.4.44-18.1
libldap-2_4-2-debuginfo-32bit-2.4.44-18.1
openldap2-debugsource-2.4.44-18.1
openldap2-back-perl-debuginfo-2.4.44-18.1
openldap2-devel-32bit-2.4.44-18.1
openldap2-back-perl-2.4.44-18.1
openldap2-client-debuginfo-2.4.44-18.1
openldap2-devel-static-2.4.44-18.1
openldap2-2.4.44-18.1
openldap2-contrib-2.4.44-18.1
openldap2-contrib-debuginfo-2.4.44-18.1
libldap-2_4-2-2.4.44-18.1

145873 - SuSE Linux 42.2 openSUSE-SU-2017:1530-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-3469

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1530-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00029.html>

SuSE Linux 42.2

x86_64

mysql-workbench-debugsource-6.3.9-2.5.2
libmysqlcppconn7-debuginfo-1.1.8-5.3.2
mysql-connector-cpp-debugsource-1.1.8-5.3.2
mysql-workbench-debuginfo-6.3.9-2.5.2
libmysqlcppconn7-1.1.8-5.3.2
libmysqlcppconn-devel-1.1.8-5.3.2
mysql-workbench-6.3.9-2.5.2

i586

libmysqlcppconn7-1.1.8-5.3.2
mysql-connector-cpp-debugsource-1.1.8-5.3.2
libmysqlcppconn-devel-1.1.8-5.3.2
libmysqlcppconn7-debuginfo-1.1.8-5.3.2

145880 - SuSE Linux 42.1 openSUSE-SU-2017:0250-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6225

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0250-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00125.html>

SuSE Linux 42.1

x86_64

xtrabackup-2.2.12-8.1

xtrabackup-debuginfo-2.2.12-8.1

xtrabackup-debugsource-2.2.12-8.1

xtrabackup-test-2.2.12-8.1

i586

xtrabackup-2.2.12-8.1

xtrabackup-debuginfo-2.2.12-8.1

xtrabackup-debugsource-2.2.12-8.1

xtrabackup-test-2.2.12-8.1

163449 - Oracle Enterprise Linux ELSA-2017-2563 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6210

Description

The scan detected that the host is missing the following update:
ELSA-2017-2563

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-August/007169.html>

OEL6

x86_64

openssh-5.3p1-123.el6_9

openssh-server-5.3p1-123.el6_9

pam_ssh_agent_auth-0.9.3-123.el6_9

openssh-askpass-5.3p1-123.el6_9

openssh-ldap-5.3p1-123.el6_9

openssh-clients-5.3p1-123.el6_9

i386

openssh-5.3p1-123.el6_9

openssh-server-5.3p1-123.el6_9

pam_ssh_agent_auth-0.9.3-123.el6_9

openssh-askpass-5.3p1-123.el6_9

openssh-ldap-5.3p1-123.el6_9

openssh-clients-5.3p1-123.el6_9

170852 - Amazon Linux AMI ALAS-2017-875 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-7488

Description

The scan detected that the host is missing the following update:
ALAS-2017-875

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://alas.aws.amazon.com/ALAS-2017-875.html>

Amazon Linux AMI

x86_64

authconfig-6.2.8-30.30.amzn1

authconfig-debuginfo-6.2.8-30.30.amzn1

i686

authconfig-6.2.8-30.30.amzn1

authconfig-debuginfo-6.2.8-30.30.amzn1

170858 - Amazon Linux AMI ALAS-2017-881 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6508

Description

The scan detected that the host is missing the following update:
ALAS-2017-881

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://alas.aws.amazon.com/ALAS-2017-881.html>

Amazon Linux AMI

x86_64

wget-1.18-3.27.amzn1

wget-debuginfo-1.18-3.27.amzn1

i686

wget-debuginfo-1.18-3.27.amzn1

wget-1.18-3.27.amzn1

170864 - Amazon Linux AMI ALAS-2017-887 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-3635, CVE-2017-3636, CVE-2017-3641, CVE-2017-3648, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Description

The scan detected that the host is missing the following update:

ALAS-2017-887

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://alas.aws.amazon.com/ALAS-2017-887.html>

Amazon Linux AMI

x86_64

mysql55-server-5.5.57-1.18.amzn1

mysql55-5.5.57-1.18.amzn1

mysql55-libs-5.5.57-1.18.amzn1

mysql55-debuginfo-5.5.57-1.18.amzn1

mysql55-embedded-devel-5.5.57-1.18.amzn1

mysql55-bench-5.5.57-1.18.amzn1

mysql55-test-5.5.57-1.18.amzn1

mysql55-embedded-5.5.57-1.18.amzn1

mysql-config-5.5.57-1.18.amzn1

mysql55-devel-5.5.57-1.18.amzn1

i686

mysql55-server-5.5.57-1.18.amzn1

mysql-config-5.5.57-1.18.amzn1

mysql55-5.5.57-1.18.amzn1

mysql55-libs-5.5.57-1.18.amzn1

mysql55-debuginfo-5.5.57-1.18.amzn1

mysql55-embedded-devel-5.5.57-1.18.amzn1

mysql55-bench-5.5.57-1.18.amzn1

mysql55-test-5.5.57-1.18.amzn1

mysql55-embedded-5.5.57-1.18.amzn1

mysql55-devel-5.5.57-1.18.amzn1

175253 - Scientific Linux Security ERRATA Moderate: openssh on SL6.x i386/x86_64 (1708-24483)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2016-6210

Description

The scan detected that the host is missing the following update:

Security ERRATA Moderate: openssh on SL6.x i386/x86_64 (1708-24483)

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=24483>

SL6

x86_64

openssh-5.3p1-123.el6_9

openssh-server-5.3p1-123.el6_9

pam_ssh_agent_auth-0.9.3-123.el6_9

openssh-askpass-5.3p1-123.el6_9

openssh-ldap-5.3p1-123.el6_9
openssh-debuginfo-5.3p1-123.el6_9
openssh-clients-5.3p1-123.el6_9

i386

openssh-5.3p1-123.el6_9
openssh-server-5.3p1-123.el6_9
pam_ssh_agent_auth-0.9.3-123.el6_9
openssh-askpass-5.3p1-123.el6_9
openssh-ldap-5.3p1-123.el6_9
openssh-debuginfo-5.3p1-123.el6_9
openssh-clients-5.3p1-123.el6_9

192589 - Fedora Linux 26 FEDORA-2017-c0cdc6ebdd Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-12927, CVE-2017-12978

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c0cdc6ebdd

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

cacti-1.1.19-1.fc26

192594 - Fedora Linux 26 FEDORA-2017-06cace06ce Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-12982

Description

The scan detected that the host is missing the following update:
FEDORA-2017-06cace06ce

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 26

mingw-openjpeg2-2.2.0-2.fc26

openjpeg2-2.2.0-2.fc26

192599 - Fedora Linux 26 FEDORA-2017-7cc0e6a5f5 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6362, CVE-2017-7890

Description

The scan detected that the host is missing the following update:

FEDORA-2017-7cc0e6a5f5

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 26

gd-2.2.5-1.fc26

192601 - Fedora Linux 25 FEDORA-2017-2f1ca6beb7 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-12927, CVE-2017-12978

Description

The scan detected that the host is missing the following update:

FEDORA-2017-2f1ca6beb7

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=2>

Fedora Core 25

cacti-1.1.19-1.fc25

130869 - Debian Linux 8.0, 9.0 DSA-3961-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-6362

Description

The scan detected that the host is missing the following update:

DSA-3961-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.debian.org/security/2017/dsa-3961>

Debian 8.0
all
libgd3_2.1.0-5+deb8u11
libgd2-xpm-dev_2.1.0-5+deb8u11
libgd-tools_2.1.0-5+deb8u11
libgd2-noxpm-dev_2.1.0-5+deb8u11
libgd-dev_2.1.0-5+deb8u11
libgd-dbg_2.1.0-5+deb8u11

Debian 9.0
all
libgd3_2.2.4-2+deb9u2
libgd-dev_2.2.4-2+deb9u2
libgd-tools_2.2.4-2+deb9u2

130870 - Debian Linux 8.0, 9.0 DSA-3964-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-14099, CVE-2017-14100

Description

The scan detected that the host is missing the following update:

DSA-3964-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.debian.org/security/2017/dsa-3964>

Debian 8.0
all
asterisk_1:11.13.1~dfsg-2+deb8u3

Debian 9.0
all
asterisk_1:13.14.1~dfsg-2+deb9u1

130873 - Debian Linux 8.0 DSA-3960-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-7526

Description

The scan detected that the host is missing the following update:

DSA-3960-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.debian.org/security/2017/dsa-3960>

Debian 8.0

all
gnupg_1.4.18-7+deb8u4

145527 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0488-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-5930

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0488-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00076.html>

SuSE Linux 42.1
noarch
postfixadmin-3.0.2-5.1

SuSE Linux 42.2
noarch
postfixadmin-3.0.2-3.1

145593 - SuSE Linux 42.2 openSUSE-SU-2017:0827-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2015-5191

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0827-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00092.html>

SuSE Linux 42.2
x86_64
open-vm-tools-desktop-10.1.0-3.1
libvmttools-devel-10.1.0-3.1
open-vm-tools-debugsource-10.1.0-3.1
libvmttools0-debuginfo-10.1.0-3.1
open-vm-tools-10.1.0-3.1
open-vm-tools-desktop-debuginfo-10.1.0-3.1
open-vm-tools-debuginfo-10.1.0-3.1
libvmttools0-10.1.0-3.1

145612 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0826-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0826-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00091.html>

SuSE Linux 42.1

i586

dbus-1-x11-debugsource-1.8.22-13.1

dbus-1-devel-1.8.22-13.1

dbus-1-x11-debuginfo-1.8.22-13.1

libdbus-1-3-debuginfo-1.8.22-13.1

libdbus-1-3-1.8.22-13.1

dbus-1-debuginfo-1.8.22-13.1

dbus-1-x11-1.8.22-13.1

dbus-1-1.8.22-13.1

dbus-1-debugsource-1.8.22-13.1

noarch

dbus-1-devel-doc-1.8.22-13.1

x86_64

dbus-1-debugsource-1.8.22-13.1

libdbus-1-3-32bit-1.8.22-13.1

dbus-1-x11-debuginfo-1.8.22-13.1

dbus-1-1.8.22-13.1

libdbus-1-3-1.8.22-13.1

libdbus-1-3-debuginfo-1.8.22-13.1

libdbus-1-3-debuginfo-32bit-1.8.22-13.1

dbus-1-debuginfo-32bit-1.8.22-13.1

dbus-1-x11-debugsource-1.8.22-13.1

dbus-1-devel-1.8.22-13.1

dbus-1-devel-32bit-1.8.22-13.1

dbus-1-x11-1.8.22-13.1

dbus-1-debuginfo-1.8.22-13.1

SuSE Linux 42.2

i586

dbus-1-devel-1.8.22-3.1

dbus-1-x11-1.8.22-3.1

libdbus-1-3-debuginfo-1.8.22-3.1

dbus-1-x11-debugsource-1.8.22-3.1

dbus-1-debugsource-1.8.22-3.1

dbus-1-debuginfo-1.8.22-3.1

dbus-1-x11-debuginfo-1.8.22-3.1

dbus-1-1.8.22-3.1

libdbus-1-3-1.8.22-3.1

noarch

dbus-1-devel-doc-1.8.22-3.1

x86_64
dbus-1-1.8.22-3.1
dbus-1-x11-debuginfo-1.8.22-3.1
dbus-1-debugsource-1.8.22-3.1
dbus-1-devel-32bit-1.8.22-3.1
libdbus-1-3-32bit-1.8.22-3.1
dbus-1-x11-1.8.22-3.1
dbus-1-devel-1.8.22-3.1
dbus-1-debuginfo-1.8.22-3.1
libdbus-1-3-1.8.22-3.1
dbus-1-x11-debugsource-1.8.22-3.1
libdbus-1-3-debuginfo-32bit-1.8.22-3.1
dbus-1-debuginfo-32bit-1.8.22-3.1
libdbus-1-3-debuginfo-1.8.22-3.1

145729 - SuSE Linux 42.2 openSUSE-SU-2017:1506-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-10376

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1506-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00020.html>

SuSE Linux 42.2
noarch
gajim-0.16.7-2.3.1
gajim-lang-0.16.7-2.3.1

145864 - SuSE Linux 42.1 openSUSE-SU-2017:0509-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2015-5191

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0509-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-02/msg00088.html>

SuSE Linux 42.1
x86_64
libvmttools0-debuginfo-10.1.0-6.1

open-vm-tools-desktop-10.1.0-6.1
open-vm-tools-10.1.0-6.1
libvmttools-devel-10.1.0-6.1
libvmttools0-10.1.0-6.1
open-vm-tools-desktop-debuginfo-10.1.0-6.1
open-vm-tools-debuginfo-10.1.0-6.1
open-vm-tools-debugsource-10.1.0-6.1

i586

libvmttools0-debuginfo-10.1.0-6.1
open-vm-tools-desktop-10.1.0-6.1
open-vm-tools-10.1.0-6.1
libvmttools-devel-10.1.0-6.1
libvmttools0-10.1.0-6.1
open-vm-tools-desktop-debuginfo-10.1.0-6.1
open-vm-tools-debuginfo-10.1.0-6.1
open-vm-tools-debugsource-10.1.0-6.1

145882 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0663-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2014-4000

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0663-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00023.html>

SuSE Linux 42.1
noarch
cacti-doc-1.0.4-14.1
cacti-1.0.4-14.1

SuSE Linux 42.2
noarch
cacti-doc-1.0.4-14.1
cacti-1.0.4-14.1

182432 - FreeBSD gdk-pixbuf Multiple Vulnerabilities (5a1f1a86-8f4c-11e7-b5af-a4badb2f4699)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-2862, CVE-2017-2870

Description

The scan detected that the host is missing the following update:
gdk-pixbuf -- multiple vulnerabilities (5a1f1a86-8f4c-11e7-b5af-a4badb2f4699)

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.vuxml.org/freebsd/5a1f1a86-8f4c-11e7-b5af-a4badb2f4699.html>

Affected packages:
gtk-pixbuf2 < 2.36.7

182434 - FreeBSD asterisk Remote Crash Vulnerability In Res_pjsip (ec1df2a1-8ee6-11e7-8be8-001999f8d30b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-14098

Description

The scan detected that the host is missing the following update:
asterisk -- Remote Crash Vulnerability in res_pjsip (ec1df2a1-8ee6-11e7-8be8-001999f8d30b)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://www.vuxml.org/freebsd/ec1df2a1-8ee6-11e7-8be8-001999f8d30b.html>

Affected packages:
asterisk13 < 13.17.1

182435 - FreeBSD asterisk Unauthorized Data Disclosure And Shell Access Command Injection In App_minivm (c599f95c-8ee5-11e7-8be8-001999f8d30b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-14099, CVE-2017-14100

Description

The scan detected that the host is missing the following update:
asterisk -- Unauthorized data disclosure and shell access command injection in app_minivm (c599f95c-8ee5-11e7-8be8-001999f8d30b)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://www.vuxml.org/freebsd/c599f95c-8ee5-11e7-8be8-001999f8d30b.html>

Affected packages:
asterisk11 < 11.25.2
asterisk13 < 13.17.1

185866 - Ubuntu Linux 16.04, 17.04 USN-3407-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-11424

Description

The scan detected that the host is missing the following update:
USN-3407-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004032.html>

Ubuntu 17.04

python-jwt_1.4.2-1ubuntu0.1
python3-jwt_1.4.2-1ubuntu0.1

Ubuntu 16.04

python-jwt_1.3.0-1ubuntu0.1
python3-jwt_1.3.0-1ubuntu0.1

192585 - Fedora Linux 25 FEDORA-2017-4b4c022807 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-7558

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4b4c022807

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=2>

Fedora Core 25

kernel-4.12.9-200.fc25

192587 - Fedora Linux 26 FEDORA-2017-78c4c71539 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-7558

Description

The scan detected that the host is missing the following update:
FEDORA-2017-78c4c71539

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

kernel-4.12.9-300.fc26

192603 - Fedora Linux 26 FEDORA-2017-382c240580 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-14032

Description

The scan detected that the host is missing the following update:
FEDORA-2017-382c240580

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 26

mbedtls-2.6.0-1.fc26

192605 - Fedora Linux 25 FEDORA-2017-270ab2baa3 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-12133

Description

The scan detected that the host is missing the following update:
FEDORA-2017-270ab2baa3

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/9/?count=200&page=1>

Fedora Core 25

glibc-2.24-10.fc25

145563 - SuSE Linux 42.2 openSUSE-SU-2017:1402-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9401

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1402-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00082.html>

SuSE Linux 42.2

i586

bash-debugsource-4.3-80.3.1

bash-4.3-80.3.1

bash-loadables-debuginfo-4.3-80.3.1

bash-loadables-4.3-80.3.1

bash-debuginfo-4.3-80.3.1

libreadline6-6.3-80.3.1

bash-devel-4.3-80.3.1

libreadline6-debuginfo-6.3-80.3.1

readline-devel-6.3-80.3.1

noarch

bash-lang-4.3-80.3.1

bash-doc-4.3-80.3.1

readline-doc-6.3-80.3.1

x86_64

readline-devel-6.3-80.3.1

libreadline6-32bit-6.3-80.3.1

readline-devel-32bit-6.3-80.3.1

bash-loadables-debuginfo-4.3-80.3.1

bash-debuginfo-32bit-4.3-80.3.1

libreadline6-debuginfo-32bit-6.3-80.3.1

bash-debugsource-4.3-80.3.1

bash-debuginfo-4.3-80.3.1

bash-devel-4.3-80.3.1

libreadline6-6.3-80.3.1

libreadline6-debuginfo-6.3-80.3.1

bash-loadables-4.3-80.3.1

bash-4.3-80.3.1

145580 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1035-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-7418

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1035-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00062.html>

SuSE Linux 42.1

i586

proftpd-ldap-debuginfo-1.3.5d-7.1

proftpd-devel-1.3.5d-7.1
proftpd-radius-1.3.5d-7.1
proftpd-pgsql-1.3.5d-7.1
proftpd-ldap-1.3.5d-7.1
proftpd-debuginfo-1.3.5d-7.1
proftpd-doc-1.3.5d-7.1
proftpd-radius-debuginfo-1.3.5d-7.1
proftpd-sqlite-1.3.5d-7.1
proftpd-mysql-debuginfo-1.3.5d-7.1
proftpd-debugsource-1.3.5d-7.1
proftpd-pgsql-debuginfo-1.3.5d-7.1
proftpd-1.3.5d-7.1
proftpd-sqlite-debuginfo-1.3.5d-7.1
proftpd-mysql-1.3.5d-7.1

noarch
proftpd-lang-1.3.5d-7.1

x86_64
proftpd-ldap-debuginfo-1.3.5d-7.1
proftpd-devel-1.3.5d-7.1
proftpd-radius-1.3.5d-7.1
proftpd-pgsql-1.3.5d-7.1
proftpd-ldap-1.3.5d-7.1
proftpd-debuginfo-1.3.5d-7.1
proftpd-doc-1.3.5d-7.1
proftpd-radius-debuginfo-1.3.5d-7.1
proftpd-sqlite-1.3.5d-7.1
proftpd-mysql-debuginfo-1.3.5d-7.1
proftpd-debugsource-1.3.5d-7.1
proftpd-pgsql-debuginfo-1.3.5d-7.1
proftpd-1.3.5d-7.1
proftpd-sqlite-debuginfo-1.3.5d-7.1
proftpd-mysql-1.3.5d-7.1

SuSE Linux 42.2
i586

proftpd-pgsql-1.3.5d-6.3.1
proftpd-sqlite-debuginfo-1.3.5d-6.3.1
proftpd-radius-1.3.5d-6.3.1
proftpd-ldap-debuginfo-1.3.5d-6.3.1
proftpd-pgsql-debuginfo-1.3.5d-6.3.1
proftpd-sqlite-1.3.5d-6.3.1
proftpd-mysql-debuginfo-1.3.5d-6.3.1
proftpd-mysql-1.3.5d-6.3.1
proftpd-debuginfo-1.3.5d-6.3.1
proftpd-1.3.5d-6.3.1
proftpd-ldap-1.3.5d-6.3.1
proftpd-debugsource-1.3.5d-6.3.1
proftpd-radius-debuginfo-1.3.5d-6.3.1
proftpd-devel-1.3.5d-6.3.1
proftpd-doc-1.3.5d-6.3.1

noarch
proftpd-lang-1.3.5d-6.3.1

x86_64
proftpd-pgsql-1.3.5d-6.3.1
proftpd-sqlite-debuginfo-1.3.5d-6.3.1
proftpd-radius-1.3.5d-6.3.1

proftpd-ldap-debuginfo-1.3.5d-6.3.1
proftpd-pgsql-debuginfo-1.3.5d-6.3.1
proftpd-sqlite-1.3.5d-6.3.1
proftpd-mysql-debuginfo-1.3.5d-6.3.1
proftpd-mysql-1.3.5d-6.3.1
proftpd-debuginfo-1.3.5d-6.3.1
proftpd-1.3.5d-6.3.1
proftpd-ldap-1.3.5d-6.3.1
proftpd-debugsource-1.3.5d-6.3.1
proftpd-radius-debuginfo-1.3.5d-6.3.1
proftpd-devel-1.3.5d-6.3.1
proftpd-doc-1.3.5d-6.3.1

145652 - SuSE Linux 42.2 openSUSE-SU-2017:1625-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-1000369

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1625-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-06/msg00074.html>

SuSE Linux 42.2
x86_64
eximstats-html-4.86.2-10.3.1
eximon-debuginfo-4.86.2-10.3.1
exim-debuginfo-4.86.2-10.3.1
eximon-4.86.2-10.3.1
exim-4.86.2-10.3.1
exim-debugsource-4.86.2-10.3.1

145667 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1105-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9586, CVE-2017-7407

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1105-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00094.html>

SuSE Linux 42.1
x86_64

curl-debugsource-7.37.0-19.1
libcurl4-32bit-7.37.0-19.1
curl-debuginfo-7.37.0-19.1
libcurl4-debuginfo-7.37.0-19.1
libcurl-devel-7.37.0-19.1
libcurl-devel-32bit-7.37.0-19.1
libcurl4-7.37.0-19.1
libcurl4-debuginfo-32bit-7.37.0-19.1
curl-7.37.0-19.1

i586

curl-debugsource-7.37.0-19.1
curl-debuginfo-7.37.0-19.1
libcurl4-debuginfo-7.37.0-19.1
libcurl-devel-7.37.0-19.1
libcurl4-7.37.0-19.1
curl-7.37.0-19.1

SuSE Linux 42.2

x86_64

curl-debuginfo-7.37.0-16.3.1
libcurl-devel-32bit-7.37.0-16.3.1
curl-debugsource-7.37.0-16.3.1
curl-7.37.0-16.3.1
libcurl-devel-7.37.0-16.3.1
libcurl4-7.37.0-16.3.1
libcurl4-debuginfo-32bit-7.37.0-16.3.1
libcurl4-32bit-7.37.0-16.3.1
libcurl4-debuginfo-7.37.0-16.3.1

i586

curl-debuginfo-7.37.0-16.3.1
curl-debugsource-7.37.0-16.3.1
curl-7.37.0-16.3.1
libcurl-devel-7.37.0-16.3.1
libcurl4-7.37.0-16.3.1
libcurl4-debuginfo-7.37.0-16.3.1

145712 - SuSE Linux 42.2 openSUSE-SU-2017:0988-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-5985

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:0988-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-04/msg00043.html>

SuSE Linux 42.2

x86_64

lxc-devel-1.1.5-15.3.1
lxc-debuginfo-1.1.5-15.3.1

lxc-debugsource-1.1.5-15.3.1
lxc-1.1.5-15.3.1

145724 - SuSE Linux 42.1 openSUSE-SU-2017:0002-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9756

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0002-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-01/msg00000.html>

SuSE Linux 42.1

i586

kernel-syms-4.1.36-44.1
kernel-obs-qa-4.1.36-44.1
kernel-default-base-debuginfo-4.1.36-44.1
kernel-default-devel-4.1.36-44.1
kernel-obs-build-4.1.36-44.3
kernel-default-4.1.36-44.1
kernel-obs-build-debugsource-4.1.36-44.3
kernel-default-base-4.1.36-44.1
kernel-default-debuginfo-4.1.36-44.1
kernel-default-debugsource-4.1.36-44.1

i686

kernel-xen-debuginfo-4.1.36-44.1
kernel-ec2-4.1.36-44.1
kernel-pae-debuginfo-4.1.36-44.1
kernel-vanilla-debugsource-4.1.36-44.1
kernel-xen-devel-4.1.36-44.1
kernel-pv-devel-4.1.36-44.1
kernel-debug-devel-debuginfo-4.1.36-44.1
kernel-pv-debuginfo-4.1.36-44.1
kernel-ec2-debugsource-4.1.36-44.1
kernel-pae-4.1.36-44.1
kernel-pae-base-4.1.36-44.1
kernel-xen-4.1.36-44.1
kernel-debug-debugsource-4.1.36-44.1
kernel-vanilla-debuginfo-4.1.36-44.1
kernel-pae-debugsource-4.1.36-44.1
kernel-debug-4.1.36-44.1
kernel-ec2-debuginfo-4.1.36-44.1
kernel-pv-base-4.1.36-44.1
kernel-ec2-devel-4.1.36-44.1
kernel-pae-base-debuginfo-4.1.36-44.1
kernel-vanilla-devel-4.1.36-44.1
kernel-ec2-base-4.1.36-44.1
kernel-xen-debugsource-4.1.36-44.1
kernel-debug-base-debuginfo-4.1.36-44.1
kernel-pv-base-debuginfo-4.1.36-44.1

kernel-xen-base-4.1.36-44.1
kernel-pv-4.1.36-44.1
kernel-debug-devel-4.1.36-44.1
kernel-vanilla-4.1.36-44.1
kernel-ec2-base-debuginfo-4.1.36-44.1
kernel-pae-devel-4.1.36-44.1
kernel-pv-debugsource-4.1.36-44.1
kernel-debug-base-4.1.36-44.1
kernel-debug-debuginfo-4.1.36-44.1
kernel-xen-base-debuginfo-4.1.36-44.1

noarch

kernel-macros-4.1.36-44.1
kernel-docs-pdf-4.1.36-44.2
kernel-docs-html-4.1.36-44.2
kernel-docs-4.1.36-44.2
kernel-source-4.1.36-44.1
kernel-devel-4.1.36-44.1
kernel-source-vanilla-4.1.36-44.1

x86_64

kernel-xen-debuginfo-4.1.36-44.1
kernel-default-4.1.36-44.1
kernel-vanilla-debugsource-4.1.36-44.1
kernel-obs-qa-4.1.36-44.1
kernel-xen-devel-4.1.36-44.1
kernel-pv-devel-4.1.36-44.1
kernel-debug-devel-debuginfo-4.1.36-44.1
kernel-default-devel-4.1.36-44.1
kernel-ec2-4.1.36-44.1
kernel-default-base-4.1.36-44.1
kernel-ec2-debugsource-4.1.36-44.1
kernel-ec2-devel-4.1.36-44.1
kernel-debug-debugsource-4.1.36-44.1
kernel-vanilla-debuginfo-4.1.36-44.1
kernel-obs-build-4.1.36-44.3
kernel-ec2-debuginfo-4.1.36-44.1
kernel-pv-base-4.1.36-44.1
kernel-xen-4.1.36-44.1
kernel-vanilla-devel-4.1.36-44.1
kernel-ec2-base-4.1.36-44.1
kernel-xen-debugsource-4.1.36-44.1
kernel-debug-base-debuginfo-4.1.36-44.1
kernel-pv-base-debuginfo-4.1.36-44.1
kernel-xen-base-4.1.36-44.1
kernel-pv-debuginfo-4.1.36-44.1
kernel-pv-4.1.36-44.1
kernel-syms-4.1.36-44.1
kernel-default-debuginfo-4.1.36-44.1
kernel-debug-devel-4.1.36-44.1
kernel-default-debugsource-4.1.36-44.1
kernel-vanilla-4.1.36-44.1
kernel-ec2-base-debuginfo-4.1.36-44.1
kernel-pv-debugsource-4.1.36-44.1
kernel-obs-build-debugsource-4.1.36-44.3
kernel-debug-4.1.36-44.1
kernel-debug-base-4.1.36-44.1
kernel-debug-debuginfo-4.1.36-44.1
kernel-default-base-debuginfo-4.1.36-44.1
kernel-xen-base-debuginfo-4.1.36-44.1

145764 - SuSE SLES 11 SP4 SUSE-SU-2017:2312-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9586, CVE-2017-1000100, CVE-2017-7407

Description

The scan detected that the host is missing the following update:

SUSE-SU-2017:2312-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003173.html>

SuSE SLES 11 SP4

i586

libcurl4-7.19.7-1.70.3.1

curl-7.19.7-1.70.3.1

x86_64

curl-7.19.7-1.70.3.1

libcurl4-32bit-7.19.7-1.70.3.1

libcurl4-7.19.7-1.70.3.1

145779 - SuSE Linux 42.2 openSUSE-SU-2017:1221-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9603, CVE-2017-7718

Description

The scan detected that the host is missing the following update:

openSUSE-SU-2017:1221-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00032.html>

SuSE Linux 42.2

x86_64

xen-libs-32bit-4.7.2_04-11.6.1

xen-libs-debuginfo-32bit-4.7.2_04-11.6.1

xen-devel-4.7.2_04-11.6.1

xen-libs-4.7.2_04-11.6.1

xen-tools-domU-debuginfo-4.7.2_04-11.6.1

xen-debugsource-4.7.2_04-11.6.1

xen-tools-4.7.2_04-11.6.1

xen-tools-domU-4.7.2_04-11.6.1

xen-4.7.2_04-11.6.1

xen-tools-debuginfo-4.7.2_04-11.6.1

xen-doc-html-4.7.2_04-11.6.1

xen-libs-debuginfo-4.7.2_04-11.6.1

i586
xen-devel-4.7.2_04-11.6.1
xen-libs-4.7.2_04-11.6.1
xen-tools-domU-debuginfo-4.7.2_04-11.6.1
xen-debugsource-4.7.2_04-11.6.1
xen-tools-domU-4.7.2_04-11.6.1
xen-libs-debuginfo-4.7.2_04-11.6.1

145863 - SuSE Linux 42.2 openSUSE-SU-2017:0665-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9921, CVE-2016-9922, CVE-2017-2615, CVE-2017-2620

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0665-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00025.html>

SuSE Linux 42.2
x86_64
xen-tools-domU-debuginfo-4.7.1_06-9.2
xen-debugsource-4.7.1_06-9.2
xen-devel-4.7.1_06-9.2
xen-libs-32bit-4.7.1_06-9.2
xen-tools-debuginfo-4.7.1_06-9.2
xen-doc-html-4.7.1_06-9.2
xen-tools-domU-4.7.1_06-9.2
xen-tools-4.7.1_06-9.2
xen-libs-debuginfo-32bit-4.7.1_06-9.2
xen-4.7.1_06-9.2
xen-libs-4.7.1_06-9.2
xen-libs-debuginfo-4.7.1_06-9.2

i586
xen-tools-domU-debuginfo-4.7.1_06-9.2
xen-debugsource-4.7.1_06-9.2
xen-devel-4.7.1_06-9.2
xen-tools-domU-4.7.1_06-9.2
xen-libs-4.7.1_06-9.2
xen-libs-debuginfo-4.7.1_06-9.2

192597 - Fedora Linux 26 FEDORA-2017-f5177f3a16 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-1000369

Description

The scan detected that the host is missing the following update:

FEDORA-2017-f5177f3a16

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

exim-4.89-5.fc26

145735 - SuSE Linux 42.2 openSUSE-SU-2017:1211-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-0702, CVE-2016-7056

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1211-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00026.html>

SuSE Linux 42.2

i586

libressl-2.5.3-5.3.1

libressl-debugsource-2.5.3-5.3.1

libtls15-2.5.3-5.3.1

libssl43-2.5.3-5.3.1

libssl43-debuginfo-2.5.3-5.3.1

libcrypto41-debuginfo-2.5.3-5.3.1

libressl-debuginfo-2.5.3-5.3.1

libcrypto41-2.5.3-5.3.1

libressl-devel-2.5.3-5.3.1

libtls15-debuginfo-2.5.3-5.3.1

noarch

libressl-devel-doc-2.5.3-5.3.1

x86_64

libssl43-32bit-2.5.3-5.3.1

libressl-debuginfo-2.5.3-5.3.1

libtls15-debuginfo-32bit-2.5.3-5.3.1

libcrypto41-debuginfo-2.5.3-5.3.1

libressl-devel-32bit-2.5.3-5.3.1

libtls15-debuginfo-2.5.3-5.3.1

libcrypto41-2.5.3-5.3.1

libressl-2.5.3-5.3.1

libtls15-32bit-2.5.3-5.3.1

libressl-debugsource-2.5.3-5.3.1

libcrypto41-debuginfo-32bit-2.5.3-5.3.1

libssl43-2.5.3-5.3.1

libcrypto41-32bit-2.5.3-5.3.1
libressl-devel-2.5.3-5.3.1
libssl43-debuginfo-2.5.3-5.3.1
libtls15-2.5.3-5.3.1
libssl43-debuginfo-32bit-2.5.3-5.3.1

145744 - SuSE Linux 42.1 openSUSE-SU-2017:1212-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-0702, CVE-2016-7056

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:1212-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-05/msg00027.html>

SuSE Linux 42.1
i586
libressl-2.5.3-13.1
libcrypto41-debuginfo-2.5.3-13.1
libcrypto41-2.5.3-13.1
libressl-devel-2.5.3-13.1
libtls15-debuginfo-2.5.3-13.1
libtls15-2.5.3-13.1
libssl43-2.5.3-13.1
libressl-debuginfo-2.5.3-13.1
libressl-debugsource-2.5.3-13.1
libssl43-debuginfo-2.5.3-13.1

noarch
libressl-devel-doc-2.5.3-13.1

x86_64
libcrypto41-32bit-2.5.3-13.1
libressl-2.5.3-13.1
libtls15-debuginfo-2.5.3-13.1
libressl-devel-2.5.3-13.1
libressl-debugsource-2.5.3-13.1
libssl43-32bit-2.5.3-13.1
libtls15-debuginfo-32bit-2.5.3-13.1
libressl-devel-32bit-2.5.3-13.1
libssl43-2.5.3-13.1
libtls15-32bit-2.5.3-13.1
libssl43-debuginfo-32bit-2.5.3-13.1
libcrypto41-debuginfo-2.5.3-13.1
libtls15-2.5.3-13.1
libcrypto41-debuginfo-32bit-2.5.3-13.1
libssl43-debuginfo-2.5.3-13.1
libressl-debuginfo-2.5.3-13.1
libcrypto41-2.5.3-13.1

145898 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0621-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-6188

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:0621-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-03/msg00013.html>

SuSE Linux 42.1

noarch

munin-node-2.0.25-7.1

munin-2.0.25-7.1

SuSE Linux 42.2

noarch

munin-node-2.0.25-9.1

munin-2.0.25-9.1

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

130847 - Debian Linux 8.0, 9.0 DSA-3942-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-11610

Update Details

Risk is updated

130857 - Debian Linux 8.0, 9.0 DSA-3947-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-12904

Update Details

Risk is updated

182418 - FreeBSD Supervisord An Authenticated Client Can Run Arbitrary Shell Commands Via Malicious XML-RPC Requests (c9460380-81e3-11e7-

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-11610

[Update Details](#)

Risk is updated

192479 - Fedora Linux 24 FEDORA-2017-713430fb15 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-11610

[Update Details](#)

Risk is updated

192488 - Fedora Linux 26 FEDORA-2017-307eab89e1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Federa Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-11610

[Update Details](#)

Risk is updated

192498 - Fedora Linux 25 FEDORA-2017-85eb9f7a36 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-11610

[Update Details](#)

Risk is updated

130868 - Debian Linux 8.0, 9.0 DSA-3956-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-12865

[Update Details](#)

Risk is updated

145156 - SuSE Linux 13.2 openSUSE-SU-2017:0183-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-2120, CVE-2016-7068, CVE-2016-7072, CVE-2016-7073, CVE-2016-7074

[Update Details](#)

FASLScript is updated

145171 - SuSE Linux 13.2 openSUSE-SU-2017:0156-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-7459

[Update Details](#)

FASLScript is updated

170626 - Amazon Linux AMI ALAS-2016-646 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-7700

[Update Details](#)

Risk is updated

170849 - Amazon Linux AMI ALAS-2017-874 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-10970, CVE-2017-12065, CVE-2017-12066

[Update Details](#)

CVE is updated

181333 - FreeBSD Xymon Buffer Overrun (1c7cfd05-aeee-11e4-83b4-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-1430

[Update Details](#)

Risk is updated

130819 - Debian Linux 8.0 DSA-3911-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

130824 - Debian Linux 8.0, 9.0 DSA-3916-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

130867 - Debian Linux 9.0 DSA-3953-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-12440

[Update Details](#)

Risk is updated

141642 - Red Hat Enterprise Linux RHSA-2017-2388 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

145453 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:1893-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

163429 - Oracle Enterprise Linux ELSA-2017-2388 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

170848 - Amazon Linux AMI ALAS-2017-873 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5648, CVE-2017-5664, CVE-2017-7674

[Update Details](#)

CVE is updated

175224 - Scientific Linux Security ERRATA Important: evince on SL7.x x86_64 (1708-7506)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

182425 - FreeBSD evince and atril Command Injection Vulnerability In CBT Handler (01a197ca-67f1-11e7-a266-28924a333806)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

185776 - Ubuntu Linux 14.04, 16.04, 16.10, 17.04 USN-3351-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

192367 - Fedora Linux 26 FEDORA-2017-0f75ee2f38 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

192374 - Fedora Linux 25 FEDORA-2017-cdead07e99 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

192495 - Fedora Linux 24 FEDORA-2017-06c1422db8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000083

[Update Details](#)

Risk is updated

130862 - Debian Linux 9.0 DSA-3959-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-0379

Update Details

Risk is updated

145148 - SuSE Linux 13.2 openSUSE-SU-2017:0093-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5193, CVE-2017-5194, CVE-2017-5195, CVE-2017-5196

Update Details

FASLScript is updated

145165 - SuSE Linux 13.2 openSUSE-SU-2017:0158-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3462

Update Details

FASLScript is updated

145173 - SuSE Linux 13.2 openSUSE-SU-2017:0178-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10109

Update Details

FASLScript is updated

182422 - FreeBSD pspp Multiple Vulnerabilities (6876b163-8708-11e7-8568-e8e0b747a45a)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-10791, CVE-2017-10792, CVE-2017-12958, CVE-2017-12959, CVE-2017-12960, CVE-2017-12961

Update Details

FASLScript is updated

188968 - Fedora Linux 21 FEDORA-2015-2828 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-0928

[Update Details](#)

Risk is updated

188976 - Fedora Linux 22 FEDORA-2015-2790 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-0928

[Update Details](#)

Risk is updated

189387 - Fedora Linux 21 FEDORA-2015-7886 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-0928

[Update Details](#)

Risk is updated

191503 - Fedora Linux 25 FEDORA-2016-ca1d1e1dc1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-7030, CVE-2016-9575

[Update Details](#)

Risk is updated

191557 - Fedora Linux 24 FEDORA-2016-d337166907 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-7030, CVE-2016-9575

[Update Details](#)

Risk is updated

145144 - SuSE Linux 13.2 openSUSE-SU-2017:0034-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

70042 - aix.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational
CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70087 - hp.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2017 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates