

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

24917 - Mozilla Firefox Multiple Vulnerabilities Prior To 66

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

Risk Level: High

CVE: CVE-2019-9788, CVE-2019-9789, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9797, CVE-2019-9798, CVE-2019-9799, CVE-2019-9801, CVE-2019-9802, CVE-2019-9803, CVE-2019-9804, CVE-2019-9805, CVE-2019-9806, CVE-2019-9807, CVE-2019-9808, CVE-2019-9809

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system and cause a denial of service condition.

24928 - (APSB19-15) Vulnerability In Adobe Photoshop CC

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

Risk Level: High

CVE: CVE-2019-7094

Description

A vulnerability is present in some versions of Adobe Photoshop CC.

Observation

Adobe Photoshop CC is a product for media editing and management.

A vulnerability is present in some versions of Adobe Photoshop CC. The flaw is due to heap corruption. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

24968 - Cisco NX-OS Software NX-API Command Injection Vulnerability (CVE-2019-1614)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1614

Description

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

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in NX-API of Cisco NX-OS Software. Successful exploitation could allow an attacker to execute arbitrary commands with the security context of the root user.

147759 - SuSE Linux 15.0 openSUSE-SU-2019:1109-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1109-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00020.html>

SuSE Linux 15.0

x86_64

libssh2-1-debuginfo-1.8.0-lp150.3.3.1

libssh2-devel-1.8.0-lp150.3.3.1

libssh2_org-debugsource-1.8.0-lp150.3.3.1

libssh2-1-32bit-1.8.0-lp150.3.3.1

libssh2-1-32bit-debuginfo-1.8.0-lp150.3.3.1

libssh2-1-1.8.0-lp150.3.3.1

i586

libssh2-1-debuginfo-1.8.0-lp150.3.3.1

libssh2-1-1.8.0-lp150.3.3.1

libssh2-devel-1.8.0-lp150.3.3.1

libssh2_org-debugsource-1.8.0-lp150.3.3.1

147768 - SuSE Linux 42.3 openSUSE-SU-2019:1079-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16873, CVE-2018-16874, CVE-2018-16875, CVE-2019-5736

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1079-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00117.html>

SuSE Linux 42.3

i586

docker-libnetwork-debuginfo-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-libnetwork-kubic-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
containerd-1.2.2-22.1
docker-runc-1.0.0rc6+gitr3748_96ec2177ae84-11.1
golang-github-docker-libnetwork-debugsource-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
containerd-kubic-ctr-1.2.2-22.1
docker-runc-kubic-1.0.0rc6+gitr3748_96ec2177ae84-11.1
docker-libnetwork-kubic-debuginfo-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-runc-kubic-debugsource-1.0.0rc6+gitr3748_96ec2177ae84-11.1
containerd-kubic-1.2.2-22.1
golang-github-docker-libnetwork-kubic-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
containerd-ctr-1.2.2-22.1
golang-github-docker-libnetwork-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-runc-debuginfo-1.0.0rc6+gitr3748_96ec2177ae84-11.1
docker-libnetwork-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-runc-kubic-debuginfo-1.0.0rc6+gitr3748_96ec2177ae84-11.1
golang-github-docker-libnetwork-kubic-debugsource-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-runc-debugsource-1.0.0rc6+gitr3748_96ec2177ae84-11.1

noarch

docker-zsh-completion-18.09.1_ce-54.1
docker-runc-kubic-test-1.0.0rc6+gitr3748_96ec2177ae84-11.1
docker-runc-test-1.0.0rc6+gitr3748_96ec2177ae84-11.1
docker-bash-completion-18.09.1_ce-54.1
docker-kubic-zsh-completion-18.09.1_ce-54.1
docker-kubic-bash-completion-18.09.1_ce-54.1
containerd-kubic-test-1.2.2-22.1
containerd-test-1.2.2-22.1

x86_64

docker-libnetwork-debuginfo-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-kubic-18.09.1_ce-54.1
docker-kubic-debuginfo-18.09.1_ce-54.1
docker-kubic-kubeadm-criconfig-18.09.1_ce-54.1
docker-kubic-test-debuginfo-18.09.1_ce-54.1
golang-github-docker-libnetwork-debugsource-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-kubic-debugsource-18.09.1_ce-54.1
docker-test-debuginfo-18.09.1_ce-54.1
containerd-1.2.2-22.1
docker-kubic-test-18.09.1_ce-54.1
docker-runc-kubic-debugsource-1.0.0rc6+gitr3748_96ec2177ae84-11.1
containerd-kubic-1.2.2-22.1
docker-libnetwork-kubic-debuginfo-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-debugsource-18.09.1_ce-54.1
docker-libnetwork-kubic-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-test-18.09.1_ce-54.1
docker-libnetwork-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-runc-debuginfo-1.0.0rc6+gitr3748_96ec2177ae84-11.1
docker-runc-kubic-debuginfo-1.0.0rc6+gitr3748_96ec2177ae84-11.1
docker-runc-1.0.0rc6+gitr3748_96ec2177ae84-11.1
golang-github-docker-libnetwork-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
docker-runc-debugsource-1.0.0rc6+gitr3748_96ec2177ae84-11.1
docker-18.09.1_ce-54.1
docker-runc-kubic-1.0.0rc6+gitr3748_96ec2177ae84-11.1
docker-debuginfo-18.09.1_ce-54.1
golang-github-docker-libnetwork-kubic-0.7.0.1+gitr2711_2cfbf9b1f981-11.1
containerd-ctr-1.2.2-22.1
containerd-kubic-ctr-1.2.2-22.1
golang-github-docker-libnetwork-kubic-debugsource-0.7.0.1+gitr2711_2cfbf9b1f981-11.1

147778 - SuSE Linux 42.3 openSUSE-SU-2019:1075-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1075-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00111.html>

SuSE Linux 42.3

x86_64

libssh2_org-debugsource-1.4.3-19.3.1

libssh2-1-32bit-1.4.3-19.3.1

libssh2-1-debuginfo-1.4.3-19.3.1

libssh2-devel-1.4.3-19.3.1

libssh2-1-debuginfo-32bit-1.4.3-19.3.1

libssh2-1-1.4.3-19.3.1

i586

libssh2-devel-1.4.3-19.3.1

libssh2-1-debuginfo-1.4.3-19.3.1

libssh2-1-1.4.3-19.3.1

libssh2_org-debugsource-1.4.3-19.3.1

160539 - CentOS 7 CESA-2019-0671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
CESA-2019-0671

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2019-April/023257.html>

CentOS 7

x86_64

firefox-60.6.1-1.el7.centos

i686

firefox-60.6.1-1.el7.centos

160540 - CentOS 6 CESA-2019-0672 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
CESA-2019-0672

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2019-April/023255.html>

CentOS 6
x86_64
firefox-60.6.1-1.el6.centos

i686
firefox-60.6.1-1.el6.centos

160542 - CentOS 7 CESA-2019-0679 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
CESA-2019-0679

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2019-April/023259.html>

CentOS 7
i686
libssh2-1.4.3-12.el7_6.2
libssh2-devel-1.4.3-12.el7_6.2

noarch
libssh2-docs-1.4.3-12.el7_6.2

x86_64
libssh2-1.4.3-12.el7_6.2
libssh2-devel-1.4.3-12.el7_6.2

163832 - Oracle Enterprise Linux ELSA-2019-0672 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
ELSA-2019-0672

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-March/008606.html>

OEL6
x86_64
firefox-60.6.1-1.0.1.el6_10

163833 - Oracle Enterprise Linux ELSA-2019-0671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
ELSA-2019-0671

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-March/008605.html>

OEL7
x86_64
firefox-60.6.1-1.0.1.el7_6

163834 - Oracle Enterprise Linux ELSA-2019-0679 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
ELSA-2019-0679

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-March/008613.html>
<http://oss.oracle.com/pipermail/el-errata/2019-March/008608.html>

OEL7
x86_64

libssh2-docs-1.4.3-12.el7_6.2
libssh2-1.4.3-12.el7_6.2
libssh2-devel-1.4.3-12.el7_6.2

196279 - Red Hat Enterprise Linux RHSA-2019-0672 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
RHSA-2019-0672

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-March/msg00041.html>

RHEL6D
x86_64
firefox-debuginfo-60.6.1-1.el6_10
firefox-60.6.1-1.el6_10

i386
firefox-debuginfo-60.6.1-1.el6_10
firefox-60.6.1-1.el6_10

RHEL6S
i386
firefox-debuginfo-60.6.1-1.el6_10
firefox-60.6.1-1.el6_10

x86_64
firefox-debuginfo-60.6.1-1.el6_10
firefox-60.6.1-1.el6_10

RHEL6WS
x86_64
firefox-debuginfo-60.6.1-1.el6_10
firefox-60.6.1-1.el6_10

i386
firefox-debuginfo-60.6.1-1.el6_10
firefox-60.6.1-1.el6_10

196281 - Red Hat Enterprise Linux RHSA-2019-0671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
RHSA-2019-0671

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-March/msg00040.html>

RHEL7D

x86_64
firefox-60.6.1-1.el7_6
firefox-debuginfo-60.6.1-1.el7_6

RHEL7S

x86_64
firefox-60.6.1-1.el7_6
firefox-debuginfo-60.6.1-1.el7_6

RHEL7WS

x86_64
firefox-60.6.1-1.el7_6
firefox-debuginfo-60.6.1-1.el7_6

196282 - Red Hat Enterprise Linux RHSA-2019-0679 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
RHSA-2019-0679

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-March/msg00044.html>

RHEL7D

x86_64
libssh2-1.4.3-12.el7_6.2
libssh2-devel-1.4.3-12.el7_6.2
libssh2-debuginfo-1.4.3-12.el7_6.2

noarch

libssh2-docs-1.4.3-12.el7_6.2

RHEL7S

noarch
libssh2-docs-1.4.3-12.el7_6.2

x86_64

libssh2-1.4.3-12.el7_6.2
libssh2-devel-1.4.3-12.el7_6.2
libssh2-debuginfo-1.4.3-12.el7_6.2

RHEL7WS

x86_64

libssh2-1.4.3-12.el7_6.2
libssh2-devel-1.4.3-12.el7_6.2
libssh2-debuginfo-1.4.3-12.el7_6.2

noarch
libssh2-docs-1.4.3-12.el7_6.2

24919 - Google Chrome Multiple Vulnerabilities Prior To 73.0.3683.75

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

Risk Level: High

CVE: CVE-2019-5787, CVE-2019-5788, CVE-2019-5789, CVE-2019-5790, CVE-2019-5791, CVE-2019-5792, CVE-2019-5793, CVE-2019-5794, CVE-2019-5795, CVE-2019-5796, CVE-2019-5797, CVE-2019-5798, CVE-2019-5799, CVE-2019-5800, CVE-2019-5801, CVE-2019-5802, CVE-2019-5803, CVE-2019-5804

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute remote code on the targeted system.

24903 - IBM DB2 Multiple Vulnerabilities (ibm10740413)

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

Risk Level: High

CVE: CVE-2018-1922, CVE-2018-1923, CVE-2018-1978, CVE-2018-1980, CVE-2019-4015, CVE-2019-4016

Description

Multiple vulnerabilities are present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

Multiple vulnerabilities are present in some versions of IBM DB2. The flaws lie in multiple components. Successful exploitation could allow a local attacker to execute arbitrary code on the target system.

24904 - IBM DB2 Multiple Vulnerabilities (ibm10740413)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-1922, CVE-2018-1923, CVE-2018-1978, CVE-2018-1980, CVE-2019-4015, CVE-2019-4016

Description

Multiple vulnerabilities are present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

Multiple vulnerabilities are present in some versions of IBM DB2. The flaws lie in multiple components. Successful exploitation could allow a local attacker to execute arbitrary code on the target system.

24906 - Cisco NX-OS Software Privilege Escalation Vulnerability (CVE-2019-1602)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1602

Description

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

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in file system permissions of Cisco NX-OS software. Successful exploitation could allow a local attacker to access sensitive data, which could lead to privilege escalation.

24920 - (K54167061) F5 BIG-IP TMM SSL Profile Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2019-6592

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's BIG-IP products. The flaw lies in Traffic Management Microkernel. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

24923 - Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1609)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1609

Description

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

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to insufficient validation of CLI commands arguments. Successful exploitation could allow an authenticated attacker to execute arbitrary commands on the target.

24929 - Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1607)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1607

Description

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

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in CLI of Cisco NX-OS Software. Successful exploitation could allow a local attacker to execute arbitrary code in the system with elevated privileges.

131323 - Debian Linux 9.0 DSA-4418-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-7524

Description

The scan detected that the host is missing the following update:
DSA-4418-1

Observation

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

<http://www.debian.org/security/2019/dsa-4418>

Debian 9.0

all

dovecot-lmtpd_1:2.2.27-3+deb9u4

dovecot-pgsq1_1:2.2.27-3+deb9u4

dovecot-dev_1:2.2.27-3+deb9u4

dovecot-dbg_1:2.2.27-3+deb9u4

dovecot-managesieved_1:2.2.27-3+deb9u4

dovecot-solr_1:2.2.27-3+deb9u4

dovecot-core_1:2.2.27-3+deb9u4

dovecot-lucene_1:2.2.27-3+deb9u4

dovecot-sieve_1:2.2.27-3+deb9u4

dovecot-sqlite_1:2.2.27-3+deb9u4

dovecot-mysql_1:2.2.27-3+deb9u4

dovecot-imapd_1:2.2.27-3+deb9u4

dovecot-pop3d_1:2.2.27-3+deb9u4

dovecot-ldap_1:2.2.27-3+deb9u4

dovecot-gssapi_1:2.2.27-3+deb9u4

147738 - SuSE Linux 15.0 openSUSE-SU-2019:1089-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20105

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1089-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00009.html>

SuSE Linux 15.0
noarch
yast2-rmt-1.2.2-lp150.2.19.1

147741 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0789-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8936

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0789-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005258.html>

SuSE SLED 12 SP3
x86_64
ntp-doc-4.2.8p13-85.1
ntp-debuginfo-4.2.8p13-85.1
ntp-4.2.8p13-85.1
ntp-debugsource-4.2.8p13-85.1

SuSE SLED 12 SP4
x86_64
ntp-doc-4.2.8p13-85.1
ntp-debuginfo-4.2.8p13-85.1
ntp-4.2.8p13-85.1
ntp-debugsource-4.2.8p13-85.1

SuSE SLES 12 SP4
x86_64
ntp-doc-4.2.8p13-85.1
ntp-debuginfo-4.2.8p13-85.1
ntp-4.2.8p13-85.1
ntp-debugsource-4.2.8p13-85.1

SuSE SLES 12 SP3
x86_64
ntp-doc-4.2.8p13-85.1
ntp-debuginfo-4.2.8p13-85.1
ntp-4.2.8p13-85.1
ntp-debugsource-4.2.8p13-85.1

147743 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0766-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12181, CVE-2019-0160

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0766-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005247.html>

SuSE SLED 12 SP4

noarch

qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-3.13.1

SuSE SLES 12 SP4

noarch

qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-3.13.1

qemu-uefi-aarch64-2017+git1510945757.b2662641d5-3.13.1

x86_64

ovmf-tools-2017+git1510945757.b2662641d5-3.13.1

ovmf-2017+git1510945757.b2662641d5-3.13.1

147752 - SuSE SLES 12 SP4 SUSE-SU-2019:0767-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20669, CVE-2019-2024, CVE-2019-3459, CVE-2019-3460, CVE-2019-3819, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0767-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005245.html>

SuSE SLES 12 SP4

x86_64

kernel-azure-debugsource-4.12.14-6.9.1

kernel-syms-azure-4.12.14-6.9.1

kernel-azure-base-debuginfo-4.12.14-6.9.1

kernel-azure-devel-4.12.14-6.9.1

kernel-azure-4.12.14-6.9.1

kernel-azure-base-4.12.14-6.9.1

kernel-azure-debuginfo-4.12.14-6.9.1

noarch

kernel-devel-azure-4.12.14-6.9.1

kernel-source-azure-4.12.14-6.9.1

147755 - SuSE Linux 15.0 openSUSE-SU-2019:1106-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-0804

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1106-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00018.html>

SuSE Linux 15.0

noarch

python-azure-agent-2.2.36-lp150.5.10.1

python-azure-agent-test-2.2.36-lp150.5.10.1

147757 - SuSE Linux 42.3 openSUSE-SU-2019:1059-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10916

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1059-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00097.html>

SuSE Linux 42.3

x86_64

lftp-debuginfo-4.7.4-2.6.1

lftp-4.7.4-2.6.1

lftp-debugsource-4.7.4-2.6.1

i586

lftp-debuginfo-4.7.4-2.6.1

lftp-4.7.4-2.6.1

lftp-debugsource-4.7.4-2.6.1

147758 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0838-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9924

Description

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

SUSE-SU-2019:0838-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-April/005282.html>

SuSE SLES 12 SP3

noarch

readline-doc-6.3-83.23.1

bash-doc-4.3-83.23.1

x86_64

bash-debugsource-4.3-83.23.1

bash-4.3-83.23.1

libreadline6-32bit-6.3-83.23.1

libreadline6-6.3-83.23.1

libreadline6-debuginfo-6.3-83.23.1

libreadline6-debuginfo-32bit-6.3-83.23.1

bash-debuginfo-4.3-83.23.1

SuSE SLES 12 SP4

noarch

readline-doc-6.3-83.23.1

bash-doc-4.3-83.23.1

x86_64

bash-debugsource-4.3-83.23.1

bash-4.3-83.23.1

libreadline6-32bit-6.3-83.23.1

libreadline6-6.3-83.23.1

libreadline6-debuginfo-6.3-83.23.1

libreadline6-debuginfo-32bit-6.3-83.23.1

bash-debuginfo-4.3-83.23.1

SuSE SLED 12 SP4

x86_64

bash-debugsource-4.3-83.23.1

bash-4.3-83.23.1

libreadline6-32bit-6.3-83.23.1

libreadline6-6.3-83.23.1

libreadline6-debuginfo-6.3-83.23.1

libreadline6-debuginfo-32bit-6.3-83.23.1

bash-debuginfo-4.3-83.23.1

noarch

bash-lang-4.3-83.23.1

readline-doc-6.3-83.23.1

bash-doc-4.3-83.23.1

SuSE SLED 12 SP3

x86_64

bash-debugsource-4.3-83.23.1

bash-4.3-83.23.1

libreadline6-32bit-6.3-83.23.1

libreadline6-6.3-83.23.1

libreadline6-debuginfo-6.3-83.23.1
libreadline6-debuginfo-32bit-6.3-83.23.1
bash-debuginfo-4.3-83.23.1

noarch
bash-lang-4.3-83.23.1
readline-doc-6.3-83.23.1
bash-doc-4.3-83.23.1

147767 - SuSE SLES 11 SP4 SUSE-SU-2019:13991-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8936

Description

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

SUSE-SU-2019:13991-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005255.html>

SuSE SLES 11 SP4
i586
ntp-4.2.8p13-64.13.1
ntp-doc-4.2.8p13-64.13.1

x86_64
ntp-4.2.8p13-64.13.1
ntp-doc-4.2.8p13-64.13.1

147777 - SuSE Linux 15.0 openSUSE-SU-2019:1110-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10916

Description

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

openSUSE-SU-2019:1110-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00028.html>

SuSE Linux 15.0
x86_64
lftp-debuginfo-4.8.3-lp150.3.3.1
lftp-4.8.3-lp150.3.3.1
lftp-debugsource-4.8.3-lp150.3.3.1

147779 - SuSE Linux 15.0 openSUSE-SU-2019:1113-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9894, CVE-2019-9895, CVE-2019-9896, CVE-2019-9897, CVE-2019-9898

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1113-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00021.html>

SuSE Linux 15.0

x86_64

putty-debugsource-0.71-lp150.9.1

putty-0.71-lp150.9.1

putty-debuginfo-0.71-lp150.9.1

147786 - SuSE Linux 15.0 openSUSE-SU-2019:1084-1 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-2019:1084-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00122.html>

SuSE Linux 15.0

x86_64

ucode-intel-20190312-lp150.2.14.1

147792 - SuSE Linux 15.0 openSUSE-SU-2019:1062-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5787, CVE-2019-5788, CVE-2019-5789, CVE-2019-5790, CVE-2019-5791, CVE-2019-5792, CVE-2019-5793, CVE-2019-5794, CVE-2019-5795, CVE-2019-5796, CVE-2019-5797, CVE-2019-5798, CVE-2019-5799, CVE-2019-5800, CVE-2019-5801, CVE-2019-5802, CVE-2019-5803, CVE-2019-5804

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1062-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00108.html>

SuSE Linux 15.0

x86_64

chromium-73.0.3683.75-lp150.206.1

chromium-debugsource-73.0.3683.75-lp150.206.1

chromedriver-debuginfo-73.0.3683.75-lp150.206.1

chromium-debuginfo-73.0.3683.75-lp150.206.1

chromedriver-73.0.3683.75-lp150.206.1

163835 - Oracle Enterprise Linux ELSA-2019-4596 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1066, CVE-2018-10881, CVE-2018-10882, CVE-2019-3701

Description

The scan detected that the host is missing the following update:
ELSA-2019-4596

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-April/008617.html>

<http://oss.oracle.com/pipermail/el-errata/2019-April/008616.html>

OEL7

x86_64

kernel-uek-doc-4.1.12-124.26.7.el7uek

kernel-uek-debug-4.1.12-124.26.7.el7uek

kernel-uek-devel-4.1.12-124.26.7.el7uek

kernel-uek-4.1.12-124.26.7.el7uek

kernel-uek-debug-devel-4.1.12-124.26.7.el7uek

kernel-uek-firmware-4.1.12-124.26.7.el7uek

OEL6

x86_64

kernel-uek-4.1.12-124.26.7.el6uek

kernel-uek-doc-4.1.12-124.26.7.el6uek

kernel-uek-firmware-4.1.12-124.26.7.el6uek

kernel-uek-debug-devel-4.1.12-124.26.7.el6uek

kernel-uek-debug-4.1.12-124.26.7.el6uek

kernel-uek-devel-4.1.12-124.26.7.el6uek

163838 - Oracle Enterprise Linux ELSA-2019-0697 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-8786, CVE-2018-8787, CVE-2018-8788

Description

The scan detected that the host is missing the following update:
ELSA-2019-0697

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-April/008620.html>

OEL7
x86_64
freerdp-devel-1.0.2-15.el7_6.1
freerdp-libs-1.0.2-15.el7_6.1
freerdp-plugins-1.0.2-15.el7_6.1
freerdp-1.0.2-15.el7_6.1

178721 - Gentoo Linux GLSA-201903-19 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-19

Observation

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

<https://security.gentoo.org/glsa/201903-19>

Affected packages:
dev-lang/nasm < 2.14.02

178724 - Gentoo Linux GLSA-201903-22 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-22

Observation

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

<https://security.gentoo.org/glsa/201903-22>

Affected packages:
net-libs/zeromq < 4.3.1

178728 - Gentoo Linux GLSA-201903-23 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-23

Observation

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

<https://security.gentoo.org/glsa/201903-23>

Affected packages:

www-client/chromium < 73.0.3683.75

182944 - FreeBSD dovecot Buffer Overflow Reading Extension Header (7862213c-5152-11e9-8b26-a4badb296695)

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

Risk Level: High

CVE: CVE-2019-7524

Description

The scan detected that the host is missing the following update:
dovecot -- Buffer overflow reading extension header (7862213c-5152-11e9-8b26-a4badb296695)

Observation

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

<http://www.vuxml.org/freebsd/7862213c-5152-11e9-8b26-a4badb296695.html>

Affected packages:

dovecot < 2.3.5.1

186623 - Ubuntu Linux 18.04 USN-3930-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8956, CVE-2019-8980, CVE-2019-9003, CVE-2019-9162, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
USN-3930-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004827.html>

Ubuntu 18.04

linux-image-4.18.0-17-lowlatency_4.18.0-17.18~18.04.1
linux-image-azure_4.18.0.1014.13
linux-image-snapdragon-hwe-18.04_4.18.0.17.67
linux-image-4.18.0-1014-azure_4.18.0-1014.14~18.04.1
linux-image-4.18.0-17-snapdragon_4.18.0-17.18~18.04.1
linux-image-lowlatency-hwe-18.04_4.18.0.17.67
linux-image-virtual-hwe-18.04_4.18.0.17.67
linux-image-generic-hwe-18.04_4.18.0.17.67
linux-image-4.18.0-17-generic-lpae_4.18.0-17.18~18.04.1
linux-image-generic-lpae-hwe-18.04_4.18.0.17.67
linux-image-4.18.0-17-generic_4.18.0-17.18~18.04.1

186626 - Ubuntu Linux 14.04, 16.04 USN-3931-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14678, CVE-2018-18021, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
USN-3931-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004829.html>

Ubuntu 14.04

linux-image-azure_4.15.0.1041.28
linux-image-4.15.0-1041-azure_4.15.0-1041.45~14.04.1

Ubuntu 16.04

linux-image-virtual-hwe-16.04_4.15.0.47.68
linux-image-oracle_4.15.0.1010.4
linux-image-4.15.0-47-generic-lpae_4.15.0-47.50~16.04.1
linux-image-4.15.0-47-generic_4.15.0-47.50~16.04.1
linux-image-4.15.0-1035-aws_4.15.0-1035.37~16.04.1
linux-image-4.15.0-1029-gcp_4.15.0-1029.31~16.04.1
linux-image-4.15.0-47-lowlatency_4.15.0-47.50~16.04.1
linux-image-oem_4.15.0.47.68
linux-image-generic-hwe-16.04_4.15.0.47.68
linux-image-4.15.0-1041-azure_4.15.0-1041.45
linux-image-lowlatency-hwe-16.04_4.15.0.47.68
linux-image-gke_4.15.0.1029.43
linux-image-generic-lpae-hwe-16.04_4.15.0.47.68
linux-image-azure_4.15.0.1041.45
linux-image-4.15.0-1010-oracle_4.15.0-1010.12~16.04.1
linux-image-gcp_4.15.0.1029.43
linux-image-aws-hwe_4.15.0.1035.35

186628 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3928-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-7524

Description

The scan detected that the host is missing the following update:
USN-3928-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004824.html>

Ubuntu 16.04

dovecot-core_2.2.22-1ubuntu2.10

Ubuntu 18.10

dovecot-core_2.3.2.1-1ubuntu3.2

Ubuntu 14.04

dovecot-core_2.2.9-1ubuntu2.6

Ubuntu 18.04

dovecot-core_2.2.33.2-1ubuntu4.3

186629 - Ubuntu Linux 16.04 USN-3932-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18249, CVE-2018-13097, CVE-2018-13099, CVE-2018-13100, CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613, CVE-2018-14614, CVE-2018-14616, CVE-2018-16884, CVE-2018-9517, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-3819, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
USN-3932-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004830.html>

Ubuntu 16.04

linux-image-4.4.0-1079-aws_4.4.0-1079.89

linux-image-snapdragon_4.4.0.1110.102

linux-image-lowlatency_4.4.0.145.153

linux-image-4.4.0-145-powerpc-smp_4.4.0-145.171

linux-image-4.4.0-145-powerpc64-smp_4.4.0-145.171

linux-image-4.4.0-145-powerpc-e500mc_4.4.0-145.171

linux-image-powerpc-e500mc_4.4.0.145.153
linux-image-powerpc-smp_4.4.0.145.153
linux-image-4.4.0-145-powerpc64-emb_4.4.0-145.171
linux-image-kvm_4.4.0.1043.43
linux-image-raspi2_4.4.0.1106.106
linux-image-powerpc64-emb_4.4.0.145.153
linux-image-generic-lpae_4.4.0.145.153
linux-image-4.4.0-1043-kvm_4.4.0-1043.49
linux-image-4.4.0-1110-snapdragon_4.4.0-1110.115
linux-image-generic_4.4.0.145.153
linux-image-virtual_4.4.0.145.153
linux-image-powerpc64-smp_4.4.0.145.153
linux-image-4.4.0-145-generic_4.4.0-145.171
linux-image-4.4.0-145-lowlatency_4.4.0-145.171
linux-image-aws_4.4.0.1079.82
linux-image-4.4.0-1106-raspi2_4.4.0-1106.114
linux-image-4.4.0-145-generic-lpae_4.4.0-145.171

186630 - Ubuntu Linux 18.10 USN-3930-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8956, CVE-2019-8980, CVE-2019-9003, CVE-2019-9162, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
USN-3930-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004826.html>

Ubuntu 18.10

linux-image-gke_4.18.0.1008.8
linux-image-virtual_4.18.0.17.18
linux-image-4.18.0-17-snapdragon_4.18.0-17.18
linux-image-kvm_4.18.0.1009.9
linux-image-4.18.0-17-generic_4.18.0-17.18
linux-image-raspi2_4.18.0.1011.8
linux-image-4.18.0-1014-azure_4.18.0-1014.14
linux-image-aws_4.18.0.1012.12
linux-image-generic-lpae_4.18.0.17.18
linux-image-snapdragon_4.18.0.17.18
linux-image-4.18.0-1011-raspi2_4.18.0-1011.13
linux-image-azure_4.18.0.1014.15
linux-image-4.18.0-1012-aws_4.18.0-1012.14
linux-image-lowlatency_4.18.0.17.18
linux-image-4.18.0-17-lowlatency_4.18.0-17.18
linux-image-gcp_4.18.0.1008.8
linux-image-generic_4.18.0.17.18
linux-image-4.18.0-1008-gcp_4.18.0-1008.9
linux-image-4.18.0-17-generic-lpae_4.18.0-17.18
linux-image-4.18.0-1009-kvm_4.18.0-1009.9

186632 - Ubuntu Linux 18.04 USN-3931-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14678, CVE-2018-18021, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
USN-3931-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004828.html>

Ubuntu 18.04

linux-image-4.15.0-1029-gcp_4.15.0-1029.31
linux-image-4.15.0-1031-kvm_4.15.0-1031.31
linux-image-4.15.0-47-generic-lpae_4.15.0-47.50
linux-image-gke_4.15.0.1029.31
linux-image-4.15.0-1010-oracle_4.15.0-1010.12
linux-image-4.15.0-1033-raspi2_4.15.0-1033.35
linux-image-kvm_4.15.0.1031.31
linux-image-generic-lpae_4.15.0.47.49
linux-image-snapdragon_4.15.0.47.49
linux-image-4.15.0-47-lowlatency_4.15.0-47.50
linux-image-4.15.0-47-snapdragon_4.15.0-47.50
linux-image-aws_4.15.0.1035.34
linux-image-oem_4.15.0.1035.40
linux-image-4.15.0-1035-oem_4.15.0-1035.40
linux-image-generic_4.15.0.47.49
linux-image-oracle_4.15.0.1010.13
linux-image-gcp_4.15.0.1029.31
linux-image-4.15.0-1035-aws_4.15.0-1035.37
linux-image-virtual_4.15.0.47.49
linux-image-4.15.0-47-generic_4.15.0-47.50
linux-image-lowlatency_4.15.0.47.49
linux-image-raspi2_4.15.0.1033.31

186635 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3926-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000100, CVE-2018-13005, CVE-2018-13006, CVE-2018-20760, CVE-2018-20761, CVE-2018-20762, CVE-2018-20763, CVE-2018-7752

Description

The scan detected that the host is missing the following update:
USN-3926-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004823.html>

Ubuntu 16.04

libgpac4_0.5.2-426-gc5ad4e4+dfsg5-1ubuntu0.1
gpac_0.5.2-426-gc5ad4e4+dfsg5-1ubuntu0.1
gpac-modules-base_0.5.2-426-gc5ad4e4+dfsg5-1ubuntu0.1

Ubuntu 18.10

libgpac4_0.5.2-426-gc5ad4e4+dfsg5-4ubuntu0.1
gpac-modules-base_0.5.2-426-gc5ad4e4+dfsg5-4ubuntu0.1
gpac_0.5.2-426-gc5ad4e4+dfsg5-4ubuntu0.1

Ubuntu 18.04

gpac-modules-base_0.5.2-426-gc5ad4e4+dfsg5-3ubuntu0.1
libgpac4_0.5.2-426-gc5ad4e4+dfsg5-3ubuntu0.1
gpac_0.5.2-426-gc5ad4e4+dfsg5-3ubuntu0.1

186636 - Ubuntu Linux 14.04 USN-3932-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18249, CVE-2018-13097, CVE-2018-13099, CVE-2018-13100, CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613, CVE-2018-14614, CVE-2018-14616, CVE-2018-16884, CVE-2018-9517, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-3819, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
USN-3932-2

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004831.html>

Ubuntu 14.04

linux-image-4.4.0-144-powerpc64-emb_4.4.0-144.170~14.04.1
linux-image-virtual-lts-xenial_4.4.0.144.127
linux-image-powerpc64-smp-lts-xenial_4.4.0.144.127
linux-image-4.4.0-144-generic-lpae_4.4.0-144.170~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.144.127
linux-image-generic-lts-xenial_4.4.0.144.127
linux-image-4.4.0-144-generic_4.4.0-144.170~14.04.1
linux-image-4.4.0-1040-aws_4.4.0-1040.43
linux-image-lowlatency-lts-xenial_4.4.0.144.127
linux-image-4.4.0-144-powerpc-smp_4.4.0-144.170~14.04.1
linux-image-4.4.0-144-powerpc64-smp_4.4.0-144.170~14.04.1
linux-image-powerpc-smp-lts-xenial_4.4.0.144.127
linux-image-generic-lpae-lts-xenial_4.4.0.144.127
linux-image-aws_4.4.0.1040.41
linux-image-powerpc64-emb-lts-xenial_4.4.0.144.127
linux-image-4.4.0-144-lowlatency_4.4.0-144.170~14.04.1
linux-image-4.4.0-144-powerpc-e500mc_4.4.0-144.170~14.04.1

194925 - Fedora Linux 30 FEDORA-2019-7d689dd314 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18407, CVE-2018-18408, CVE-2019-8376, CVE-2019-8377, CVE-2019-8381

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7d689dd314

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/2019/3/?count=200&page=4>

Fedora Core 30

tcpreplay-4.3.2-1.fc30

194930 - Fedora Linux 30 FEDORA-2019-44643e8bcb Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18342

Description

The scan detected that the host is missing the following update:
FEDORA-2019-44643e8bcb

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/2019/3/?count=200&page=3>

Fedora Core 30

PyYAML-5.1-1.fc30

194934 - Fedora Linux 29 FEDORA-2019-5776dfe300 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9894, CVE-2019-9895, CVE-2019-9897, CVE-2019-9898

Description

The scan detected that the host is missing the following update:
FEDORA-2019-5776dfe300

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/2019/3/?count=200&page=8>

Fedora Core 29

putty-0.71-1.fc29

194940 - Fedora Linux 30 FEDORA-2019-2eddaf40d0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9894, CVE-2019-9895, CVE-2019-9897, CVE-2019-9898

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2eddaf40d0

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/2019/3/?count=200&page=3>

Fedora Core 30

putty-0.71-1.fc30

194944 - Fedora Linux 28 FEDORA-2019-2fbce03df3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-2922, CVE-2018-7602, CVE-2019-6341

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2fbce03df3

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/2019/4/?count=200&page=1>

Fedora Core 28

drupal7-7.65-1.fc28

194946 - Fedora Linux 29 FEDORA-2019-023ea18e20 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-11254, CVE-2018-11255, CVE-2018-11256, CVE-2018-12982, CVE-2018-14320, CVE-2018-19532, CVE-2018-20751, CVE-2018-5783, CVE-2019-9199, CVE-2019-9687

Description

The scan detected that the host is missing the following update:
FEDORA-2019-023ea18e20

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/2019/3/?count=200&page=8>

Fedora Core 29

mingw-podof0-0.9.6-8.fc29
podof0-0.9.6-6.fc29

194954 - Fedora Linux 28 FEDORA-2018-b18f9dd65b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-11784, CVE-2018-1336, CVE-2018-8014, CVE-2018-8034, CVE-2018-8037

Description

The scan detected that the host is missing the following update:
FEDORA-2018-b18f9dd65b

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/2019/4/?count=200&page=1>

Fedora Core 28

tomcat-8.5.35-1.fc28

194973 - Fedora Linux 30 FEDORA-2019-a1dc51a9e2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9199, CVE-2019-9687

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a1dc51a9e2

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/2019/3/?count=200&page=3>

Fedora Core 30

podof0-0.9.6-6.fc30
mingw-podof0-0.9.6-8.fc30

194976 - Fedora Linux 28 FEDORA-2019-9e1a1cd634 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9894, CVE-2019-9895, CVE-2019-9897, CVE-2019-9898

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9e1a1cd634

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/2019/3/?count=200&page=8>

Fedora Core 28

putty-0.71-1.fc28

194980 - Fedora Linux 28 FEDORA-2019-79bd99f9a8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6926, CVE-2017-6927, CVE-2017-6930, CVE-2017-6931, CVE-2018-7600, CVE-2018-7602, CVE-2018-9861, CVE-2019-6341

Description

The scan detected that the host is missing the following update:
FEDORA-2019-79bd99f9a8

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/2019/4/?count=200&page=1>

Fedora Core 28

drupal8-8.6.13-1.fc28

196280 - Red Hat Enterprise Linux RHSA-2019-0697 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-8786, CVE-2018-8787, CVE-2018-8788

Description

The scan detected that the host is missing the following update:
RHSA-2019-0697

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-April/msg00001.html>

RHEL7D

x86_64
freerdp-debuginfo-1.0.2-15.el7_6.1
freerdp-devel-1.0.2-15.el7_6.1
freerdp-libs-1.0.2-15.el7_6.1
freerdp-plugins-1.0.2-15.el7_6.1
freerdp-1.0.2-15.el7_6.1

RHEL7S

x86_64
freerdp-debuginfo-1.0.2-15.el7_6.1
freerdp-devel-1.0.2-15.el7_6.1
freerdp-libs-1.0.2-15.el7_6.1
freerdp-plugins-1.0.2-15.el7_6.1
freerdp-1.0.2-15.el7_6.1

RHEL7WS

x86_64
freerdp-debuginfo-1.0.2-15.el7_6.1
freerdp-devel-1.0.2-15.el7_6.1
freerdp-libs-1.0.2-15.el7_6.1
freerdp-plugins-1.0.2-15.el7_6.1
freerdp-1.0.2-15.el7_6.1

89013 - Slackware Linux 14.2 SSA:2019-092-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3835, CVE-2019-3838, CVE-2019-6116

Description

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

SSA:2019-092-01

Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.371149>

Slackware 14.2

x86_64
ghostscript-9.26-x86_64-1

i586
ghostscript-9.26-i586-1

132499 - Oracle VM OVMSA-2019-0011 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10879

Description

The scan detected that the host is missing the following update:
OVMSA-2019-0011

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2019-March/000933.html>

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-124.26.5.el6uek
kernel-uek-4.1.12-124.26.5.el6uek

147749 - SuSE Linux 42.3 openSUSE-SU-2019:1104-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000807, CVE-2018-1000808

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1104-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00032.html>

SuSE Linux 42.3
x86_64
python3-cryptography-debuginfo-1.3.1-5.3.1
python3-cryptography-1.3.1-5.3.1
python-cryptography-debuginfo-1.3.1-5.3.1
python-cryptography-1.3.1-5.3.1
python-cryptography-debugsource-1.3.1-5.3.1

noarch
python3-pyOpenSSL-16.0.0-5.8.2
python-pyOpenSSL-doc-16.0.0-5.8.2
python3-pyOpenSSL-doc-16.0.0-5.8.2
python-pyOpenSSL-16.0.0-5.8.2

147764 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0839-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10360, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0839-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-April/005284.html>

SuSE SLED 12 SP3

x86_64
file-debugsource-5.22-10.12.2
file-5.22-10.12.2
libmagic1-debuginfo-32bit-5.22-10.12.2
file-debuginfo-5.22-10.12.2
libmagic1-32bit-5.22-10.12.2
libmagic1-debuginfo-5.22-10.12.2
libmagic1-5.22-10.12.2
file-magic-5.22-10.12.2

SuSE SLED 12 SP4

x86_64
file-debugsource-5.22-10.12.2
file-5.22-10.12.2
libmagic1-debuginfo-32bit-5.22-10.12.2
file-debuginfo-5.22-10.12.2
libmagic1-32bit-5.22-10.12.2
libmagic1-debuginfo-5.22-10.12.2
libmagic1-5.22-10.12.2
file-magic-5.22-10.12.2

SuSE SLES 12 SP4

x86_64
file-debugsource-5.22-10.12.2
file-5.22-10.12.2
libmagic1-debuginfo-32bit-5.22-10.12.2
file-debuginfo-5.22-10.12.2
libmagic1-32bit-5.22-10.12.2
libmagic1-debuginfo-5.22-10.12.2
libmagic1-5.22-10.12.2
file-magic-5.22-10.12.2

SuSE SLES 12 SP3

x86_64
file-debugsource-5.22-10.12.2
file-5.22-10.12.2
libmagic1-debuginfo-32bit-5.22-10.12.2
file-debuginfo-5.22-10.12.2
libmagic1-32bit-5.22-10.12.2
libmagic1-debuginfo-5.22-10.12.2
libmagic1-5.22-10.12.2
file-magic-5.22-10.12.2

147766 - SuSE Linux 15.0 openSUSE-SU-2019:1083-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12178, CVE-2018-12180, CVE-2018-3630

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1083-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00120.html>

SuSE Linux 15.0

i586

ovmf-2017+git1510945757.b2662641d5-lp150.4.13.1

ovmf-tools-2017+git1510945757.b2662641d5-lp150.4.13.1

noarch

qemu-ovmf-ia32-2017+git1510945757.b2662641d5-lp150.4.13.1

qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-lp150.4.13.1

x86_64

qemu-ovmf-x86_64-debug-2017+git1510945757.b2662641d5-lp150.4.13.1

ovmf-2017+git1510945757.b2662641d5-lp150.4.13.1

ovmf-tools-2017+git1510945757.b2662641d5-lp150.4.13.1

147771 - SuSE SLES 11 SP4 SUSE-SU-2019:14003-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20346

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:14003-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-April/005281.html>

SuSE SLES 11 SP4

i586

sqlite3-3.7.6.3-1.4.7.3.1

libsqlite3-0-3.7.6.3-1.4.7.3.1

x86_64

libsqlite3-0-32bit-3.7.6.3-1.4.7.3.1

sqlite3-3.7.6.3-1.4.7.3.1

libsqlite3-0-3.7.6.3-1.4.7.3.1

147781 - SuSE SLES 11 SP4 SUSE-SU-2019:14002-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5102, CVE-2019-6128

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:14002-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-April/005277.html>

SuSE SLES 11 SP4

i586

libtiff3-3.8.2-141.169.31.1

tiff-3.8.2-141.169.31.1

x86_64

libtiff3-32bit-3.8.2-141.169.31.1

tiff-3.8.2-141.169.31.1

libtiff3-3.8.2-141.169.31.1

147787 - SuSE SLES 11 SP4 SUSE-SU-2019:13998-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7572, CVE-2019-7573, CVE-2019-7574, CVE-2019-7575, CVE-2019-7576, CVE-2019-7577, CVE-2019-7578, CVE-2019-7635, CVE-2019-7636, CVE-2019-7637, CVE-2019-7638

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13998-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005272.html>

SuSE SLES 11 SP4

i586

SDL-1.2.13-106.11.1

x86_64

SDL-1.2.13-106.11.1

SDL-32bit-1.2.13-106.11.1

147790 - SuSE SLES 11 SP4 SUSE-SU-2019:13993-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16412, CVE-2018-16413, CVE-2018-18544, CVE-2018-20467, CVE-2019-7175, CVE-2019-7397, CVE-2019-7398

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13993-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005256.html>

SuSE SLES 11 SP4

i586

libMagickCore1-6.4.3.6-78.92.1

x86_64

libMagickCore1-32bit-6.4.3.6-78.92.1

libMagickCore1-6.4.3.6-78.92.1

182943 - FreeBSD Gitlab Multiple Vulnerabilities (da459dbc-5586-11e9-abd6-001b217b3468)

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

Risk Level: Medium

CVE: CVE-2018-5158, CVE-2019-10108, CVE-2019-10109, CVE-2019-10110, CVE-2019-10111, CVE-2019-10112, CVE-2019-10113, CVE-2019-10114, CVE-2019-10115, CVE-2019-10116, CVE-2019-10117, CVE-2019-10640

Description

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

Gitlab -- Multiple vulnerabilities (da459dbc-5586-11e9-abd6-001b217b3468)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/da459dbc-5586-11e9-abd6-001b217b3468.html>

Affected packages:

11.9.0 <= gitlab-ce < 11.9.4

11.8.0 <= gitlab-ce < 11.8.6

gitlab-ce < 11.7.10

186624 - Ubuntu Linux 12.04 USN-3933-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000410, CVE-2017-18360, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7222, CVE-2019-9213

Description

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

USN-3933-2

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004833.html>

Ubuntu 12.04

linux-image-generic-lpae-lts-trusty_3.13.0.168.157

linux-image-3.13.0-168-generic_3.13.0-168.218~precise1

linux-image-3.13.0-168-generic-lpae_3.13.0-168.218~precise1

linux-image-generic-lts-trusty_3.13.0.168.157

linux-image-3.13.0-168-lowlatency_3.13.0-168.218~precise1

186627 - Ubuntu Linux 14.04, 16.04 USN-3925-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5684

Description

The scan detected that the host is missing the following update:
USN-3925-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004820.html>

Ubuntu 14.04

libfreeimage3_3.15.4-3ubuntu0.1

Ubuntu 16.04

libfreeimageplus3_3.17.0+ds1-2ubuntu0.1

libfreeimage3_3.17.0+ds1-2ubuntu0.1

186631 - Ubuntu Linux 14.04 USN-3933-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000410, CVE-2017-18360, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7222, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
USN-3933-1

Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004832.html>

Ubuntu 14.04

linux-image-generic-lpae_3.13.0.168.179

linux-image-3.13.0-168-generic-lpae_3.13.0-168.218

linux-image-3.13.0-168-powerpc64-smp_3.13.0-168.218

linux-image-generic_3.13.0.168.179

linux-image-powerpc64-emb_3.13.0.168.179

linux-image-3.13.0-168-generic_3.13.0-168.218

linux-image-powerpc-smp_3.13.0.168.179

linux-image-powerpc-e500mc_3.13.0.168.179

linux-image-3.13.0-168-powerpc-e500mc_3.13.0-168.218

linux-image-3.13.0-168-lowlatency_3.13.0-168.218

linux-image-3.13.0-168-powerpc64-emb_3.13.0-168.218

linux-image-powerpc-e500_3.13.0.168.179
linux-image-virtual_3.13.0.168.179
linux-image-powerpc64-smp_3.13.0.168.179
linux-image-lowlatency_3.13.0.168.179
linux-image-3.13.0-168-powerpc-e500_3.13.0-168.218
linux-image-3.13.0-168-powerpc-smp_3.13.0-168.218

186634 - Ubuntu Linux 14.04 USN-3929-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9323, CVE-2017-6369

Description

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

USN-3929-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004825.html>

Ubuntu 14.04

firebird2.5-classic_2.5.2.26540.ds4-9ubuntu1.1
libfbembed2.5_2.5.2.26540.ds4-9ubuntu1.1
libib-util_2.5.2.26540.ds4-9ubuntu1.1
firebird2.5-server-common_2.5.2.26540.ds4-9ubuntu1.1
firebird2.5-superclassic_2.5.2.26540.ds4-9ubuntu1.1
firebird2.5-classic-common_2.5.2.26540.ds4-9ubuntu1.1
libfbclient2_2.5.2.26540.ds4-9ubuntu1.1
firebird2.5-super_2.5.2.26540.ds4-9ubuntu1.1

194926 - Fedora Linux 30 FEDORA-2019-3b96bb5186 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5731, CVE-2017-5732, CVE-2017-5733, CVE-2017-5734, CVE-2017-5735, CVE-2018-12178, CVE-2018-12180, CVE-2018-12181, CVE-2018-3613, CVE-2018-3630

Description

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

FEDORA-2019-3b96bb5186

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/2019/3/?count=200&page=1>

Fedora Core 30

edk2-20190308stable-1.fc30

194933 - Fedora Linux 30 FEDORA-2019-05a780936d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5754, CVE-2019-5755, CVE-2019-5756, CVE-2019-5757, CVE-2019-5758, CVE-2019-5759, CVE-2019-5760, CVE-2019-5761, CVE-2019-5762, CVE-2019-5763, CVE-2019-5764, CVE-2019-5765, CVE-2019-5766, CVE-2019-5767, CVE-2019-5768, CVE-2019-5769, CVE-2019-5770, CVE-2019-5771, CVE-2019-5772, CVE-2019-5773, CVE-2019-5774, CVE-2019-5775, CVE-2019-5776, CVE-2019-5777, CVE-2019-5778, CVE-2019-5779, CVE-2019-5780, CVE-2019-5781, CVE-2019-5782, CVE-2019-5784, CVE-2019-5786, CVE-2019-5787, CVE-2019-5788, CVE-2019-5789, CVE-2019-5790, CVE-2019-5791, CVE-2019-5792, CVE-2019-5793, CVE-2019-5794, CVE-2019-5795, CVE-2019-5796, CVE-2019-5797, CVE-2019-5798, CVE-2019-5799, CVE-2019-5800, CVE-2019-5801, CVE-2019-5802, CVE-2019-5803, CVE-2019-5804

Description

The scan detected that the host is missing the following update:
FEDORA-2019-05a780936d

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/2019/3/?count=200&page=2>

Fedora Core 30

chromium-73.0.3683.75-2.fc30

194945 - Fedora Linux 30 FEDORA-2019-9ef30a3636 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7577

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9ef30a3636

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/2019/3/?count=200&page=4>

Fedora Core 30

SDL-1.2.15-38.fc30

194947 - Fedora Linux 30 FEDORA-2019-fbe83d0e32 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000877, CVE-2018-1000878, CVE-2018-1000879, CVE-2018-1000880, CVE-2019-1000019, CVE-2019-1000020

Description

The scan detected that the host is missing the following update:
FEDORA-2019-fbe83d0e32

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/2019/3/?count=200&page=2>

Fedora Core 30

libarchive-3.3.3-6.fc30

194958 - Fedora Linux 29 FEDORA-2019-bff1cbaba3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5731, CVE-2017-5732, CVE-2017-5733, CVE-2017-5734, CVE-2017-5735, CVE-2018-12178, CVE-2018-12180, CVE-2018-12181, CVE-2018-3613, CVE-2018-3630

Description

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

FEDORA-2019-bff1cbaba3

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/2019/4/?count=200&page=1>

Fedora Core 29

edk2-20190308stable-1.fc29

194962 - Fedora Linux 30 FEDORA-2019-4182dd32eb Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20004, CVE-2018-20005, CVE-2018-20592, CVE-2018-20593

Description

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

FEDORA-2019-4182dd32eb

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/2019/3/?count=200&page=3>

Fedora Core 30

mxml-3.0-1.fc30

194969 - Fedora Linux 29 FEDORA-2019-9993d32c48 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10851, CVE-2018-14626, CVE-2019-3871

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9993d32c48

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/2019/3/?count=200&page=8>

Fedora Core 29

pdns-4.1.7-1.fc29

194972 - Fedora Linux 28 FEDORA-2019-8b5e704a73 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18267, CVE-2018-13988, CVE-2018-20662, CVE-2019-7310

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8b5e704a73

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/2019/4/?count=200&page=2>

Fedora Core 28

poppler-0.62.0-16.fc28

194979 - Fedora Linux 29 FEDORA-2019-f99619e34d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20004, CVE-2018-20005, CVE-2018-20592, CVE-2018-20593

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f99619e34d

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/2019/3/?count=200&page=1>

Fedora Core 29

mxml-3.0-1.fc29

194985 - Fedora Linux 28 FEDORA-2019-b85d4171d4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10851, CVE-2018-14626, CVE-2019-3871

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b85d4171d4

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/2019/3/?count=200&page=8>

Fedora Core 28

pdns-4.1.7-1.fc28

194987 - Fedora Linux 28 FEDORA-2019-3c1aed2aa9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-3846, CVE-2018-3848, CVE-2018-3849

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3c1aed2aa9

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/2019/3/?count=200&page=8>

Fedora Core 28

cfitsio-3.430-2.fc28

194989 - Fedora Linux 29 FEDORA-2019-1a2c059afd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3835, CVE-2019-3838, CVE-2019-6116

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1a2c059afd

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/2019/3/?count=200&page=1>

Fedora Core 29

ghostscript-9.26-4.fc29

194993 - Fedora Linux 29 FEDORA-2019-db1e9b3002 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3877, CVE-2019-3878

Description

The scan detected that the host is missing the following update:
FEDORA-2019-db1e9b3002

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/2019/4/?count=200&page=1>

Fedora Core 29

mod_auth_mellon-0.14.0-5.fc29

194994 - Fedora Linux 30 FEDORA-2019-2fca900a42 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3871

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2fca900a42

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/2019/3/?count=200&page=2>

Fedora Core 30

pdns-4.1.7-1.fc30

194997 - Fedora Linux 30 FEDORA-2019-9f06aa44f6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6116

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9f06aa44f6

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/2019/3/?count=200&page=7>

Fedora Core 30

ghostscript-9.26-3.fc30

24907 - (K10065173) F5 BIG-IP TMM TLS Virtual Server Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2019-6593

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 SSL/TLS CBC ciphers. Successful exploitation could allow an unauthorized attacker to obtain sensitive information.

24916 - (VMSA-2019-0003) VMware Horizon Connection Server Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2019-5513

Description

An information disclosure vulnerability is present in some versions of VMware Horizon Connection Server.

Observation

VMware Horizon Connection Server is a software used for virtual machines connection and configuration.

An information disclosure vulnerability is present in some versions of VMware Horizon Connection Server. The flaw lies in unspecified component. Successful exploitation could allow an attacker to obtain sensitive information.

24921 - Mozilla Firefox ESR Vulnerabilities Prior To ESR 60.6

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9801

Description

Multiple Vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple Vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

24925 - Joomla Missing ACL Check In Sample Data Plugins Vulnerability (20190304)

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

Risk Level: Medium

CVE: CVE-2019-9713

Description

A cross-site scripting vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A cross-site scripting vulnerability is present in some versions of Joomla! CMS. The flaw is due to the lack of ACL checks for sample data plugins. Successful exploitation could allow an attacker to disclose sensitive information on the target system.

24980 - (HT209604) Apple iTunes Multiple Vulnerabilities Prior To 12.9.4

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

Risk Level: Medium

CVE: CVE-2019-6201, CVE-2019-7285, CVE-2019-7292, CVE-2019-8503, CVE-2019-8506, CVE-2019-8515, CVE-2019-8518, CVE-2019-8523, CVE-2019-8524, CVE-2019-8535, CVE-2019-8536, CVE-2019-8542, CVE-2019-8544, CVE-2019-8551, CVE-2019-8556, CVE-2019-8558, CVE-2019-8559, CVE-2019-8562, CVE-2019-8563

Description

Multiple vulnerabilities are present in some versions of Apple iTunes.

Observation

Apple iTunes is a media management software.

Multiple vulnerabilities are present in some versions of Apple iTunes. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code or retrieve sensitive information on the target system.

147739 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:1114-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12558

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1114-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00030.html>

SuSE Linux 15.0
noarch
perl-Email-Address-1.912-lp150.2.3.1

SuSE Linux 42.3
noarch
perl-Email-Address-1.912-5.3.1

147740 - SuSE SLED 15 SUSE-SU-2019:0841-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9918

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0841-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-April/005283.html>

SuSE SLED 15
x86_64
bluez-cups-5.48-5.13.10
bluez-debugsource-5.48-5.13.10
bluez-cups-debuginfo-5.48-5.13.10
bluez-debuginfo-5.48-5.13.10

147744 - SuSE Linux 42.3 openSUSE-SU-2019:1076-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1559, CVE-2019-5737, CVE-2019-5739

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1076-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00112.html>

SuSE Linux 42.3
i586
npm4-4.9.1-23.1
nodejs4-devel-4.9.1-23.1

nodejs4-debugsource-4.9.1-23.1
nodejs4-debuginfo-4.9.1-23.1
nodejs4-4.9.1-23.1

noarch
nodejs4-docs-4.9.1-23.1

x86_64
npm4-4.9.1-23.1
nodejs4-devel-4.9.1-23.1
nodejs4-debugsource-4.9.1-23.1
nodejs4-debuginfo-4.9.1-23.1
nodejs4-4.9.1-23.1

147753 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:1107-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-8955

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1107-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00031.html>
<https://lists.opensuse.org/opensuse-updates/2019-04/msg00034.html>

SuSE Linux 15.0
x86_64
tor-0.3.4.11-lp150.22.1
tor-debuginfo-0.3.4.11-lp150.22.1
tor-debugsource-0.3.4.11-lp150.22.1

SuSE Linux 42.3
x86_64
tor-debugsource-0.3.4.11-21.1
tor-debuginfo-0.3.4.11-21.1
tor-0.3.4.11-21.1

i586
tor-debugsource-0.3.4.11-21.1
tor-debuginfo-0.3.4.11-21.1
tor-0.3.4.11-21.1

147754 - SuSE Linux 15.0 openSUSE-SU-2019:1118-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1152, CVE-2018-11813, CVE-2018-14498

Description

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

openSUSE-SU-2019:1118-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00033.html>

SuSE Linux 15.0

x86_64

libjpeg62-32bit-debuginfo-62.2.0-lp150.4.3.2
libjpeg8-8.1.2-lp150.4.3.2
libturbojpeg0-8.1.2-lp150.4.3.2
libjpeg8-devel-8.1.2-lp150.4.3.2
libjpeg8-debuginfo-8.1.2-lp150.4.3.2
libjpeg62-32bit-62.2.0-lp150.4.3.2
libjpeg8-devel-32bit-8.1.2-lp150.4.3.2
libjpeg62-devel-62.2.0-lp150.4.3.2
libturbojpeg0-debuginfo-8.1.2-lp150.4.3.2
libjpeg-turbo-debuginfo-1.5.3-lp150.4.3.2
libturbojpeg0-32bit-8.1.2-lp150.4.3.2
libjpeg62-devel-32bit-62.2.0-lp150.4.3.2
libjpeg8-32bit-8.1.2-lp150.4.3.2
libjpeg-turbo-1.5.3-lp150.4.3.2
libjpeg8-32bit-debuginfo-8.1.2-lp150.4.3.2
libjpeg62-debuginfo-62.2.0-lp150.4.3.2
libjpeg-turbo-debugsource-1.5.3-lp150.4.3.2
libjpeg62-turbo-debugsource-1.5.3-lp150.4.3.2
libjpeg62-62.2.0-lp150.4.3.2
libjpeg62-turbo-1.5.3-lp150.4.3.2
libturbojpeg0-32bit-debuginfo-8.1.2-lp150.4.3.2

i586

libjpeg8-8.1.2-lp150.4.3.2
libturbojpeg0-8.1.2-lp150.4.3.2
libjpeg8-devel-8.1.2-lp150.4.3.2
libjpeg8-debuginfo-8.1.2-lp150.4.3.2
libjpeg62-devel-62.2.0-lp150.4.3.2
libturbojpeg0-debuginfo-8.1.2-lp150.4.3.2
libjpeg-turbo-debuginfo-1.5.3-lp150.4.3.2
libjpeg-turbo-1.5.3-lp150.4.3.2
libjpeg62-debuginfo-62.2.0-lp150.4.3.2
libjpeg-turbo-debugsource-1.5.3-lp150.4.3.2
libjpeg62-turbo-debugsource-1.5.3-lp150.4.3.2
libjpeg62-62.2.0-lp150.4.3.2
libjpeg62-turbo-1.5.3-lp150.4.3.2

147756 - SuSE SLES 11 SP4 SUSE-SU-2019:14005-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5357

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:14005-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-April/005279.html>

SuSE SLES 11 SP4
i586
ed-0.2-1001.30.3.4

x86_64
ed-0.2-1001.30.3.4

147761 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0787-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1543

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0787-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005259.html>

SuSE SLED 12 SP4
x86_64
libopenssl1_1-debuginfo-32bit-1.1.1-2.9.1
openssl-1_1-debuginfo-1.1.1-2.9.1
libopenssl1_1-32bit-1.1.1-2.9.1
libopenssl1_1-debuginfo-1.1.1-2.9.1
openssl-1_1-debugsource-1.1.1-2.9.1
libopenssl1_1-1.1.1-2.9.1

SuSE SLES 12 SP4
x86_64
libopenssl1_1-debuginfo-32bit-1.1.1-2.9.1
openssl-1_1-debuginfo-1.1.1-2.9.1
libopenssl1_1-32bit-1.1.1-2.9.1
libopenssl1_1-debuginfo-1.1.1-2.9.1
openssl-1_1-debugsource-1.1.1-2.9.1
libopenssl1_1-1.1.1-2.9.1

147765 - SuSE Linux 15.0 openSUSE-SU-2019:1108-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9208, CVE-2019-9209, CVE-2019-9214

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1108-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00025.html>

SuSE Linux 15.0

x86_64

wireshark-ui-qt-debuginfo-2.4.13-lp150.2.23.1
libwireshark9-debuginfo-2.4.13-lp150.2.23.1
libwireshark9-2.4.13-lp150.2.23.1
wireshark-2.4.13-lp150.2.23.1
libwsutil8-2.4.13-lp150.2.23.1
libwscodecs1-debuginfo-2.4.13-lp150.2.23.1
libwiretap7-2.4.13-lp150.2.23.1
libwscodecs1-2.4.13-lp150.2.23.1
wireshark-devel-2.4.13-lp150.2.23.1
wireshark-debuginfo-2.4.13-lp150.2.23.1
libwsutil8-debuginfo-2.4.13-lp150.2.23.1
wireshark-ui-qt-2.4.13-lp150.2.23.1
wireshark-debugsource-2.4.13-lp150.2.23.1
libwiretap7-debuginfo-2.4.13-lp150.2.23.1

i586

wireshark-ui-qt-debuginfo-2.4.13-lp150.2.23.1
libwireshark9-debuginfo-2.4.13-lp150.2.23.1
libwireshark9-2.4.13-lp150.2.23.1
wireshark-2.4.13-lp150.2.23.1
libwsutil8-2.4.13-lp150.2.23.1
libwscodecs1-debuginfo-2.4.13-lp150.2.23.1
libwiretap7-2.4.13-lp150.2.23.1
libwscodecs1-2.4.13-lp150.2.23.1
wireshark-devel-2.4.13-lp150.2.23.1
wireshark-debuginfo-2.4.13-lp150.2.23.1
libwsutil8-debuginfo-2.4.13-lp150.2.23.1
wireshark-ui-qt-2.4.13-lp150.2.23.1
wireshark-debugsource-2.4.13-lp150.2.23.1
libwiretap7-debuginfo-2.4.13-lp150.2.23.1

147772 - SuSE Linux 15.0 openSUSE-SU-2019:1111-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3816, CVE-2019-3833

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1111-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00023.html>

SuSE Linux 15.0

x86_64

libwsman_clientpp1-2.6.7-lp150.2.3.1

libwsman3-2.6.7-lp150.2.3.1
winrs-2.6.7-lp150.2.3.1
libwsman-devel-2.6.7-lp150.2.3.1
libwsman_clientpp-devel-2.6.7-lp150.2.3.1
openwsman-debuginfo-2.6.7-lp150.2.3.1
openwsman-ruby-debuginfo-2.6.7-lp150.2.3.1
openwsman-server-2.6.7-lp150.2.3.1
openwsman-perl-2.6.7-lp150.2.3.1
openwsman-ruby-docs-2.6.7-lp150.2.3.1
libwsman3-debuginfo-2.6.7-lp150.2.3.1
openwsman-java-2.6.7-lp150.2.3.1
openwsman-server-plugin-ruby-2.6.7-lp150.2.3.1
openwsman-ruby-2.6.7-lp150.2.3.1
python3-openwsman-debuginfo-2.6.7-lp150.2.3.1
openwsman-server-debuginfo-2.6.7-lp150.2.3.1
openwsman-perl-debuginfo-2.6.7-lp150.2.3.1
libwsman_clientpp1-debuginfo-2.6.7-lp150.2.3.1
openwsman-server-plugin-ruby-debuginfo-2.6.7-lp150.2.3.1
openwsman-debugsource-2.6.7-lp150.2.3.1
python3-openwsman-2.6.7-lp150.2.3.1

147773 - SuSE Linux 42.3 openSUSE-SU-2019:1058-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7175

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1058-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00099.html>

SuSE Linux 42.3

x86_64

GraphicsMagick-devel-1.3.25-129.1
GraphicsMagick-debugsource-1.3.25-129.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-129.1
perl-GraphicsMagick-1.3.25-129.1
libGraphicsMagick3-config-1.3.25-129.1
libGraphicsMagick++-devel-1.3.25-129.1
GraphicsMagick-debuginfo-1.3.25-129.1
libGraphicsMagick++-Q16-12-1.3.25-129.1
GraphicsMagick-1.3.25-129.1
libGraphicsMagick-Q16-3-1.3.25-129.1
perl-GraphicsMagick-debuginfo-1.3.25-129.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-129.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-129.1
libGraphicsMagickWand-Q16-2-1.3.25-129.1

i586

GraphicsMagick-devel-1.3.25-129.1
GraphicsMagick-debugsource-1.3.25-129.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-129.1

perl-GraphicsMagick-1.3.25-129.1
libGraphicsMagick3-config-1.3.25-129.1
libGraphicsMagick++-devel-1.3.25-129.1
GraphicsMagick-debuginfo-1.3.25-129.1
libGraphicsMagick++-Q16-12-1.3.25-129.1
GraphicsMagick-1.3.25-129.1
libGraphicsMagick-Q16-3-1.3.25-129.1
perl-GraphicsMagick-debuginfo-1.3.25-129.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-129.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-129.1
libGraphicsMagickWand-Q16-2-1.3.25-129.1

147780 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0776-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6196, CVE-2018-6197, CVE-2018-6198

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0776-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005254.html>

SuSE SLED 12 SP3

x86_64
w3m-0.5.3.git20161120-161.3.4
w3m-debugsource-0.5.3.git20161120-161.3.4
w3m-debuginfo-0.5.3.git20161120-161.3.4

SuSE SLED 12 SP4

x86_64
w3m-0.5.3.git20161120-161.3.4
w3m-debugsource-0.5.3.git20161120-161.3.4
w3m-debuginfo-0.5.3.git20161120-161.3.4

SuSE SLES 12 SP4

x86_64
w3m-0.5.3.git20161120-161.3.4
w3m-debugsource-0.5.3.git20161120-161.3.4
w3m-debuginfo-0.5.3.git20161120-161.3.4

SuSE SLES 12 SP3

x86_64
w3m-0.5.3.git20161120-161.3.4
w3m-debugsource-0.5.3.git20161120-161.3.4
w3m-debuginfo-0.5.3.git20161120-161.3.4

147782 - SuSE Linux 15.0 openSUSE-SU-2019:1112-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000656

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1112-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00035.html>

SuSE Linux 15.0
noarch
python2-Flask-doc-0.12.4-lp150.2.3.1
python2-Flask-0.12.4-lp150.2.3.1
python3-Flask-doc-0.12.4-lp150.2.3.1
python3-Flask-0.12.4-lp150.2.3.1

147791 - SuSE SLES 11 SP4 SUSE-SU-2019:13989-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9763

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13989-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005250.html>

SuSE SLES 11 SP4
x86_64
grub2-x86_64-xen-2.00-0.66.8.1
grub2-x86_64-efi-2.00-0.66.8.1

178714 - Gentoo Linux GLSA-201904-05 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-05

Observation

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

<https://security.gentoo.org/glsa/201904-05>

Affected packages:
app-backup/burp < 2.1.32-r1

178715 - Gentoo Linux GLSA-201903-18 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-18

Observation

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

<https://security.gentoo.org/glsa/201903-18>

Affected packages:
media-libs/gd < 2.2.5-r2

178716 - Gentoo Linux GLSA-201903-17 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-17

Observation

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

<https://security.gentoo.org/glsa/201903-17>

Affected packages:
media-libs/sdl2-image < 2.0.4

178717 - Gentoo Linux GLSA-201904-04 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-04

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201904-04>

Affected packages:

app-text/poppler < 0.70.0

178718 - Gentoo Linux GLSA-201903-21 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

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

GLSA-201903-21

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201903-21>

Affected packages:

www-servers/apache < 2.4.38-r1

178719 - Gentoo Linux GLSA-201904-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

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

GLSA-201904-02

Observation

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

For more information see:

<https://security.gentoo.org/glsa/201904-02>

Affected packages:

dev-libs/libical < 3.0.0

178720 - Gentoo Linux GLSA-201904-06 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

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

GLSA-201904-06

Observation

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

<https://security.gentoo.org/glsa/201904-06>

Affected packages:

sys-cluster/glusterfs < 4.1.8

178722 - Gentoo Linux GLSA-201903-20 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-20

Observation

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

<https://security.gentoo.org/glsa/201903-20>

Affected packages:

app-arch/cabextract < 1.8

dev-libs/libmspack < 0.8

178723 - Gentoo Linux GLSA-201904-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-03

Observation

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

<https://security.gentoo.org/glsa/201904-03>

Affected packages:

net-dns/unbound < 1.8.3

178725 - Gentoo Linux GLSA-201904-08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-08

Observation

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

<https://security.gentoo.org/glsa/201904-08>

Affected packages:

dev-vcs/subversion < 1.10.4

178726 - Gentoo Linux GLSA-201904-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-01

Observation

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

<https://security.gentoo.org/glsa/201904-01>

Affected packages:

x11-libs/cairo < 1.16.0-r3

178727 - Gentoo Linux GLSA-201904-07 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-07

Observation

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

<https://security.gentoo.org/glsa/201904-07>

Affected packages:

mail-client/thunderbird < 60.6.1

mail-client/thunderbird-bin < 60.6.1

www-client/firefox < 60.6.1

www-client/firefox-bin < 60.6.1

182949 - FreeBSD Jupyter notebook Open Redirect Vulnerability (fe7e322f-522d-11e9-98b5-216e512dad89)

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

Risk Level: Medium

CVE: CVE-2019-10255

Description

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

Jupyter notebook -- open redirect vulnerability (fe7e322f-522d-11e9-98b5-216e512dad89)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/fe7e322f-522d-11e9-98b5-216e512dad89.html>

Affected packages:

py27-notebook < 5.7.7

py35-notebook < 5.7.7

py36-notebook < 5.7.7

py37-notebook < 5.7.7

186633 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3923-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16867, CVE-2018-16872, CVE-2018-19489, CVE-2018-20123, CVE-2018-20124, CVE-2018-20125, CVE-2018-20126, CVE-2018-20191, CVE-2018-20216, CVE-2019-3812, CVE-2019-6778

Description

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

USN-3923-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004818.html>

Ubuntu 16.04

qemu-system_2.5+dfsg-5ubuntu10.36

qemu-system-ppc_2.5+dfsg-5ubuntu10.36

qemu-system-x86_2.5+dfsg-5ubuntu10.36

qemu-system-sparc_2.5+dfsg-5ubuntu10.36

qemu-system-mips_2.5+dfsg-5ubuntu10.36

qemu-system-aarch64_2.5+dfsg-5ubuntu10.36

qemu-system-misc_2.5+dfsg-5ubuntu10.36

qemu-system-arm_2.5+dfsg-5ubuntu10.36

qemu-system-s390x_2.5+dfsg-5ubuntu10.36

Ubuntu 18.10

qemu-system-ppc_2.12+dfsg-3ubuntu8.6

qemu-system-data_2.12+dfsg-3ubuntu8.6

qemu-system_2.12+dfsg-3ubuntu8.6

qemu-system-misc_2.12+dfsg-3ubuntu8.6
qemu-system-gui_2.12+dfsg-3ubuntu8.6
qemu-system-sparc_2.12+dfsg-3ubuntu8.6
qemu-system-s390x_2.12+dfsg-3ubuntu8.6
qemu-system-arm_2.12+dfsg-3ubuntu8.6
qemu-system-x86_2.12+dfsg-3ubuntu8.6
qemu-system-mips_2.12+dfsg-3ubuntu8.6

Ubuntu 14.04

qemu-system-arm_2.0.0+dfsg-2ubuntu1.45
qemu-system-mips_2.0.0+dfsg-2ubuntu1.45
qemu-system-ppc_2.0.0+dfsg-2ubuntu1.45
qemu-system-aarch64_2.0.0+dfsg-2ubuntu1.45
qemu-system-x86_2.0.0+dfsg-2ubuntu1.45
qemu-system-misc_2.0.0+dfsg-2ubuntu1.45
qemu-system-sparc_2.0.0+dfsg-2ubuntu1.45
qemu-system_2.0.0+dfsg-2ubuntu1.45

Ubuntu 18.04

qemu-system-misc_2.11+dfsg-1ubuntu7.12
qemu-system-mips_2.11+dfsg-1ubuntu7.12
qemu-system-x86_2.11+dfsg-1ubuntu7.12
qemu-system-sparc_2.11+dfsg-1ubuntu7.12
qemu-system-arm_2.11+dfsg-1ubuntu7.12
qemu-system-ppc_2.11+dfsg-1ubuntu7.12
qemu-system-s390x_2.11+dfsg-1ubuntu7.12
qemu-system_2.11+dfsg-1ubuntu7.12

194931 - Fedora Linux 29 FEDORA-2019-e8c1cf958f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3829, CVE-2019-3836

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e8c1cf958f

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/2019/3/?count=200&page=1>

Fedora Core 29

gnutls-3.6.7-1.fc29

194932 - Fedora Linux 28 FEDORA-2019-6baeb15da3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20406, CVE-2019-5010, CVE-2019-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6baeb15da3

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/2019/3/?count=200&page=8>

Fedora Core 28

python34-3.4.10-1.fc28

194935 - Fedora Linux 30 FEDORA-2019-51f1e08207 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1060, CVE-2018-1061, CVE-2018-20406, CVE-2019-5010, CVE-2019-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2019-51f1e08207

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/2019/3/?count=200&page=2>

Fedora Core 30

python35-3.5.7-1.fc30

194939 - Fedora Linux 30 FEDORA-2019-971ded6f90 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3829, CVE-2019-3836

Description

The scan detected that the host is missing the following update:
FEDORA-2019-971ded6f90

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/2019/3/?count=200&page=1>

Fedora Core 30

gnutls-3.6.7-1.fc30

194943 - Fedora Linux 28 FEDORA-2019-87e2fa8e0f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1152, CVE-2018-11813, CVE-2018-14498

Description

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

FEDORA-2019-87e2fa8e0f

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/2019/3/?count=200&page=8>

Fedora Core 28

libjpeg-turbo-1.5.3-7.fc28

194949 - Fedora Linux 29 FEDORA-2019-6b02154aa0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14647, CVE-2018-20406, CVE-2019-5010, CVE-2019-9636

Description

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

FEDORA-2019-6b02154aa0

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/2019/3/?count=200&page=8>

Fedora Core 29

python34-3.4.10-1.fc29

194952 - Fedora Linux 30 FEDORA-2019-af0cd1b8f7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3816, CVE-2019-3833

Description

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

FEDORA-2019-af0cd1b8f7

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/2019/3/?count=200&page=3>

Fedora Core 30

openwsman-2.6.8-5.fc30

194953 - Fedora Linux 30 FEDORA-2019-0c91ce7b3c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1752, CVE-2018-14647, CVE-2019-5010

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0c91ce7b3c

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/2019/3/?count=200&page=7>

Fedora Core 30

python2-docs-2.7.16-1.fc30

python2-2.7.16-1.fc30

194959 - Fedora Linux 29 FEDORA-2019-64b384de9b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3816, CVE-2019-3833

Description

The scan detected that the host is missing the following update:
FEDORA-2019-64b384de9b

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/2019/3/?count=200&page=8>

Fedora Core 29

openwsman-2.6.5-9.fc29

194964 - Fedora Linux 30 FEDORA-2019-735d3953e8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5617

Description

The scan detected that the host is missing the following update:
FEDORA-2019-735d3953e8

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/2019/3/?count=200&page=2>

Fedora Core 30

svgsalamander-1.1.2-1.fc30

194967 - Fedora Linux 28 FEDORA-2019-348166f7fd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3816, CVE-2019-3833

Description

The scan detected that the host is missing the following update:
FEDORA-2019-348166f7fd

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/2019/3/?count=200&page=8>

Fedora Core 28

openwsman-2.6.5-4.fc28

194970 - Fedora Linux 29 FEDORA-2019-3cbce64a64 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5617

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3cbce64a64

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/2019/3/?count=200&page=8>

Fedora Core 29

svgsalamander-1.1.2-1.fc29

194971 - Fedora Linux 28 FEDORA-2019-cf725dd20b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1060, CVE-2018-1061, CVE-2018-14647, CVE-2018-20406, CVE-2019-5010, CVE-2019-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2019-cf725dd20b

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/2019/3/?count=200&page=8>

Fedora Core 28

python35-3.5.7-1.fc28

194974 - Fedora Linux 30 FEDORA-2019-75b4a34d4f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17189

Description

The scan detected that the host is missing the following update:
FEDORA-2019-75b4a34d4f

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/2019/3/?count=200&page=3>

Fedora Core 30

mod_http2-1.14.1-1.fc30

194977 - Fedora Linux 29 FEDORA-2019-35589cfcb5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2922, CVE-2019-6341

Description

The scan detected that the host is missing the following update:
FEDORA-2019-35589cfcb5

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/2019/4/?count=200&page=1>

Fedora Core 29

drupal7-7.65-1.fc29

194990 - Fedora Linux 29 FEDORA-2019-6e1938a3c5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1060, CVE-2018-1061, CVE-2018-14647, CVE-2018-20406, CVE-2019-5010, CVE-2019-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6e1938a3c5

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/2019/3/?count=200&page=8>

Fedora Core 29

python35-3.5.7-1.fc29

194992 - Fedora Linux 30 FEDORA-2019-7d9f3cf3ce Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20406, CVE-2019-5010, CVE-2019-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7d9f3cf3ce

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/2019/3/?count=200&page=2>

Fedora Core 30

python34-3.4.10-1.fc30

194995 - Fedora Linux 30 FEDORA-2019-a122fe704d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a122fe704d

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/2019/3/?count=200&page=2>

Fedora Core 30

python3-3.7.2-8.fc30

194996 - Fedora Linux 30 FEDORA-2019-0664c7724d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16872, CVE-2018-20123, CVE-2018-20191, CVE-2019-3812, CVE-2019-6501, CVE-2019-6778

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0664c7724d

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/2019/3/?count=200&page=8>

Fedora Core 30

qemu-3.1.0-6.fc30

24647 - Oracle WebCenter Sites Critical Patch Update January 2019

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

Risk Level: Medium

CVE: CVE-2017-14735

Description

A vulnerability is present in some versions of Oracle WebCenter Sites.

Observation

Oracle WebCenter Sites is a business-oriented product used to create web pages.

A vulnerability is present in some versions of Oracle WebCenter Sites. The flaw lies in third party tools. Successful exploitation could allow an attacker to affect confidentiality and integrity of the target system.

131322 - Debian Linux 9.0 DSA-4419-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9942

Description

The scan detected that the host is missing the following update:
DSA-4419-1

Observation

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

<http://www.debian.org/security/2019/dsa-4419>

Debian 9.0
all
php-twig-doc_1.24.0-2+deb9u1
php-twig_1.24.0-2+deb9u1

131324 - Debian Linux 9.0 DSA-4420-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796

Description

The scan detected that the host is missing the following update:
DSA-4420-1

Observation

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

<http://www.debian.org/security/2019/dsa-4420>

Debian 9.0
all
thunderbird_1:60.6.1-1~deb9u1

147742 - SuSE SLES 11 SP4 SUSE-SU-2019:13990-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19840

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13990-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005251.html>

SuSE SLES 11 SP4
i586
libwavpack1-4.50.1-1.30.1

x86_64
libwavpack1-4.50.1-1.30.1

147745 - SuSE Linux 15.0 openSUSE-SU-2019:1105-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1559

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1105-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00037.html>

SuSE Linux 15.0

i586

libopenssl1_0_0-1.0.2p-lp150.2.13.1
openssl-1_0_0-debugsource-1.0.2p-lp150.2.13.1
openssl-1_0_0-cavs-1.0.2p-lp150.2.13.1
libopenssl1_0_0-hmac-1.0.2p-lp150.2.13.1
openssl-1_0_0-debuginfo-1.0.2p-lp150.2.13.1
openssl-1_0_0-cavs-debuginfo-1.0.2p-lp150.2.13.1
libopenssl1_0_0-debuginfo-1.0.2p-lp150.2.13.1
openssl-1_0_0-1.0.2p-lp150.2.13.1
libopenssl-1_0_0-devel-1.0.2p-lp150.2.13.1

noarch

openssl-1_0_0-doc-1.0.2p-lp150.2.13.1

x86_64

libopenssl1_0_0-debuginfo-1.0.2p-lp150.2.13.1
openssl-1_0_0-debuginfo-1.0.2p-lp150.2.13.1
openssl-1_0_0-debugsource-1.0.2p-lp150.2.13.1
openssl-1_0_0-1.0.2p-lp150.2.13.1
libopenssl1_0_0-hmac-32bit-1.0.2p-lp150.2.13.1
libopenssl-1_0_0-devel-1.0.2p-lp150.2.13.1
libopenssl1_0_0-32bit-debuginfo-1.0.2p-lp150.2.13.1
libopenssl1_0_0-hmac-1.0.2p-lp150.2.13.1
libopenssl1_0_0-1.0.2p-lp150.2.13.1
libopenssl-1_0_0-devel-32bit-1.0.2p-lp150.2.13.1
libopenssl1_0_0-32bit-1.0.2p-lp150.2.13.1
openssl-1_0_0-cavs-1.0.2p-lp150.2.13.1
openssl-1_0_0-cavs-debuginfo-1.0.2p-lp150.2.13.1

147746 - SuSE SLES 11 SP4 SUSE-SU-2019:13992-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18584, CVE-2018-18585

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13992-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005252.html>

SuSE SLES 11 SP4

i586

libmspack0-0.0.20060920alpha-74.11.6.1

x86_64

libmspack0-0.0.20060920alpha-74.11.6.1

147747 - SuSE Linux 15.0 openSUSE-SU-2019:1116-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19869

Description

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

openSUSE-SU-2019:1116-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00026.html>

SuSE Linux 15.0

i586

libQt5Svg5-debuginfo-5.9.4-lp150.2.3.2

libqt5-qtsvg-devel-5.9.4-lp150.2.3.2

libqt5-qtsvg-debugsource-5.9.4-lp150.2.3.2

libqt5-qtsvg-examples-5.9.4-lp150.2.3.2

libQt5Svg5-5.9.4-lp150.2.3.2

libqt5-qtsvg-examples-debuginfo-5.9.4-lp150.2.3.2

noarch

libqt5-qtsvg-private-headers-devel-5.9.4-lp150.2.3.2

x86_64

libQt5Svg5-debuginfo-5.9.4-lp150.2.3.2

libqt5-qtsvg-devel-5.9.4-lp150.2.3.2

libqt5-qtsvg-debugsource-5.9.4-lp150.2.3.2

libqt5-qtsvg-examples-5.9.4-lp150.2.3.2

libQt5Svg5-32bit-5.9.4-lp150.2.3.2

libQt5Svg5-32bit-debuginfo-5.9.4-lp150.2.3.2

libqt5-qtsvg-devel-32bit-5.9.4-lp150.2.3.2

libQt5Svg5-5.9.4-lp150.2.3.2

libqt5-qtsvg-examples-debuginfo-5.9.4-lp150.2.3.2

147748 - SuSE SLES 11 SP4 SUSE-SU-2019:13999-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13999-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005270.html>

SuSE SLES 11 SP4

i586

ofed-kmp-pae-1.5.4.1_3.0.101_108.87-22.6.1
drbd-kmp-trace-8.4.4_3.0.101_108.87-0.27.6.1
ofed-kmp-default-1.5.4.1_3.0.101_108.87-22.6.1
gfs2-kmp-default-2_3.0.101_108.87-0.24.6.1
iscsitarget-1.4.20-0.43.7.1
drbd-8.4.4-0.27.6.1
ocfs2-kmp-default-1.6_3.0.101_108.87-0.28.9.1
cluster-network-kmp-trace-1.4_3.0.101_108.87-2.32.6.1
ofed-kmp-trace-1.5.4.1_3.0.101_108.87-22.6.1
drbd-kmp-default-8.4.4_3.0.101_108.87-0.27.6.1
drbd-pacemaker-8.4.4-0.27.6.1
iscsitarget-kmp-pae-1.4.20_3.0.101_108.87-0.43.7.1
drbd-heartbeat-8.4.4-0.27.6.1
iscsitarget-kmp-trace-1.4.20_3.0.101_108.87-0.43.7.1
iscsitarget-kmp-xen-1.4.20_3.0.101_108.87-0.43.7.1
drbd-bash-completion-8.4.4-0.27.6.1
drbd-kmp-pae-8.4.4_3.0.101_108.87-0.27.6.1
drbd-utils-8.4.4-0.27.6.1
drbd-kmp-xen-8.4.4_3.0.101_108.87-0.27.6.1
gfs2-kmp-trace-2_3.0.101_108.87-0.24.6.1
oracleasm-kmp-pae-2.0.5_3.0.101_108.87-7.44.2.1
oracleasm-kmp-trace-2.0.5_3.0.101_108.87-7.44.2.1
ocfs2-kmp-xen-1.6_3.0.101_108.87-0.28.9.1
drbd-udev-8.4.4-0.27.6.1
iscsitarget-kmp-default-1.4.20_3.0.101_108.87-0.43.7.1
cluster-network-kmp-default-1.4_3.0.101_108.87-2.32.6.1
ocfs2-kmp-trace-1.6_3.0.101_108.87-0.28.9.1
oracleasm-2.0.5-7.44.2.1
cluster-network-kmp-xen-1.4_3.0.101_108.87-2.32.6.1
gfs2-kmp-xen-2_3.0.101_108.87-0.24.6.1
ocfs2-kmp-pae-1.6_3.0.101_108.87-0.28.9.1
ofed-1.5.4.1-22.6.1
ofed-doc-1.5.4.1-22.6.1
cluster-network-kmp-pae-1.4_3.0.101_108.87-2.32.6.1
gfs2-kmp-pae-2_3.0.101_108.87-0.24.6.1
oracleasm-kmp-xen-2.0.5_3.0.101_108.87-7.44.2.1
oracleasm-kmp-default-2.0.5_3.0.101_108.87-7.44.2.1

x86_64

gfs2-kmp-default-2_3.0.101_108.87-0.24.6.1
drbd-kmp-trace-8.4.4_3.0.101_108.87-0.27.6.1
ofed-kmp-default-1.5.4.1_3.0.101_108.87-22.6.1
ofed-1.5.4.1-22.6.1
iscsitarget-1.4.20-0.43.7.1
drbd-8.4.4-0.27.6.1
ocfs2-kmp-default-1.6_3.0.101_108.87-0.28.9.1
oracleasm-kmp-xen-2.0.5_3.0.101_108.87-7.44.2.1
cluster-network-kmp-trace-1.4_3.0.101_108.87-2.32.6.1
ofed-kmp-trace-1.5.4.1_3.0.101_108.87-22.6.1

drbd-kmp-default-8.4.4_3.0.101_108.87-0.27.6.1
drbd-pacemaker-8.4.4-0.27.6.1
gfs2-kmp-rt-2_3.0.101_rt130_69.42-0.24.6.1
drbd-heartbeat-8.4.4-0.27.6.1
iscsitarget-kmp-trace-1.4.20_3.0.101_108.87-0.43.7.1
iscsitarget-kmp-xen-1.4.20_3.0.101_108.87-0.43.7.1
drbd-kmp-rt-8.4.4_3.0.101_rt130_69.42-0.27.6.1
cluster-network-kmp-xen-1.4_3.0.101_108.87-2.32.6.1
drbd-utils-8.4.4-0.27.6.1
ocfs2-kmp-rt_trace-1.6_3.0.101_rt130_69.42-0.28.9.1
drbd-kmp-xen-8.4.4_3.0.101_108.87-0.27.6.1
gfs2-kmp-trace-2_3.0.101_108.87-0.24.6.1
ocfs2-kmp-rt-1.6_3.0.101_rt130_69.42-0.28.9.1
oracleasm-kmp-trace-2.0.5_3.0.101_108.87-7.44.2.1
iscsitarget-kmp-rt_trace-1.4.20_3.0.101_rt130_69.42-0.43.7.1
cluster-network-kmp-rt_trace-1.4_3.0.101_rt130_69.42-2.32.6.1
ocfs2-kmp-xen-1.6_3.0.101_108.87-0.28.9.1
drbd-udev-8.4.4-0.27.6.1
iscsitarget-kmp-default-1.4.20_3.0.101_108.87-0.43.7.1
cluster-network-kmp-default-1.4_3.0.101_108.87-2.32.6.1
ocfs2-kmp-trace-1.6_3.0.101_108.87-0.28.9.1
oracleasm-2.0.5-7.44.2.1
ofed-kmp-rt_trace-1.5.4.1_3.0.101_rt130_69.42-22.6.1
gfs2-kmp-xen-2_3.0.101_108.87-0.24.6.1
ofed-kmp-rt-1.5.4.1_3.0.101_rt130_69.42-22.6.1
drbd-bash-completion-8.4.4-0.27.6.1
iscsitarget-kmp-rt-1.4.20_3.0.101_rt130_69.42-0.43.7.1
ofed-doc-1.5.4.1-22.6.1
gfs2-kmp-rt_trace-2_3.0.101_rt130_69.42-0.24.6.1
drbd-kmp-rt_trace-8.4.4_3.0.101_rt130_69.42-0.27.6.1
oracleasm-kmp-default-2.0.5_3.0.101_108.87-7.44.2.1
drbd-xen-8.4.4-0.27.6.1
cluster-network-kmp-rt-1.4_3.0.101_rt130_69.42-2.32.6.1

147750 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0803-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-1559

Description

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

SUSE-SU-2019:0803-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005266.html>

SuSE SLED 12 SP3

x86_64

libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.49.1

libopenssl-devel-1.0.2j-60.49.1

libopenssl1_0_0-1.0.2j-60.49.1

openssl-debugsource-1.0.2j-60.49.1

libopenssl1_0_0-32bit-1.0.2j-60.49.1

libopenssl1_0_0-debuginfo-1.0.2j-60.49.1

openssl-1.0.2j-60.49.1
openssl-debuginfo-1.0.2j-60.49.1

SuSE SLES 12 SP3

noarch
openssl-doc-1.0.2j-60.49.1

x86_64
libopenssl1_0_0-hmac-1.0.2j-60.49.1
openssl-debuginfo-1.0.2j-60.49.1
openssl-1.0.2j-60.49.1
libopenssl1_0_0-1.0.2j-60.49.1
openssl-debugsource-1.0.2j-60.49.1
libopenssl1_0_0-32bit-1.0.2j-60.49.1
libopenssl1_0_0-debuginfo-1.0.2j-60.49.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.49.1
libopenssl-devel-1.0.2j-60.49.1
libopenssl1_0_0-hmac-32bit-1.0.2j-60.49.1

147751 - SuSE Linux 42.3 openSUSE-SU-2019:1119-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3838

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1119-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00029.html>

SuSE Linux 42.3

x86_64
ghostscript-devel-9.26a-14.18.1
ghostscript-x11-9.26a-14.18.1
ghostscript-debugsource-9.26a-14.18.1
ghostscript-mini-devel-9.26a-14.18.1
ghostscript-mini-debugsource-9.26a-14.18.1
ghostscript-debuginfo-9.26a-14.18.1
ghostscript-mini-debuginfo-9.26a-14.18.1
ghostscript-x11-debuginfo-9.26a-14.18.1
ghostscript-9.26a-14.18.1
ghostscript-mini-9.26a-14.18.1

i586

ghostscript-devel-9.26a-14.18.1
ghostscript-x11-9.26a-14.18.1
ghostscript-debugsource-9.26a-14.18.1
ghostscript-mini-devel-9.26a-14.18.1
ghostscript-mini-debugsource-9.26a-14.18.1
ghostscript-debuginfo-9.26a-14.18.1
ghostscript-mini-debuginfo-9.26a-14.18.1
ghostscript-x11-debuginfo-9.26a-14.18.1
ghostscript-9.26a-14.18.1

147760 - SuSE SLES 11 SP4 SUSE-SU-2019:14008-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17456, CVE-2017-17457, CVE-2018-19758

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:14008-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-April/005286.html>

SuSE SLES 11 SP4

i586

libsndfile-1.0.20-2.19.12.1

x86_64

libsndfile-1.0.20-2.19.12.1

libsndfile-32bit-1.0.20-2.19.12.1

147762 - SuSE Linux 42.3 openSUSE-SU-2019:1056-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1056-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00095.html>

SuSE Linux 42.3

x86_64

MozillaFirefox-buildsymbols-60.6.1-135.1

MozillaFirefox-devel-60.6.1-135.1

MozillaFirefox-debugsource-60.6.1-135.1

MozillaFirefox-debuginfo-60.6.1-135.1

MozillaFirefox-branding-upstream-60.6.1-135.1

MozillaFirefox-translations-common-60.6.1-135.1

MozillaFirefox-translations-other-60.6.1-135.1

MozillaFirefox-60.6.1-135.1

147763 - SuSE Linux 15.0 openSUSE-SU-2019:1120-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10733

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1120-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00022.html>

SuSE Linux 15.0

x86_64

libgxps-tools-debuginfo-0.3.0-lp150.3.3.2

libgxps-debuginfo-0.3.0-lp150.3.3.2

libgxps-tools-0.3.0-lp150.3.3.2

typelib-1_0-GXPS-0_1-0.3.0-lp150.3.3.2

libgxps-debugsource-0.3.0-lp150.3.3.2

libgxps2-debuginfo-0.3.0-lp150.3.3.2

libgxps2-0.3.0-lp150.3.3.2

libgxps-devel-0.3.0-lp150.3.3.2

147769 - SuSE Linux 15.0 openSUSE-SU-2019:1117-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18384

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1117-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00027.html>

SuSE Linux 15.0

x86_64

unzip-debugsource-6.00-lp150.8.3

unzip-debuginfo-6.00-lp150.8.3

unzip-6.00-lp150.8.3

unzip-doc-6.00-lp150.8.3

unzip-rcc-debuginfo-6.00-lp150.8.3

unzip-rcc-6.00-lp150.8.3

unzip-rcc-debugsource-6.00-lp150.8.3

i586

unzip-debuginfo-6.00-lp150.8.3

unzip-debugsource-6.00-lp150.8.3

unzip-6.00-lp150.8.3

unzip-doc-6.00-lp150.8.3

147770 - SuSE SLES 11 SP4 SUSE-SU-2019:13994-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17294

Description

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

SUSE-SU-2019:13994-1

Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005267.html>

SuSE SLES 11 SP4

i586

python-louis-1.7.0-1.3.16.1

liblouis0-1.7.0-1.3.16.1

liblouis-1.7.0-1.3.16.1

x86_64

python-louis-1.7.0-1.3.16.1

liblouis0-1.7.0-1.3.16.1

liblouis-1.7.0-1.3.16.1

147774 - SuSE Linux 15.0 openSUSE-SU-2019:1121-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3838

Description

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

openSUSE-SU-2019:1121-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00036.html>

SuSE Linux 15.0

x86_64

ghostscript-x11-9.26a-lp150.2.17.2

ghostscript-mini-debugsource-9.26a-lp150.2.17.2

ghostscript-devel-9.26a-lp150.2.17.2

ghostscript-mini-9.26a-lp150.2.17.2

ghostscript-mini-devel-9.26a-lp150.2.17.2

ghostscript-x11-debuginfo-9.26a-lp150.2.17.2

ghostscript-9.26a-lp150.2.17.2

ghostscript-debugsource-9.26a-lp150.2.17.2

ghostscript-mini-debuginfo-9.26a-lp150.2.17.2

ghostscript-debuginfo-9.26a-lp150.2.17.2

i586
ghostscript-x11-9.26a-lp150.2.17.2
ghostscript-mini-debugsource-9.26a-lp150.2.17.2
ghostscript-devel-9.26a-lp150.2.17.2
ghostscript-mini-9.26a-lp150.2.17.2
ghostscript-mini-devel-9.26a-lp150.2.17.2
ghostscript-x11-debuginfo-9.26a-lp150.2.17.2
ghostscript-9.26a-lp150.2.17.2
ghostscript-debugsource-9.26a-lp150.2.17.2
ghostscript-mini-debuginfo-9.26a-lp150.2.17.2
ghostscript-debuginfo-9.26a-lp150.2.17.2

147776 - SuSE Linux 42.3 openSUSE-SU-2019:1085-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2024, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1085-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00118.html>

SuSE Linux 42.3

x86_64
kernel-debug-debugsource-4.4.176-96.1
kernel-syms-4.4.176-96.1
kernel-debug-4.4.176-96.1
kernel-debug-debuginfo-4.4.176-96.1
kernel-debug-devel-4.4.176-96.1
kernel-vanilla-4.4.176-96.1
kernel-default-base-4.4.176-96.1
kernel-default-devel-4.4.176-96.1
kernel-vanilla-base-4.4.176-96.1
kernel-vanilla-debugsource-4.4.176-96.1
kernel-debug-base-debuginfo-4.4.176-96.1
kernel-obs-build-debugsource-4.4.176-96.1
kernel-vanilla-base-debuginfo-4.4.176-96.1
kernel-default-base-debuginfo-4.4.176-96.1
kernel-default-debugsource-4.4.176-96.1
kernel-default-debuginfo-4.4.176-96.1
kernel-debug-devel-debuginfo-4.4.176-96.1
kernel-vanilla-debuginfo-4.4.176-96.1
kernel-vanilla-devel-4.4.176-96.1
kernel-debug-base-4.4.176-96.1
kernel-obs-qa-4.4.176-96.1
kernel-default-4.4.176-96.1
kernel-obs-build-4.4.176-96.1

noarch

kernel-docs-html-4.4.176-96.1
kernel-docs-pdf-4.4.176-96.1
kernel-source-vanilla-4.4.176-96.1

kernel-source-4.4.176-96.1
kernel-devel-4.4.176-96.1
kernel-docs-4.4.176-96.1
kernel-macros-4.4.176-96.1

147783 - SuSE Linux 15.0 openSUSE-SU-2019:1077-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1077-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00114.html>

SuSE Linux 15.0

x86_64

MozillaFirefox-buildsymbols-60.6.1-lp150.3.45.1

MozillaFirefox-60.6.1-lp150.3.45.1

MozillaFirefox-debugsource-60.6.1-lp150.3.45.1

MozillaFirefox-devel-60.6.1-lp150.3.45.1

MozillaFirefox-translations-common-60.6.1-lp150.3.45.1

MozillaFirefox-branding-upstream-60.6.1-lp150.3.45.1

MozillaFirefox-debuginfo-60.6.1-lp150.3.45.1

MozillaFirefox-translations-other-60.6.1-lp150.3.45.1

147784 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0801-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2024, CVE-2019-9213

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0801-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005262.html>

SuSE SLED 12 SP3

x86_64

kernel-default-debugsource-4.4.176-94.88.1

kernel-default-extra-4.4.176-94.88.1

kernel-default-debuginfo-4.4.176-94.88.1

kernel-default-extra-debuginfo-4.4.176-94.88.1

kernel-default-4.4.176-94.88.1

kernel-syms-4.4.176-94.88.1
kernel-default-devel-4.4.176-94.88.1

noarch
kernel-macros-4.4.176-94.88.1
kernel-devel-4.4.176-94.88.1
kernel-source-4.4.176-94.88.1

SuSE SLES 12 SP3
noarch
kernel-macros-4.4.176-94.88.1
kernel-devel-4.4.176-94.88.1
kernel-source-4.4.176-94.88.1

x86_64
kernel-default-base-debuginfo-4.4.176-94.88.1
kernel-default-debugsource-4.4.176-94.88.1
kernel-default-debuginfo-4.4.176-94.88.1
kernel-default-4.4.176-94.88.1
kernel-syms-4.4.176-94.88.1
kernel-default-base-4.4.176-94.88.1
kernel-default-devel-4.4.176-94.88.1

147785 - SuSE SLES 11 SP4 SUSE-SU-2019:14001-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6778, CVE-2019-9824

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:14001-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-April/005274.html>

SuSE SLES 11 SP4
x86_64
xen-tools-domU-4.4.4_40-61.43.2
xen-tools-4.4.4_40-61.43.2
xen-4.4.4_40-61.43.2
xen-doc-html-4.4.4_40-61.43.2
xen-libs-32bit-4.4.4_40-61.43.2
xen-libs-4.4.4_40-61.43.2
xen-kmp-default-4.4.4_40_3.0.101_108.87-61.43.2

i586
xen-tools-domU-4.4.4_40-61.43.2
xen-libs-4.4.4_40-61.43.2
xen-kmp-pae-4.4.4_40_3.0.101_108.87-61.43.2
xen-kmp-default-4.4.4_40_3.0.101_108.87-61.43.2

147788 - SuSE Linux 42.3 openSUSE-SU-2019:1074-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13672, CVE-2017-13673, CVE-2018-16872, CVE-2018-18954, CVE-2018-19364, CVE-2018-19489, CVE-2018-7858, CVE-2019-6778

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1074-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-03/msg00113.html>

SuSE Linux 42.3

i586

qemu-linux-user-debugsource-2.9.1-56.1

qemu-linux-user-2.9.1-56.1

qemu-linux-user-debuginfo-2.9.1-56.1

noarch

qemu-seabios-1.10.2-56.1

qemu-sgabios-8-56.1

qemu-ipxe-1.0.0+-56.1

qemu-vgabios-1.10.2-56.1

x86_64

qemu-ppc-2.9.1-56.1

qemu-block-ssh-2.9.1-56.1

qemu-tools-debuginfo-2.9.1-56.1

qemu-s390-debuginfo-2.9.1-56.1

qemu-block-dmg-debuginfo-2.9.1-56.1

qemu-linux-user-2.9.1-56.1

qemu-extra-2.9.1-56.1

qemu-block-iscsi-2.9.1-56.1

qemu-block-curl-debuginfo-2.9.1-56.1

qemu-guest-agent-debuginfo-2.9.1-56.1

qemu-ppc-debuginfo-2.9.1-56.1

qemu-2.9.1-56.1

qemu-ksm-2.9.1-56.1

qemu-block-ssh-debuginfo-2.9.1-56.1

qemu-lang-2.9.1-56.1

qemu-s390-2.9.1-56.1

qemu-guest-agent-2.9.1-56.1

qemu-tools-2.9.1-56.1

qemu-block-iscsi-debuginfo-2.9.1-56.1

qemu-testsuite-2.9.1-56.2

qemu-linux-user-debugsource-2.9.1-56.1

qemu-debugsource-2.9.1-56.1

qemu-block-rbd-debuginfo-2.9.1-56.1

qemu-linux-user-debuginfo-2.9.1-56.1

qemu-block-rbd-2.9.1-56.1

qemu-kvm-2.9.1-56.1

qemu-x86-2.9.1-56.1

qemu-x86-debuginfo-2.9.1-56.1

qemu-arm-debuginfo-2.9.1-56.1

qemu-block-dmg-2.9.1-56.1

qemu-block-curl-2.9.1-56.1

qemu-extra-debuginfo-2.9.1-56.1

147789 - SuSE Linux 15.0 openSUSE-SU-2019:1115-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19871

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1115-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-04/msg00019.html>

SuSE Linux 15.0

x86_64

libqt5-qtimageformats-5.9.4-lp150.2.3.2
libqt5-qtimageformats-debuginfo-5.9.4-lp150.2.3.2
libqt5-qtimageformats-debugsource-5.9.4-lp150.2.3.2
libqt5-qtimageformats-32bit-debuginfo-5.9.4-lp150.2.3.2
libqt5-qtimageformats-32bit-5.9.4-lp150.2.3.2
libqt5-qtimageformats-devel-5.9.4-lp150.2.3.2

i586

libqt5-qtimageformats-debuginfo-5.9.4-lp150.2.3.2
libqt5-qtimageformats-5.9.4-lp150.2.3.2
libqt5-qtimageformats-devel-5.9.4-lp150.2.3.2
libqt5-qtimageformats-debugsource-5.9.4-lp150.2.3.2

160538 - CentOS 6 CESA-2019-0680 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
CESA-2019-0680

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2019-April/023256.html>

CentOS 6

x86_64

thunderbird-60.6.1-1.el6.centos

i686

thunderbird-60.6.1-1.el6.centos

160541 - CentOS 7 CESA-2019-0681 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
CESA-2019-0681

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2019-April/023258.html>

CentOS 7
x86_64
thunderbird-60.6.1-1.el7.centos

163836 - Oracle Enterprise Linux ELSA-2019-0680 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
ELSA-2019-0680

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-March/008610.html>

OEL6
x86_64
thunderbird-60.6.1-1.0.1.el6_10

163837 - Oracle Enterprise Linux ELSA-2019-0681 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
ELSA-2019-0681

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-March/008609.html>

OEL7
x86_64
thunderbird-60.6.1-1.0.1.el7_6

182946 - FreeBSD znc Denial Of Service (b22d6d4c-53b9-11e9-9310-28d244aee256)

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

Risk Level: Medium

CVE: CVE-2019-9917

Description

The scan detected that the host is missing the following update:
znc -- Denial of Service (b22d6d4c-53b9-11e9-9310-28d244aee256)

Observation

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

<http://www.vuxml.org/freebsd/b22d6d4c-53b9-11e9-9310-28d244aee256.html>

Affected packages:
znc < 1.7.3

194936 - Fedora Linux 30 FEDORA-2019-ee98058a22 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9210

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ee98058a22

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/2019/3/?count=200&page=7>

Fedora Core 30
advancecomp-2.1-10.fc30

194948 - Fedora Linux 30 FEDORA-2019-d5d9cfd359 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3835, CVE-2019-3838

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d5d9cfd359

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/2019/3/?count=200&page=1>

Fedora Core 30

ghostscript-9.26-4.fc30

194963 - Fedora Linux 29 FEDORA-2019-31722b8f33 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10906

Description

The scan detected that the host is missing the following update:
FEDORA-2019-31722b8f33

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/2019/3/?count=200&page=1>

Fedora Core 29

fuse-2.9.9-1.fc29

194975 - Fedora Linux 28 FEDORA-2019-b5e690b96e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19872

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b5e690b96e

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/2019/4/?count=200&page=2>

Fedora Core 28

qt-4.8.7-45.fc28

194978 - Fedora Linux 29 FEDORA-2019-ae913a2f00 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19872

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ae913a2f00

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/2019/3/?count=200&page=1>

Fedora Core 29

qt-4.8.7-45.fc29

194981 - Fedora Linux 30 FEDORA-2019-6dcb6b21de Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9211

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6dcb6b21de

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/2019/4/?count=200&page=1>

Fedora Core 30

pspp-1.2.0-2.fc30

194982 - Fedora Linux 30 FEDORA-2019-03ac7f1d2f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19872

Description

The scan detected that the host is missing the following update:
FEDORA-2019-03ac7f1d2f

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/2019/3/?count=200&page=1>

Fedora Core 30

qt-4.8.7-47.fc30

194999 - Fedora Linux 30 FEDORA-2019-dd00364b71 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10906

Description

The scan detected that the host is missing the following update:
FEDORA-2019-dd00364b71

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/2019/3/?count=200&page=1>

Fedora Core 30

fuse-2.9.9-1.fc30

196283 - Red Hat Enterprise Linux RHSA-2019-0681 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813

Description

The scan detected that the host is missing the following update:
RHSA-2019-0681

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-March/msg00043.html>

RHEL7D

x86_64

thunderbird-60.6.1-1.el7_6

thunderbird-debuginfo-60.6.1-1.el7_6

RHEL7S

x86_64

thunderbird-60.6.1-1.el7_6

thunderbird-debuginfo-60.6.1-1.el7_6

RHEL7WS

x86_64

thunderbird-60.6.1-1.el7_6

thunderbird-debuginfo-60.6.1-1.el7_6

196284 - Red Hat Enterprise Linux RHSA-2019-0680 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18506, CVE-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813

Description

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

RHSA-2019-0680

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2019-March/msg00042.html>

RHEL6S

i386

thunderbird-debuginfo-60.6.1-1.el6_10

thunderbird-60.6.1-1.el6_10

x86_64

thunderbird-debuginfo-60.6.1-1.el6_10

thunderbird-60.6.1-1.el6_10

RHEL6D

x86_64

thunderbird-debuginfo-60.6.1-1.el6_10

thunderbird-60.6.1-1.el6_10

i386

thunderbird-debuginfo-60.6.1-1.el6_10

thunderbird-60.6.1-1.el6_10

RHEL6WS

x86_64

thunderbird-debuginfo-60.6.1-1.el6_10

thunderbird-60.6.1-1.el6_10

i386

thunderbird-debuginfo-60.6.1-1.el6_10

thunderbird-60.6.1-1.el6_10

24905 - (SB10277) Database Security Vulnerability

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

Risk Level: Low

CVE: CVE-2019-3615

Description

A Vulnerability is present in some versions of McAfee Database Security.

Observation

McAfee database security provides real-time security protection for databases from all types of threats and attacks.

A Vulnerability is present in some versions of McAfee Database Security. The flaw is due to improper auto completion in the password fields in the admin login screen. Successful exploitation by an attacker results in information disclosure on the target.

89014 - Slackware Linux 14.2 SSA:2019-086-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2019-086-01

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.427640>

Slackware 14.2
x86_64
gnutls-3.6.7-x86_64-1

i586
gnutls-3.6.7-i586-1

89015 - Slackware Linux 14.2 SSA:2019-092-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2019-092-02

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.327649>

Slackware 14.2
x86_64
wget-1.20.2-x86_64-1

i586
wget-1.20.2-i586-1

182945 - FreeBSD Kubectrl Potential Directory Traversal (6a0129bf-54ad-11e9-987c-1c39475b9f84)

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

Risk Level: Low

CVE: CVE-2019-1002101

Description

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

Kubectl -- Potential directory traversal (6a0129bf-54ad-11e9-987c-1c39475b9f84)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/6a0129bf-54ad-11e9-987c-1c39475b9f84.html>

Affected packages:

kubectl < 1.11.9

1.12.0 <= kubectl < 1.12.7

1.13.0 <= kubectl < 1.13.5

182947 - FreeBSD Apache Multiple Vulnerabilities (cf2105c6-551b-11e9-b95c-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2019-0196, CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220

Description

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

Apache -- Multiple vulnerabilities (cf2105c6-551b-11e9-b95c-b499baebfeaf)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/cf2105c6-551b-11e9-b95c-b499baebfeaf.html>

Affected packages:

apache24 < 2.4.39

182948 - FreeBSD drupal Drupal Core - Moderately Critical - Cross Site Scripting (94d63fd7-508b-11e9-9ba0-4c72b94353b5)

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

Risk Level: Low

CVE: CVE-2019-6341

Description

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

drupal -- Drupal core - Moderately critical - Cross Site Scripting (94d63fd7-508b-11e9-9ba0-4c72b94353b5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/94d63fd7-508b-11e9-9ba0-4c72b94353b5.html>

Affected packages:

drupal7 < 7.65
drupal8 < 8.6.13

194927 - Fedora Linux 30 FEDORA-2019-7b36e8ad7e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7b36e8ad7e

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/2019/3/?count=200&page=2>

Fedora Core 30

drupal7-7.65-1.fc30

194928 - Fedora Linux 29 FEDORA-2019-7d09431f07 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7d09431f07

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/2019/4/?count=200&page=1>

Fedora Core 29

flatpak-1.2.4-1.fc29

194929 - Fedora Linux 29 FEDORA-2019-0767b70f4a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0767b70f4a

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/2019/3/?count=200&page=8>

Fedora Core 29

firefox-66.0.1-1.fc29

194937 - Fedora Linux 28 FEDORA-2019-a0ccc78064 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a0ccc78064

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/2019/3/?count=200&page=8>

Fedora Core 28

firefox-66.0-9.fc28

194938 - Fedora Linux 30 FEDORA-2019-e50f92e4c1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e50f92e4c1

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/2019/3/?count=200&page=3>

Fedora Core 30

glpi-9.4.1.1-1.fc30

194941 - Fedora Linux 30 FEDORA-2019-53b0dc52ee Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-53b0dc52ee

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/2019/3/?count=200&page=7>

Fedora Core 30

xen-4.11.1-4.fc30

194942 - Fedora Linux 30 FEDORA-2019-94fb5d75e6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-94fb5d75e6

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/2019/3/?count=200&page=4>

Fedora Core 30

libzip-1.5.2-1.fc30

194951 - Fedora Linux 30 FEDORA-2019-c1213f866c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c1213f866c

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/2019/3/?count=200&page=6>

Fedora Core 30

nodejs-handlebars-4.0.13-1.fc30

194955 - Fedora Linux 30 FEDORA-2019-3f4ba94260 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3f4ba94260

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/2019/3/?count=200&page=7>

Fedora Core 30

php-7.3.3-1.fc30

194956 - Fedora Linux 28 FEDORA-2019-d7ef743ef0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d7ef743ef0

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/2019/3/?count=200&page=8>

Fedora Core 28

libsvg2-2.42.7-2.fc28

194957 - Fedora Linux 30 FEDORA-2019-0bf4c4c4ed Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0bf4c4c4ed

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/2019/3/?count=200&page=3>

Fedora Core 30

wordpress-5.1.1-1.fc30

194960 - Fedora Linux 29 FEDORA-2019-72b8d3603b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-72b8d3603b

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/2019/3/?count=200&page=7>

Fedora Core 29

thunderbird-60.6.1-1.fc29

194961 - Fedora Linux 29 FEDORA-2019-1d9be4b853 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6341

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1d9be4b853

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/2019/4/?count=200&page=1>

Fedora Core 29

drupal8-8.6.13-1.fc29

194965 - Fedora Linux 30 FEDORA-2019-616045ca76 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2019-616045ca76

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/2019/4/?count=200&page=2>

Fedora Core 30

systemd-241-4.gitcbf14c9.fc30
grub2-2.02-75.fc30

194966 - Fedora Linux 30 FEDORA-2019-874015ee38 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2019-874015ee38

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/2019/3/?count=200&page=3>

Fedora Core 30

php-twig-1.38.2-2.fc30

194968 - Fedora Linux 30 FEDORA-2019-8388d9ef76 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2019-8388d9ef76

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/2019/3/?count=200&page=3>

Fedora Core 30

filezilla-3.41.2-1.fc30

194983 - Fedora Linux 30 FEDORA-2019-06bbb43c20 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2019-06bbb43c20

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/2019/4/?count=200&page=1>

Fedora Core 30

clamav-0.101.2-1.fc30

194984 - Fedora Linux 30 FEDORA-2019-e42442fb33 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9755

Description

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

FEDORA-2019-e42442fb33

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/2019/4/?count=200&page=1>

Fedora Core 30

ntfs-3g-2017.3.23-11.fc30

194986 - Fedora Linux 30 FEDORA-2019-260ca3a81e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2019-260ca3a81e

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/2019/3/?count=200&page=1>

Fedora Core 30

golang-googlecode-go-crypto-0-0.29.20190324gitb7391e9.fc30

194988 - Fedora Linux 30 FEDORA-2019-2fd70709a5 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2fd70709a5

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/2019/3/?count=200&page=1>

Fedora Core 30

flatpak-1.2.4-1.fc30

194991 - Fedora Linux 30 FEDORA-2019-c7c03cd449 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c7c03cd449

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/2019/3/?count=200&page=3>

Fedora Core 30

php-twig2-2.7.2-1.fc30

194998 - Fedora Linux 30 FEDORA-2019-54420e5182 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-54420e5182

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/2019/3/?count=200&page=2>

Fedora Core 30

drupal8-8.6.13-1.fc30

196278 - Red Hat Enterprise Linux RHSA-2019-0693 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2019-0693

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-April/msg00000.html>

RHEL5_9S

x86_64

redhat-release-5Server-5.9.0.5.1

i386

redhat-release-5Server-5.9.0.5.1

147775 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0805-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3811

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0805-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-March/005264.html>

SuSE SLED 12 SP3

x86_64

python-sssconfig-1.13.4-34.31.1

libipa_hbac0-debuginfo-1.13.4-34.31.1

sssdebuginfo-32bit-1.13.4-34.31.1

sssldap-debuginfo-1.13.4-34.31.1

sssd-krb5-debuginfo-1.13.4-34.31.1
libsss_sudo-debuginfo-1.13.4-34.31.1
python-sssd-config-debuginfo-1.13.4-34.31.1
sssd-ldap-1.13.4-34.31.1
libsss_nss_idmap0-1.13.4-34.31.1
sssd-ipa-1.13.4-34.31.1
sssd-krb5-1.13.4-34.31.1
sssd-1.13.4-34.31.1
adcli-debuginfo-0.8.2-1.3.1
libipa_hbac0-1.13.4-34.31.1
adcli-0.8.2-1.3.1
adcli-debugsource-0.8.2-1.3.1
sssd-ad-debuginfo-1.13.4-34.31.1
sssd-krb5-common-1.13.4-34.31.1
sssd-proxy-debuginfo-1.13.4-34.31.1
sssd-ipa-debuginfo-1.13.4-34.31.1
sssd-32bit-1.13.4-34.31.1
sssd-debugsource-1.13.4-34.31.1
sssd-proxy-1.13.4-34.31.1
libsss_idmap0-debuginfo-1.13.4-34.31.1
sssd-ad-1.13.4-34.31.1
libsss_sudo-1.13.4-34.31.1
sssd-krb5-common-debuginfo-1.13.4-34.31.1
libsss_nss_idmap0-debuginfo-1.13.4-34.31.1
libsss_idmap0-1.13.4-34.31.1
sssd-tools-1.13.4-34.31.1
sssd-debuginfo-1.13.4-34.31.1
sssd-tools-debuginfo-1.13.4-34.31.1

SuSE SLES 12 SP3

x86_64

python-sssd-config-1.13.4-34.31.1
libipa_hbac0-debuginfo-1.13.4-34.31.1
sssd-debuginfo-32bit-1.13.4-34.31.1
sssd-ldap-debuginfo-1.13.4-34.31.1
sssd-krb5-debuginfo-1.13.4-34.31.1
libsss_sudo-debuginfo-1.13.4-34.31.1
python-sssd-config-debuginfo-1.13.4-34.31.1
sssd-ldap-1.13.4-34.31.1
libsss_nss_idmap0-1.13.4-34.31.1
sssd-ipa-1.13.4-34.31.1
sssd-krb5-1.13.4-34.31.1
sssd-1.13.4-34.31.1
adcli-debuginfo-0.8.2-1.3.1
libipa_hbac0-1.13.4-34.31.1
adcli-0.8.2-1.3.1
adcli-debugsource-0.8.2-1.3.1
sssd-ad-debuginfo-1.13.4-34.31.1
sssd-krb5-common-1.13.4-34.31.1
sssd-proxy-debuginfo-1.13.4-34.31.1
sssd-ipa-debuginfo-1.13.4-34.31.1
sssd-32bit-1.13.4-34.31.1
sssd-debugsource-1.13.4-34.31.1
sssd-proxy-1.13.4-34.31.1
libsss_idmap0-debuginfo-1.13.4-34.31.1
sssd-ad-1.13.4-34.31.1
libsss_sudo-1.13.4-34.31.1
sssd-krb5-common-debuginfo-1.13.4-34.31.1
libsss_nss_idmap0-debuginfo-1.13.4-34.31.1
libsss_idmap0-1.13.4-34.31.1

sssd-tools-1.13.4-34.31.1
sssd-debuginfo-1.13.4-34.31.1
sssd-tools-debuginfo-1.13.4-34.31.1

194950 - Fedora Linux 30 FEDORA-2019-676e120269 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9704, CVE-2019-9705

Description

The scan detected that the host is missing the following update:
FEDORA-2019-676e120269

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/2019/3/?count=200&page=3>

Fedora Core 30

cronie-1.5.4-1.fc30

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.

182935 - FreeBSD Rails Action View Vulnerabilities (1396a74a-4997-11e9-b5f1-83edb3f89ba1)

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

Risk Level: High

CVE: CVE-2019-5418, CVE-2019-5419

Update Details

Risk is updated

194842 - Fedora Linux 29 FEDORA-2019-7d1a63acc8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3828

Update Details

Risk is updated

131287 - Debian Linux 9.0 DSA-4381-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16858

[Update Details](#)

Risk is updated

131292 - Debian Linux 9.0 DSA-4388-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12546, CVE-2018-12550, CVE-2018-12551

[Update Details](#)

Risk is updated

131316 - Debian Linux 9.0 DSA-4414-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3877, CVE-2019-3878

[Update Details](#)

Risk is updated

147667 - SuSE Linux 15.0 openSUSE-SU-2019:0233-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12546, CVE-2018-12550, CVE-2018-12551

[Update Details](#)

Risk is updated

147695 - SuSE Linux 15.0 openSUSE-SU-2019:0323-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3817

[Update Details](#)

Risk is updated

147704 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0581-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12178, CVE-2018-12180, CVE-2018-3630

[Update Details](#)

Risk is updated

147710 - SuSE SLES 12 SP3 SUSE-SU-2019:0579-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12178, CVE-2018-12180, CVE-2018-3630

[Update Details](#)

Risk is updated

147724 - SuSE Linux 42.3 openSUSE-SU-2019:0348-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12178, CVE-2018-12180, CVE-2018-3630

[Update Details](#)

Risk is updated

194775 - Fedora Linux 28 FEDORA-2019-8cbe2a05cd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12546, CVE-2018-12550, CVE-2018-12551

[Update Details](#)

Risk is updated

147621 - SuSE Linux 15.0 openSUSE-SU-2019:0143-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6690

[Update Details](#)

Risk is updated

182861 - FreeBSD Gitlab Multiple Vulnerabilities (9d3428d4-f98c-11e8-a148-001b217b3468)

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

Risk Level: Medium

CVE: CVE-2018-19856

[Update Details](#)

Risk is updated

182868 - FreeBSD Gitlab Arbitrary File Read In GitLab Project Import With Git LFS (757e6ee8-ff91-11e8-a148-001b217b3468)

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

Risk Level: Medium

CVE: CVE-2018-20144

[Update Details](#)

Risk is updated

131291 - Debian Linux 9.0 DSA-4385-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3814

[Update Details](#)

Risk is updated

131293 - Debian Linux 9.0 DSA-4389-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20340

[Update Details](#)

Risk is updated

131299 - Debian Linux 9.0 DSA-4393-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6454

[Update Details](#)

Risk is updated

147483 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2018:4194-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5731, CVE-2017-5732, CVE-2017-5733, CVE-2017-5734, CVE-2017-5735, CVE-2018-3613

[Update Details](#)

Risk is updated

147486 - SuSE SLES 12 SP3 SUSE-SU-2018:4207-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5731, CVE-2017-5732, CVE-2017-5733, CVE-2017-5734, CVE-2017-5735, CVE-2018-3613

[Update Details](#)

Risk is updated

147494 - SuSE Linux 42.3 openSUSE-SU-2018:4254-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5731, CVE-2017-5732, CVE-2017-5733, CVE-2017-5734, CVE-2017-5735, CVE-2018-3613

[Update Details](#)

Risk is updated

147501 - SuSE Linux 15.0 openSUSE-SU-2018:4240-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5731, CVE-2017-5732, CVE-2017-5733, CVE-2017-5734, CVE-2017-5735, CVE-2018-3613

[Update Details](#)

Risk is updated

147633 - SuSE Linux 42.3 openSUSE-SU-2019:0199-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20340

[Update Details](#)

Risk is updated

147649 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0428-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6454

[Update Details](#)

Risk is updated

147672 - SuSE Linux 15.0 openSUSE-SU-2019:0243-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3814

[Update Details](#)

Risk is updated

147692 - SuSE Linux 15.0 openSUSE-SU-2019:0255-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6454

[Update Details](#)

Risk is updated

147693 - SuSE Linux 42.3 openSUSE-SU-2019:0268-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2019-6454

[Update Details](#)

Risk is updated

147737 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0719-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-3838

[Update Details](#)

Risk is updated

160523 - CentOS 7 CESA-2019-0368 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-6454

[Update Details](#)

Risk is updated

160535 - CentOS 7 CESA-2019-0633 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-3835, CVE-2019-3838

[Update Details](#)

Risk is updated

163808 - Oracle Enterprise Linux ELSA-2019-0368 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-6454

[Update Details](#)

Risk is updated

163830 - Oracle Enterprise Linux ELSA-2019-0633 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-3835, CVE-2019-3838

[Update Details](#)

Risk is updated

182903 - FreeBSD mail/dovecot Suitable Client Certificate Can Be Used To Login As Other User (1340fcc1-2953-11e9-bc44-a4badb296695)

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

Risk Level: Medium

CVE: CVE-2019-3814

[Update Details](#)

Risk is updated

182911 - FreeBSD OpenJPEG Integer Overflow (5efd7a93-2dfb-11e9-9549-e980e869c2e9)

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

Risk Level: Medium

CVE: CVE-2018-5727

[Update Details](#)

FASLScript is updated

182924 - FreeBSD asterisk Remote Crash Vulnerability With SDP Protocol Violation (be0e3817-3bfe-11e9-9cd6-001999f8d30b)

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

Risk Level: Medium

CVE: CVE-2019-7251

[Update Details](#)

Risk is updated

186558 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3881-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3814

[Update Details](#)

Risk is updated

186579 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3891-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6454

[Update Details](#)

Risk is updated

186615 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3915-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3835, CVE-2019-3838

[Update Details](#)

Risk is updated

196253 - Red Hat Enterprise Linux RHSA-2019-0368 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6454

[Update Details](#)

Risk is updated

196274 - Red Hat Enterprise Linux RHSA-2019-0633 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3835, CVE-2019-3838

[Update Details](#)

Risk is updated

147679 - SuSE Linux 15.0 openSUSE-SU-2019:0261-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3827

[Update Details](#)

Risk is updated

147728 - SuSE SLES 12 SP3 SUSE-SU-2019:0738-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12181

[Update Details](#)

Risk is updated

182937 - FreeBSD Python NULL Pointer Dereference Vulnerability (d74371d2-4fee-11e9-a5cd-1df8a848de3d)

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

Risk Level: Low

CVE: CVE-2019-5010

[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 2019 McAfee, Inc.

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