2019-MAY-03
FSL version 7.6.109

MCAFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

195087 - Fedora Linux 28 FEDORA-2019-1b986880ea Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-16880, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-3882, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9500, CVE-2019-9857

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1b986880ea

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=4

Fedora Core 28

kernel-headers-5.0.9-100.fc28
kernel-5.0.9-100.fc28
kernel-tools-5.0.9-100.fc28

25078 - WECON LeviStudioU Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2019-6537, CVE-2019-6539, CVE-2019-6541

Description

Multiple vulnerabilities are present in some versions of WECON LeviStudio.

Observation

WECON LeviStudio is an HMI programming software.

Multiple vulnerabilities are present in some versions of WECON LeviStudio. The flaws occur due to buffer overflow issues. Successful exploitation could allow an attacker to execute arbitrary code.

25079 - Google Chrome Multiple Vulnerabilities Prior To 74.0.3729.108

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

Risk Level: High

CVE: CVE-2019-5805, CVE-2019-5806, CVE-2019-5807, CVE-2019-5808, CVE-2019-5809, CVE-2019-5810, CVE-2019-5811, CVE-2019-5812, CVE-2019-5813, CVE-2019-5814, CVE-2019-5815, CVE-2019-5816, CVE-2019-5817, CVE-2019-5818, CVE-2019-5819, CVE-2019-5820, CVE-2019-5821, CVE-2019-5822, CVE-2019-5823

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, conduct spoofing attacks, disclose sensitive information or bypass security on the targeted system.

147877 - SuSE Linux 15.0 openSUSE-SU-2019:1275-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6556, CVE-2019-5736

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1275-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00186.html

SuSE Linux 15.0
x86_64
lxc-3.1.0-lp150.2.10.1
lxcfs-3.0.3-lp150.2.3.1
lxc-debuginfo-3.1.0-lp150.2.10.1
liblxc1-3.1.0-lp150.2.10.1
liblxc-devel-3.1.0-lp150.2.10.1
liblxc1-debuginfo-3.1.0-lp150.2.10.1
lxcfs-debugsource-3.0.3-lp150.2.3.1
lxc-debugsource-3.1.0-lp150.2.10.1
pam_cgfs-3.1.0-lp150.2.10.1
pam_cgfs-debuginfo-3.1.0-lp150.2.10.1
lxcfs-debuginfo-3.0.3-lp150.2.3.1

noarch
lxc-bash-completion-3.1.0-lp150.2.10.1
lxcfs-hooks-lxc-3.0.3-lp150.2.3.1

24930 - Apache ActiveMQ Denial Of Service Vulnerability

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

Risk Level: High

CVE: CVE-2019-0222

Description

A vulnerability is present in some versions of Apache ActiveMQ.

Observation

Apache ActiveMQ is an open source messaging server.

A vulnerability is present in some versions of Apache ActiveMQ. The flaw is due to improper handling of corrupt MQTT frame. Successful exploitation could allow an attacker to cause a denial of service.

24932 - IBM WebSphere Application Server Admin Console Denial of Service Vulnerability (ibm10875692)

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

Risk Level: High

CVE: CVE-2019-4080

Description

A vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a server engine for Java EE Web applications.

A vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in Admin Console. Successful exploitation could allow an attacker to cause a denial of service.

25027 - Apache HTTP Server Multiple Vulnerabilities Prior To 2.4.39

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

Risk Level: High

CVE: CVE-2019-0196, CVE-2019-0197, CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220

Description

Multiple vulnerabilities are present in some versions of Apache HTTP Server.

Observation

Apache HTTP Server is an open source web server.

Multiple vulnerabilities are present in some versions of Apache HTTP Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause denial of service condition, bypass certain security restrictions and gain elevated privileges.

25038 - IBM DB2 Buffer Overflow Vulnerability (ibm10741481)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-1936

Description

A vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw is due to improper bounds checking. Successful exploitation could allow a local attacker to execute arbitrary code on the target system.

25039 - IBM DB2 Buffer Overflow Vulnerability (ibm10878793)

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

Risk Level: High

CVE: CVE-2019-4014

Description

A vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw is due to insufficient bounds checking on user supplied data. Successful exploitation could allow a local attacker to execute arbitrary code on the target system.

25040 - IBM DB2 Buffer Overflow Vulnerability (ibm10878793)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-4014

Description

A vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw is due to insufficient bounds checking on user supplied data. Successful exploitation could allow a local attacker to execute arbitrary code on the target system.

25050 - Apache Tomcat Vulnerability Prior To 7.0.94

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

Risk Level: High

CVE: CVE-2019-0232

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

A vulnerability is present in some versions of Apache Tomcat. The flaw is due to a bug in JRE passing command line arguments to windows. Successful exploitation could cause remote code execution on the target.

25052 - Apache Tomcat Vulnerability Prior To 9.0.18

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

Risk Level: High

CVE: CVE-2019-0232

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

A vulnerability is present in some versions of Apache Tomcat. The flaw is due to a bug in JRE passing command line arguments to windows. Successful exploitation could cause remote code execution on the target.

25065 - (JSA10924) Juniper Junos OS 'set System Ports Console Insecure' Root Password Recovery Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-0035

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in the Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in Junos OAM component. Successful exploitation could allow an attacker to bypass the security restriction of the system and have access to the system console.

25069 - Oracle Secure Global Desktop Critical Patch Update April 2019

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-11784, CVE-2019-1559, CVE-2019-3822

Description

Multiple vulnerabilities are present in some versions of Oracle Secure Global Desktop.

Observation

Oracle Secure Global Desktop is a secure remote access solution.

Multiple vulnerabilities are present in some versions of Oracle Secure Global Desktop. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose sensitive information and affect integrity and availability.

25074 - (K55101404) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2019-6590

Description

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

Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the Traffic Management Microkernel (TMM) component. Successful exploitation could allow an attacker to cause a denial of service condition.

25076 - IBM DB2 Buffer Overflow Vulnerability (ibm10741481)

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

Risk Level: High

CVE: CVE-2018-1936

Description

A vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw is due to improper bounds checking. Successful exploitation could allow a local attacker to execute arbitrary code on the target system.

147866 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1091-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11365, CVE-2019-11366

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1091-1

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/005408.html

SuSE SLED 12 SP3
x86_64
atftp-debugsource-0.7.0-160.8.1
atftp-debuginfo-0.7.0-160.8.1
atftp-0.7.0-160.8.1

SuSE SLED 12 SP4
x86_64
atftp-debugsource-0.7.0-160.8.1
atftp-debuginfo-0.7.0-160.8.1
atftp-0.7.0-160.8.1

SuSE SLES 12 SP4

x86_64
atftp-debugsource-0.7.0-160.8.1
atftp-debuginfo-0.7.0-160.8.1
atftp-0.7.0-160.8.1

SuSE SLES 12 SP3
x86_64
atftp-debugsource-0.7.0-160.8.1
atftp-debuginfo-0.7.0-160.8.1
atftp-0.7.0-160.8.1

147869 - SuSE Linux 42.3 openSUSE-SU-2019:1293-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20783, CVE-2019-9020, CVE-2019-9021, CVE-2019-9023, CVE-2019-9024, CVE-2019-9637, CVE-2019-9638, CVE-2019-9639, CVE-2019-9640, CVE-2019-9641, CVE-2019-9675

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1293-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00206.html

SuSE Linux 42.3
i586
php7-tokenizer-7.0.7-58.1
php7-odbc-debuginfo-7.0.7-58.1
php7-mcrypt-debuginfo-7.0.7-58.1
php7-ctype-debuginfo-7.0.7-58.1
php7-7.0.7-58.1
php7-zip-debuginfo-7.0.7-58.1
php7-zip-7.0.7-58.1
php7-bcmath-debuginfo-7.0.7-58.1
php7-bz2-7.0.7-58.1
php7-mysql-7.0.7-58.1
php7-exif-7.0.7-58.1
php7-fpm-7.0.7-58.1
php7-dom-7.0.7-58.1
php7-fpm-debuginfo-7.0.7-58.1
php7-imap-7.0.7-58.1
php7-firebird-debuginfo-7.0.7-58.1
php7-intl-debuginfo-7.0.7-58.1
php7-gd-debuginfo-7.0.7-58.1
php7-readline-7.0.7-58.1
php7-curl-7.0.7-58.1
php7-wddx-debuginfo-7.0.7-58.1
php7-gettext-7.0.7-58.1
php7-ldap-debuginfo-7.0.7-58.1
php7-fileinfo-debuginfo-7.0.7-58.1
php7-sockets-debuginfo-7.0.7-58.1
php7-tidy-debuginfo-7.0.7-58.1
php7-iconv-7.0.7-58.1
php7-zlib-debuginfo-7.0.7-58.1

php7-pdo-7.0.7-58.1
php7-sysvmsg-7.0.7-58.1
php7-dom-debuginfo-7.0.7-58.1
php7-fileinfo-7.0.7-58.1
php7-gettext-debuginfo-7.0.7-58.1
php7-sysvsem-debuginfo-7.0.7-58.1
php7-dba-debuginfo-7.0.7-58.1
php7-intl-7.0.7-58.1
php7-xmlwriter-7.0.7-58.1
php7-sysvshm-debuginfo-7.0.7-58.1
php7-xmlrpc-debuginfo-7.0.7-58.1
apache2-mod_php7-debuginfo-7.0.7-58.1
php7-bz2-debuginfo-7.0.7-58.1
php7-xmlwriter-debuginfo-7.0.7-58.1
php7-gmp-debuginfo-7.0.7-58.1
php7-json-7.0.7-58.1
php7-openssl-7.0.7-58.1
php7-posix-debuginfo-7.0.7-58.1
php7-enchant-debuginfo-7.0.7-58.1
php7-odbc-7.0.7-58.1
php7-sqlite-debuginfo-7.0.7-58.1
php7-pcntl-7.0.7-58.1
php7-sockets-7.0.7-58.1
php7-ftp-7.0.7-58.1
php7-ftp-debuginfo-7.0.7-58.1
php7-xsl-7.0.7-58.1
php7-imap-debuginfo-7.0.7-58.1
php7-readline-debuginfo-7.0.7-58.1
php7-posix-7.0.7-58.1
php7-iconv-debuginfo-7.0.7-58.1
php7-enchant-7.0.7-58.1
php7-xmlrpc-7.0.7-58.1
php7-dba-7.0.7-58.1
php7-tokenizer-debuginfo-7.0.7-58.1
apache2-mod_php7-7.0.7-58.1
php7-mbstring-debuginfo-7.0.7-58.1
php7-exif-debuginfo-7.0.7-58.1
php7-pgsql-7.0.7-58.1
php7-fastcgi-7.0.7-58.1
php7-xmlreader-7.0.7-58.1
php7-curl-debuginfo-7.0.7-58.1
php7-shmop-debuginfo-7.0.7-58.1
php7-snmp-7.0.7-58.1
php7-firebird-7.0.7-58.1
php7-ctype-7.0.7-58.1
php7-debugsource-7.0.7-58.1
php7-pspell-7.0.7-58.1
php7-pspell-debuginfo-7.0.7-58.1
php7-zlib-7.0.7-58.1
php7-gmp-7.0.7-58.1
php7-devel-7.0.7-58.1
php7-tidy-7.0.7-58.1
php7-openssl-debuginfo-7.0.7-58.1
php7-gd-7.0.7-58.1
php7-pcntl-debuginfo-7.0.7-58.1
php7-shmop-7.0.7-58.1
php7-phar-7.0.7-58.1
php7-fastcgi-debuginfo-7.0.7-58.1
php7-soap-7.0.7-58.1
php7-debuginfo-7.0.7-58.1

php7-opcache-debuginfo-7.0.7-58.1
php7-sysvshm-7.0.7-58.1
php7-opcache-7.0.7-58.1
php7-pgsql-debuginfo-7.0.7-58.1
php7-sqlite-7.0.7-58.1
php7-sysvsem-7.0.7-58.1
php7-phar-debuginfo-7.0.7-58.1
php7-xsl-debuginfo-7.0.7-58.1
php7-mcrypt-7.0.7-58.1
php7-wddx-7.0.7-58.1
php7-mbstring-7.0.7-58.1
php7-mysql-debuginfo-7.0.7-58.1
php7-json-debuginfo-7.0.7-58.1
php7-sysvmsg-debuginfo-7.0.7-58.1
php7-calendar-debuginfo-7.0.7-58.1
php7-calendar-7.0.7-58.1
php7-soap-debuginfo-7.0.7-58.1
php7-pdo-debuginfo-7.0.7-58.1
php7-ldap-7.0.7-58.1
php7-xmlreader-debuginfo-7.0.7-58.1
php7-bcmath-7.0.7-58.1
php7-snmp-debuginfo-7.0.7-58.1

noarch
php7-pear-7.0.7-58.1
php7-pear-Archive_Tar-7.0.7-58.1

x86_64
php7-tokenizer-7.0.7-58.1
php7-odbc-debuginfo-7.0.7-58.1
php7-mcrypt-debuginfo-7.0.7-58.1
php7-ctype-debuginfo-7.0.7-58.1
php7-7.0.7-58.1
php7-zip-debuginfo-7.0.7-58.1
php7-zip-7.0.7-58.1
php7-bcmath-debuginfo-7.0.7-58.1
php7-bz2-7.0.7-58.1
php7-mysql-7.0.7-58.1
php7-exif-7.0.7-58.1
php7-fpm-7.0.7-58.1
php7-dom-7.0.7-58.1
php7-fpm-debuginfo-7.0.7-58.1
php7-imap-7.0.7-58.1
php7-firebird-debuginfo-7.0.7-58.1
php7-intl-debuginfo-7.0.7-58.1
php7-gd-debuginfo-7.0.7-58.1
php7-readline-7.0.7-58.1
php7-curl-7.0.7-58.1
php7-wddx-debuginfo-7.0.7-58.1
php7-gettext-7.0.7-58.1
php7-ldap-debuginfo-7.0.7-58.1
php7-fileinfo-debuginfo-7.0.7-58.1
php7-sockets-debuginfo-7.0.7-58.1
php7-tidy-debuginfo-7.0.7-58.1
php7-iconv-7.0.7-58.1
php7-zlib-debuginfo-7.0.7-58.1
php7-pdo-7.0.7-58.1
php7-sysvmsg-7.0.7-58.1
php7-dom-debuginfo-7.0.7-58.1
php7-fileinfo-7.0.7-58.1

php7-gettext-debuginfo-7.0.7-58.1
php7-sysvsem-debuginfo-7.0.7-58.1
php7-dba-debuginfo-7.0.7-58.1
php7-intl-7.0.7-58.1
php7-xmlwriter-7.0.7-58.1
php7-sysvshm-debuginfo-7.0.7-58.1
php7-xmlrpc-debuginfo-7.0.7-58.1
apache2-mod_php7-debuginfo-7.0.7-58.1
php7-bz2-debuginfo-7.0.7-58.1
php7-xmlwriter-debuginfo-7.0.7-58.1
php7-gmp-debuginfo-7.0.7-58.1
php7-json-7.0.7-58.1
php7-openssl-7.0.7-58.1
php7-posix-debuginfo-7.0.7-58.1
php7-enchant-debuginfo-7.0.7-58.1
php7-odbc-7.0.7-58.1
php7-sqlite-debuginfo-7.0.7-58.1
php7-pcntl-7.0.7-58.1
php7-sockets-7.0.7-58.1
php7-ftp-7.0.7-58.1
php7-ftp-debuginfo-7.0.7-58.1
php7-xsl-7.0.7-58.1
php7-imap-debuginfo-7.0.7-58.1
php7-readline-debuginfo-7.0.7-58.1
php7-posix-7.0.7-58.1
php7-iconv-debuginfo-7.0.7-58.1
php7-enchant-7.0.7-58.1
php7-xmlrpc-7.0.7-58.1
php7-dba-7.0.7-58.1
php7-tokenizer-debuginfo-7.0.7-58.1
apache2-mod_php7-7.0.7-58.1
php7-mbstring-debuginfo-7.0.7-58.1
php7-exif-debuginfo-7.0.7-58.1
php7-pgsql-7.0.7-58.1
php7-fastcgi-7.0.7-58.1
php7-xmlreader-7.0.7-58.1
php7-curl-debuginfo-7.0.7-58.1
php7-shmop-debuginfo-7.0.7-58.1
php7-snmp-7.0.7-58.1
php7-firebird-7.0.7-58.1
php7-ctype-7.0.7-58.1
php7-debugsource-7.0.7-58.1
php7-pspell-7.0.7-58.1
php7-pspell-debuginfo-7.0.7-58.1
php7-zlib-7.0.7-58.1
php7-gmp-7.0.7-58.1
php7-devel-7.0.7-58.1
php7-tidy-7.0.7-58.1
php7-openssl-debuginfo-7.0.7-58.1
php7-gd-7.0.7-58.1
php7-pcntl-debuginfo-7.0.7-58.1
php7-shmop-7.0.7-58.1
php7-phar-7.0.7-58.1
php7-fastcgi-debuginfo-7.0.7-58.1
php7-soap-7.0.7-58.1
php7-debuginfo-7.0.7-58.1
php7-opcache-debuginfo-7.0.7-58.1
php7-sysvshm-7.0.7-58.1
php7-opcache-7.0.7-58.1
php7-pgsql-debuginfo-7.0.7-58.1

php7-sqlite-7.0.7-58.1
php7-sysvsem-7.0.7-58.1
php7-phar-debuginfo-7.0.7-58.1
php7-xsl-debuginfo-7.0.7-58.1
php7-mcrypt-7.0.7-58.1
php7-wddx-7.0.7-58.1
php7-mbstring-7.0.7-58.1
php7-mysql-debuginfo-7.0.7-58.1
php7-json-debuginfo-7.0.7-58.1
php7-sysvmsg-debuginfo-7.0.7-58.1
php7-calendar-debuginfo-7.0.7-58.1
php7-calendar-7.0.7-58.1
php7-soap-debuginfo-7.0.7-58.1
php7-pdo-debuginfo-7.0.7-58.1
php7-ldap-7.0.7-58.1
php7-xmlreader-debuginfo-7.0.7-58.1
php7-bcmath-7.0.7-58.1
php7-snmp-debuginfo-7.0.7-58.1

147873 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:1272-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11005, CVE-2019-11006, CVE-2019-11007, CVE-2019-11008, CVE-2019-11009, CVE-2019-11010

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1272-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00188.html

SuSE Linux 15.0
x86_64
libGraphicsMagick-Q16-3-1.3.29-lp150.3.25.1
libGraphicsMagick++-devel-1.3.29-lp150.3.25.1
GraphicsMagick-debuginfo-1.3.29-lp150.3.25.1
libGraphicsMagick3-config-1.3.29-lp150.3.25.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.29-lp150.3.25.1
libGraphicsMagick-Q16-3-debuginfo-1.3.29-lp150.3.25.1
GraphicsMagick-1.3.29-lp150.3.25.1
perl-GraphicsMagick-debuginfo-1.3.29-lp150.3.25.1
GraphicsMagick-devel-1.3.29-lp150.3.25.1
libGraphicsMagickWand-Q16-2-1.3.29-lp150.3.25.1
GraphicsMagick-debugsource-1.3.29-lp150.3.25.1
perl-GraphicsMagick-1.3.29-lp150.3.25.1
libGraphicsMagick++-Q16-12-1.3.29-lp150.3.25.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.29-lp150.3.25.1

SuSE Linux 42.3
x86_64
libGraphicsMagick++-Q16-12-1.3.25-132.1
libGraphicsMagick++-devel-1.3.25-132.1
GraphicsMagick-debuginfo-1.3.25-132.1
libGraphicsMagick-Q16-3-1.3.25-132.1

GraphicsMagick-devel-1.3.25-132.1
libGraphicsMagick3-config-1.3.25-132.1
perl-GraphicsMagick-debuginfo-1.3.25-132.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-132.1
perl-GraphicsMagick-1.3.25-132.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-132.1
GraphicsMagick-1.3.25-132.1
GraphicsMagick-debugsource-1.3.25-132.1
libGraphicsMagickWand-Q16-2-1.3.25-132.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-132.1

i586
libGraphicsMagick++-Q16-12-1.3.25-132.1
libGraphicsMagick++-devel-1.3.25-132.1
GraphicsMagick-debuginfo-1.3.25-132.1
libGraphicsMagick-Q16-3-1.3.25-132.1
GraphicsMagick-devel-1.3.25-132.1
libGraphicsMagick3-config-1.3.25-132.1
perl-GraphicsMagick-debuginfo-1.3.25-132.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-132.1
perl-GraphicsMagick-1.3.25-132.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-132.1
GraphicsMagick-1.3.25-132.1
GraphicsMagick-debugsource-1.3.25-132.1
libGraphicsMagickWand-Q16-2-1.3.25-132.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-132.1

147875 - SuSE SLED 15 SUSE-SU-2019:1001-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9755

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1001-1

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/005357.html

SuSE SLED 15
x86_64
ntfs-3g-debuginfo-2016.2.22-3.3.2
ntfsprogs-2016.2.22-3.3.2
libntfs-3g87-debuginfo-2016.2.22-3.3.2
ntfs-3g_ntfsprogs-debugsource-2016.2.22-3.3.2
ntfsprogs-debuginfo-2016.2.22-3.3.2
ntfs-3g-2016.2.22-3.3.2
ntfs-3g_ntfsprogs-debuginfo-2016.2.22-3.3.2
libntfs-3g87-2016.2.22-3.3.2

147883 - SuSE Linux 15.0 openSUSE-SU-2019:1283-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12627

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1283-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00197.html

SuSE Linux 15.0
x86_64
xerces-c-doc-3.1.4-lp150.2.3.1
xerces-c-debuginfo-3.1.4-lp150.2.3.1
libxerces-c-3_1-32bit-3.1.4-lp150.2.3.1
libxerces-c-devel-3.1.4-lp150.2.3.1
xerces-c-debugsource-3.1.4-lp150.2.3.1
libxerces-c-3_1-32bit-debuginfo-3.1.4-lp150.2.3.1
libxerces-c-3_1-3.1.4-lp150.2.3.1
xerces-c-3.1.4-lp150.2.3.1
libxerces-c-3_1-debuginfo-3.1.4-lp150.2.3.1

i586
xerces-c-doc-3.1.4-lp150.2.3.1
xerces-c-debuginfo-3.1.4-lp150.2.3.1
libxerces-c-devel-3.1.4-lp150.2.3.1
xerces-c-debugsource-3.1.4-lp150.2.3.1
libxerces-c-3_1-3.1.4-lp150.2.3.1
xerces-c-3.1.4-lp150.2.3.1
libxerces-c-3_1-debuginfo-3.1.4-lp150.2.3.1

147884 - SuSE SLED 12 SP3, 12 SP4 SUSE-SU-2019:1000-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9755

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1000-1

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/005359.html

SuSE SLED 12 SP4
x86_64
ntfs-3g-debuginfo-2013.1.13-5.6.1
libntfs-3g84-2013.1.13-5.6.1
ntfsprogs-debuginfo-2013.1.13-5.6.1
ntfs-3g_ntfsprogs-debugsource-2013.1.13-5.6.1
libntfs-3g84-debuginfo-2013.1.13-5.6.1

ntfsprogs-2013.1.13-5.6.1
ntfs-3g-2013.1.13-5.6.1

SuSE SLED 12 SP3
x86_64
ntfs-3g-debuginfo-2013.1.13-5.6.1
libntfs-3g84-2013.1.13-5.6.1
ntfsprogs-debuginfo-2013.1.13-5.6.1
ntfs-3g_ntfsprogs-debugsource-2013.1.13-5.6.1
libntfs-3g84-debuginfo-2013.1.13-5.6.1
ntfsprogs-2013.1.13-5.6.1
ntfs-3g-2013.1.13-5.6.1

147885 - SuSE Linux 42.3 openSUSE-SU-2019:1281-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5953

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1281-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00195.html

SuSE Linux 42.3
x86_64
wget-1.14-18.1
wget-debugsource-1.14-18.1
wget-debuginfo-1.14-18.1

i586
wget-1.14-18.1
wget-debugsource-1.14-18.1
wget-debuginfo-1.14-18.1

147887 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1122-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19636, CVE-2018-19637, CVE-2018-19638, CVE-2018-19639, CVE-2018-19640

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1122-1

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/005417.html

SuSE SLED 12 SP3
noarch
supportutils-3.0-95.21.1

SuSE SLED 12 SP4
noarch
supportutils-3.0-95.21.1

SuSE SLES 12 SP4
noarch
hostinfo-1.0.1-19.5.1
supportutils-3.0-95.21.1

SuSE SLES 12 SP3
noarch
hostinfo-1.0.1-19.5.1
supportutils-3.0-95.21.1

147890 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:1102-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-5155, CVE-2016-10739, CVE-2019-9169

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1102-1

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/005411.html

SuSE SLED 12 SP4
x86_64
glibc-locale-debuginfo-2.22-100.8.1
glibc-devel-debuginfo-32bit-2.22-100.8.1
glibc-debuginfo-32bit-2.22-100.8.1
glibc-locale-32bit-2.22-100.8.1
nscd-debuginfo-2.22-100.8.1
glibc-locale-debuginfo-32bit-2.22-100.8.1
glibc-debuginfo-2.22-100.8.1
glibc-devel-32bit-2.22-100.8.1
glibc-locale-2.22-100.8.1
nscd-2.22-100.8.1
glibc-2.22-100.8.1
glibc-32bit-2.22-100.8.1
glibc-debugsource-2.22-100.8.1
glibc-devel-debuginfo-2.22-100.8.1
glibc-devel-2.22-100.8.1

noarch
glibc-i18ndata-2.22-100.8.1

SuSE SLES 12 SP4
noarch
glibc-info-2.22-100.8.1

glibc-html-2.22-100.8.1
glibc-i18ndata-2.22-100.8.1

x86_64
glibc-devel-debuginfo-32bit-2.22-100.8.1
glibc-debuginfo-32bit-2.22-100.8.1
glibc-profile-32bit-2.22-100.8.1
glibc-locale-32bit-2.22-100.8.1
nscd-debuginfo-2.22-100.8.1
glibc-locale-debuginfo-32bit-2.22-100.8.1
glibc-debuginfo-2.22-100.8.1
glibc-devel-32bit-2.22-100.8.1
glibc-locale-2.22-100.8.1
nscd-2.22-100.8.1
glibc-2.22-100.8.1
glibc-32bit-2.22-100.8.1
glibc-locale-debuginfo-2.22-100.8.1
glibc-profile-2.22-100.8.1
glibc-devel-debuginfo-2.22-100.8.1
glibc-devel-2.22-100.8.1
glibc-debugsource-2.22-100.8.1

147891 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1030-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8375

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1030-1

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/005360.html

SuSE SLES 12 SP3
x86_64
libjavascriptcoregtk-4_0-18-debuginfo-2.24.0-2.38.2
libwebkit2gtk-4_0-37-debuginfo-2.24.0-2.38.2
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.0-2.38.2
typelib-1_0-JavaScriptCore-4_0-2.24.0-2.38.2
libjavascriptcoregtk-4_0-18-2.24.0-2.38.2
typelib-1_0-WebKit2-4_0-2.24.0-2.38.2
libwebkit2gtk-4_0-37-2.24.0-2.38.2
webkit2gtk-4_0-injected-bundles-2.24.0-2.38.2
webkit2gtk3-debugsource-2.24.0-2.38.2

SuSE SLES 12 SP4
x86_64
libjavascriptcoregtk-4_0-18-debuginfo-2.24.0-2.38.2
libwebkit2gtk-4_0-37-debuginfo-2.24.0-2.38.2
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.0-2.38.2
typelib-1_0-JavaScriptCore-4_0-2.24.0-2.38.2
libjavascriptcoregtk-4_0-18-2.24.0-2.38.2
typelib-1_0-WebKit2-4_0-2.24.0-2.38.2

libwebkit2gtk-4_0-37-2.24.0-2.38.2
webkit2gtk-4_0-injected-bundles-2.24.0-2.38.2
webkit2gtk3-debugsource-2.24.0-2.38.2

SuSE SLED 12 SP4
x86_64
libjavascriptcoregtk-4_0-18-debuginfo-2.24.0-2.38.2
libwebkit2gtk-4_0-37-debuginfo-2.24.0-2.38.2
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.0-2.38.2
typelib-1_0-JavaScriptCore-4_0-2.24.0-2.38.2
libjavascriptcoregtk-4_0-18-2.24.0-2.38.2
typelib-1_0-WebKit2-4_0-2.24.0-2.38.2
libwebkit2gtk-4_0-37-2.24.0-2.38.2
webkit2gtk-4_0-injected-bundles-2.24.0-2.38.2
webkit2gtk3-debugsource-2.24.0-2.38.2

noarch
libwebkit2gtk3-lang-2.24.0-2.38.2

SuSE SLED 12 SP3
x86_64
libjavascriptcoregtk-4_0-18-debuginfo-2.24.0-2.38.2
libwebkit2gtk-4_0-37-debuginfo-2.24.0-2.38.2
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.0-2.38.2
typelib-1_0-JavaScriptCore-4_0-2.24.0-2.38.2
libjavascriptcoregtk-4_0-18-2.24.0-2.38.2
typelib-1_0-WebKit2-4_0-2.24.0-2.38.2
libwebkit2gtk-4_0-37-2.24.0-2.38.2
webkit2gtk-4_0-injected-bundles-2.24.0-2.38.2
webkit2gtk3-debugsource-2.24.0-2.38.2

noarch
libwebkit2gtk3-lang-2.24.0-2.38.2

147892 - SuSE Linux 15.0 openSUSE-SU-2019:1264-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6438

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1264-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00179.html

SuSE Linux 15.0
x86_64
slurm-seff-17.11.13-lp150.5.20.1
slurm-auth-none-debuginfo-17.11.13-lp150.5.20.1
slurm-sview-17.11.13-lp150.5.20.1
slurm-lua-debuginfo-17.11.13-lp150.5.20.1
slurm-devel-17.11.13-lp150.5.20.1
slurm-17.11.13-lp150.5.20.1

slurm-munge-debuginfo-17.11.13-lp150.5.20.1
slurm-pam_slurm-debuginfo-17.11.13-lp150.5.20.1
slurm-torque-debuginfo-17.11.13-lp150.5.20.1
libpmi0-17.11.13-lp150.5.20.1
slurm-plugins-debuginfo-17.11.13-lp150.5.20.1
slurm-lua-17.11.13-lp150.5.20.1
slurm-debuginfo-17.11.13-lp150.5.20.1
slurm-slurmdbd-17.11.13-lp150.5.20.1
slurm-debugsource-17.11.13-lp150.5.20.1
slurm-pam_slurm-17.11.13-lp150.5.20.1
slurm-openlava-17.11.13-lp150.5.20.1
libslurm32-debuginfo-17.11.13-lp150.5.20.1
slurm-sjstat-17.11.13-lp150.5.20.1
slurm-node-17.11.13-lp150.5.20.1
libpmi0-debuginfo-17.11.13-lp150.5.20.1
perl-slurm-debuginfo-17.11.13-lp150.5.20.1
slurm-sql-debuginfo-17.11.13-lp150.5.20.1
slurm-munge-17.11.13-lp150.5.20.1
slurm-plugins-17.11.13-lp150.5.20.1
slurm-auth-none-17.11.13-lp150.5.20.1
slurm-config-17.11.13-lp150.5.20.1
slurm-slurmdbd-debuginfo-17.11.13-lp150.5.20.1
slurm-doc-17.11.13-lp150.5.20.1
slurm-torque-17.11.13-lp150.5.20.1
slurm-sql-17.11.13-lp150.5.20.1
perl-slurm-17.11.13-lp150.5.20.1
slurm-node-debuginfo-17.11.13-lp150.5.20.1
libslurm32-17.11.13-lp150.5.20.1
slurm-sview-debuginfo-17.11.13-lp150.5.20.1

182969 - FreeBSD py-yaml Arbitrary Code Execution (f6ea18bb-65b9-11e9-8b31-002590045d9c)

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

Risk Level: High

CVE: CVE-2017-18342

Description

The scan detected that the host is missing the following update:
py-yaml -- arbitrary code execution (f6ea18bb-65b9-11e9-8b31-002590045d9c)

Observation

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

http://www.vuxml.org/freebsd/f6ea18bb-65b9-11e9-8b31-002590045d9c.html

Affected packages:
py27-yaml < 4.1
py35-yaml < 4.1
py36-yaml < 4.1
py37-yaml < 4.1

195099 - Fedora Linux 29 FEDORA-2019-1e8a4c6958 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16862, CVE-2018-16880, CVE-2018-18710, CVE-2018-19407, CVE-2018-19824, CVE-2019-3459, CVE-2019-

3460, CVE-2019-3701, CVE-2019-3882, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9500, CVE-2019-9857

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1e8a4c6958

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=4

Fedora Core 29

kernel-tools-5.0.9-200.fc29
kernel-headers-5.0.9-200.fc29
kernel-5.0.9-200.fc29

195101 - Fedora Linux 28 FEDORA-2019-6a756fe3a5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14598, CVE-2018-14599

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6a756fe3a5

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

libX11-1.6.7-1.fc28

195104 - Fedora Linux 30 FEDORA-2019-1dfe95a864 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6446

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1dfe95a864

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

numpy-1.16.3-1.fc30

25049 - Cisco IOS Software Cluster Management Protocol Denial of Service Vulnerability (cisco-sa-20190327-cmp-dos)

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-1746

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw is due to improper input validation in Cluster Management Protocol (CMP). Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

25064 - (VMSA-2019-0006) VMware Workstation Player Multiple Vulnerabilitiess

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

Risk Level: Medium

CVE: CVE-2019-5516, CVE-2019-5517, CVE-2019-5520

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain potentially sensitive information or cause a denial of service condition on the target system.

25066 - (VMSA-2019-0006) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2019-5516, CVE-2019-5517, CVE-2019-5520

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Pro.

Observation

VMware Workstation Pro is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Pro. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information or cause a denial of service condition on the target system.

131339 - Debian Linux 9.0 DSA-4436-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10650, CVE-2019-9956

Description

The scan detected that the host is missing the following update:
DSA-4436-1

Observation

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

http://www.debian.org/security/2019/dsa-4436

Debian 9.0
all
imagemagick_8:6.9.7.4+dfsg-11+deb9u7

131340 - Debian Linux 9.0 DSA-4437-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9928

Description

The scan detected that the host is missing the following update:
DSA-4437-1

Observation

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

http://www.debian.org/security/2019/dsa-4437

Debian 9.0
all
gstreamer1.0-alsa_1.10.4-1+deb9u1
gstreamer1.0-plugins-base-dbg_1.10.4-1+deb9u1
libgstreamer-plugins-base1.0-dev_1.10.4-1+deb9u1
libgstreamer-plugins-base1.0-0_1.10.4-1+deb9u1
gstreamer1.0-plugins-base_1.10.4-1+deb9u1
gstreamer1.0-plugins-base-doc_1.10.4-1+deb9u1
gstreamer1.0-plugins-base-apps_1.10.4-1+deb9u1
gir1.2-gst-plugins-base-1.0_1.10.4-1+deb9u1
gstreamer1.0-x_1.10.4-1+deb9u1

147868 - SuSE Linux 15.0 openSUSE-SU-2019:1273-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636, CVE-2019-9948

Description

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

openSUSE-SU-2019:1273-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00187.html

SuSE Linux 15.0
x86_64
python-2.7.14-lp150.6.10.1
python-curses-debuginfo-2.7.14-lp150.6.10.1
python-gdbm-debuginfo-2.7.14-lp150.6.10.1
python-tk-debuginfo-2.7.14-lp150.6.10.1
python-debuginfo-2.7.14-lp150.6.10.1
python-curses-2.7.14-lp150.6.10.1
python-demo-2.7.14-lp150.6.10.1
python-32bit-debuginfo-2.7.14-lp150.6.10.1
python-32bit-2.7.14-lp150.6.10.1
python-gdbm-2.7.14-lp150.6.10.1
python-idle-2.7.14-lp150.6.10.1
python-debugsource-2.7.14-lp150.6.10.1
python-tk-2.7.14-lp150.6.10.1

i586
python-debugsource-2.7.14-lp150.6.10.1
python-curses-debuginfo-2.7.14-lp150.6.10.1
python-gdbm-debuginfo-2.7.14-lp150.6.10.1
python-curses-2.7.14-lp150.6.10.1
python-2.7.14-lp150.6.10.1
python-idle-2.7.14-lp150.6.10.1
python-tk-debuginfo-2.7.14-lp150.6.10.1
python-demo-2.7.14-lp150.6.10.1
python-gdbm-2.7.14-lp150.6.10.1
python-debuginfo-2.7.14-lp150.6.10.1
python-tk-2.7.14-lp150.6.10.1

147870 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1060-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3859

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1060-1

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/005377.html

SuSE SLED 12 SP3
x86_64
libssh2-1-debuginfo-32bit-1.4.3-20.6.1
libssh2-1-32bit-1.4.3-20.6.1

libssh2_org-debugsource-1.4.3-20.6.1
libssh2-1-debuginfo-1.4.3-20.6.1
libssh2-1-1.4.3-20.6.1

SuSE SLED 12 SP4
x86_64
libssh2-1-debuginfo-32bit-1.4.3-20.6.1
libssh2-1-32bit-1.4.3-20.6.1
libssh2_org-debugsource-1.4.3-20.6.1
libssh2-1-debuginfo-1.4.3-20.6.1
libssh2-1-1.4.3-20.6.1

SuSE SLES 12 SP4
x86_64
libssh2-1-debuginfo-32bit-1.4.3-20.6.1
libssh2-1-32bit-1.4.3-20.6.1
libssh2_org-debugsource-1.4.3-20.6.1
libssh2-1-debuginfo-1.4.3-20.6.1
libssh2-1-1.4.3-20.6.1

SuSE SLES 12 SP3
x86_64
libssh2-1-debuginfo-32bit-1.4.3-20.6.1
libssh2-1-32bit-1.4.3-20.6.1
libssh2_org-debugsource-1.4.3-20.6.1
libssh2-1-debuginfo-1.4.3-20.6.1
libssh2-1-1.4.3-20.6.1

147872 - SuSE Linux 15.0 openSUSE-SU-2019:1291-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3859

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1291-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00205.html

SuSE Linux 15.0
x86_64
libssh2_org-debugsource-1.8.0-lp150.3.6.1
libssh2-1-1.8.0-lp150.3.6.1
libssh2-1-32bit-1.8.0-lp150.3.6.1
libssh2-1-debuginfo-1.8.0-lp150.3.6.1
libssh2-devel-1.8.0-lp150.3.6.1
libssh2-1-32bit-debuginfo-1.8.0-lp150.3.6.1

i586
libssh2_org-debugsource-1.8.0-lp150.3.6.1
libssh2-1-debuginfo-1.8.0-lp150.3.6.1
libssh2-1-1.8.0-lp150.3.6.1
libssh2-devel-1.8.0-lp150.3.6.1

147876 - SuSE Linux 42.3 openSUSE-SU-2019:1290-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3859

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1290-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00204.html

SuSE Linux 42.3
x86_64
libssh2_org-debugsource-1.4.3-19.6.1
libssh2-1-32bit-1.4.3-19.6.1
libssh2-1-debuginfo-32bit-1.4.3-19.6.1
libssh2-1-debuginfo-1.4.3-19.6.1
libssh2-1-1.4.3-19.6.1
libssh2-devel-1.4.3-19.6.1

i586
libssh2-1-1.4.3-19.6.1
libssh2-devel-1.4.3-19.6.1
libssh2-1-debuginfo-1.4.3-19.6.1
libssh2_org-debugsource-1.4.3-19.6.1

147888 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1033-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16412, CVE-2018-16413, CVE-2018-16644, CVE-2018-20467, CVE-2019-10650, CVE-2019-11007, CVE-2019-11008, CVE-2019-11009, CVE-2019-7175, CVE-2019-7395, CVE-2019-7397, CVE-2019-7398, CVE-2019-9956

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1033-1

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/005366.html

SuSE SLES 12 SP3
x86_64
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.108.1
ImageMagick-debugsource-6.8.8.1-71.108.1
ImageMagick-config-6-SUSE-6.8.8.1-71.108.1
libMagickWand-6_Q16-1-6.8.8.1-71.108.1

ImageMagick-debuginfo-6.8.8.1-71.108.1
ImageMagick-config-6-upstream-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-6.8.8.1-71.108.1

SuSE SLES 12 SP4
x86_64
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.108.1
ImageMagick-debugsource-6.8.8.1-71.108.1
ImageMagick-config-6-SUSE-6.8.8.1-71.108.1
libMagickWand-6_Q16-1-6.8.8.1-71.108.1
ImageMagick-debuginfo-6.8.8.1-71.108.1
ImageMagick-config-6-upstream-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-6.8.8.1-71.108.1

SuSE SLED 12 SP4
x86_64
ImageMagick-config-6-SUSE-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.108.1
libMagick++-6_Q16-3-6.8.8.1-71.108.1
ImageMagick-6.8.8.1-71.108.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.108.1
ImageMagick-debugsource-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.108.1
libMagickWand-6_Q16-1-6.8.8.1-71.108.1
ImageMagick-config-6-upstream-6.8.8.1-71.108.1
ImageMagick-debuginfo-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-6.8.8.1-71.108.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.108.1

SuSE SLED 12 SP3
x86_64
ImageMagick-config-6-SUSE-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-71.108.1
libMagick++-6_Q16-3-6.8.8.1-71.108.1
ImageMagick-6.8.8.1-71.108.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-71.108.1
ImageMagick-debugsource-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-71.108.1
libMagickWand-6_Q16-1-6.8.8.1-71.108.1
ImageMagick-config-6-upstream-6.8.8.1-71.108.1
ImageMagick-debuginfo-6.8.8.1-71.108.1
libMagickCore-6_Q16-1-6.8.8.1-71.108.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-71.108.1

147889 - SuSE Linux 15.0 openSUSE-SU-2019:1265-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18444

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1265-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00178.html

SuSE Linux 15.0
x86_64
libIlmImfUtil-2_2-23-debuginfo-2.2.1-lp150.2.3.1
libIlmImfUtil-2_2-23-2.2.1-lp150.2.3.1
libIlmImf-2_2-23-2.2.1-lp150.2.3.1
libIlmImfUtil-2_2-23-32bit-2.2.1-lp150.2.3.1
openexr-2.2.1-lp150.2.3.1
libIlmImfUtil-2_2-23-32bit-debuginfo-2.2.1-lp150.2.3.1
openexr-debugsource-2.2.1-lp150.2.3.1
openexr-devel-2.2.1-lp150.2.3.1
libIlmImf-2_2-23-debuginfo-2.2.1-lp150.2.3.1
libIlmImf-2_2-23-32bit-debuginfo-2.2.1-lp150.2.3.1
openexr-doc-2.2.1-lp150.2.3.1
openexr-debuginfo-2.2.1-lp150.2.3.1
libIlmImf-2_2-23-32bit-2.2.1-lp150.2.3.1

i586
openexr-2.2.1-lp150.2.3.1
openexr-doc-2.2.1-lp150.2.3.1
libIlmImf-2_2-23-2.2.1-lp150.2.3.1
openexr-debugsource-2.2.1-lp150.2.3.1
libIlmImfUtil-2_2-23-debuginfo-2.2.1-lp150.2.3.1
libIlmImfUtil-2_2-23-2.2.1-lp150.2.3.1
libIlmImf-2_2-23-debuginfo-2.2.1-lp150.2.3.1
openexr-debuginfo-2.2.1-lp150.2.3.1
openexr-devel-2.2.1-lp150.2.3.1

160553 - CentOS 7 CESA-2019-0809 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12180

Description

The scan detected that the host is missing the following update:
CESA-2019-0809

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/023280.html

CentOS 7
noarch
OVMF-20180508-3.gitee3198e672e2.el7_6.1

160555 - CentOS 7 CESA-2019-0818 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6974, CVE-2019-7221

Description

The scan detected that the host is missing the following update:
CESA-2019-0818

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/023278.html

CentOS 7
x86_64
kernel-debug-3.10.0-957.12.1.el7
bpftool-3.10.0-957.12.1.el7
perf-3.10.0-957.12.1.el7
kernel-tools-libs-devel-3.10.0-957.12.1.el7
kernel-3.10.0-957.12.1.el7
python-perf-3.10.0-957.12.1.el7
kernel-headers-3.10.0-957.12.1.el7
kernel-tools-libs-3.10.0-957.12.1.el7
kernel-tools-3.10.0-957.12.1.el7
kernel-debug-devel-3.10.0-957.12.1.el7
kernel-devel-3.10.0-957.12.1.el7

noarch
kernel-doc-3.10.0-957.12.1.el7
kernel-abi-whitelists-3.10.0-957.12.1.el7

163852 - Oracle Enterprise Linux ELSA-2019-0809 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12180

Description

The scan detected that the host is missing the following update:
ELSA-2019-0809

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/008668.html

OEL7
x86_64
OVMF-20180508-3.gitee3198e672e2.el7_6.1

163853 - Oracle Enterprise Linux ELSA-2019-0818 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6974, CVE-2019-7221

Description

The scan detected that the host is missing the following update:
ELSA-2019-0818

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/008667.html

OEL7
x86_64
kernel-headers-3.10.0-957.12.1.el7
kernel-3.10.0-957.12.1.el7
kernel-devel-3.10.0-957.12.1.el7
kernel-tools-libs-3.10.0-957.12.1.el7
kernel-tools-3.10.0-957.12.1.el7
kernel-debug-3.10.0-957.12.1.el7
kernel-debug-devel-3.10.0-957.12.1.el7
kernel-doc-3.10.0-957.12.1.el7
kernel-tools-libs-devel-3.10.0-957.12.1.el7
bpftool-3.10.0-957.12.1.el7
kernel-abi-whitelists-3.10.0-957.12.1.el7
python-perf-3.10.0-957.12.1.el7
perf-3.10.0-957.12.1.el7

186668 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3955-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14938, CVE-2018-18409

Description

The scan detected that the host is missing the following update:
USN-3955-1

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/004865.html

Ubuntu 16.04

tcpflow_1.4.5+repack1-1ubuntu0.1
tcpflow-nox_1.4.5+repack1-1ubuntu0.1

Ubuntu 18.10

tcpflow_1.4.5+repack1-4ubuntu0.18.10.1
tcpflow-nox_1.4.5+repack1-4ubuntu0.18.10.1

Ubuntu 18.04

tcpflow-nox_1.4.5+repack1-4ubuntu0.18.04.1
tcpflow_1.4.5+repack1-4ubuntu0.18.04.1

186669 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3958-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9928

Description

The scan detected that the host is missing the following update:
USN-3958-1

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/004868.html

Ubuntu 16.04

gstreamer1.0-plugins-base_1.8.3-1ubuntu0.3
gstreamer0.10-plugins-base_0.10.36-2ubuntu0.2

Ubuntu 18.10

gstreamer1.0-plugins-base_1.14.4-1ubuntu1.1

Ubuntu 18.04

gstreamer1.0-plugins-base_1.14.1-1ubuntu1~ubuntu18.04.2

195092 - Fedora Linux 28 FEDORA-2019-019c5314a0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1050, CVE-2018-1057, CVE-2018-10858, CVE-2018-10918, CVE-2018-10919, CVE-2018-1139, CVE-2018-1140, CVE-2018-14629, CVE-2018-16841, CVE-2018-16851, CVE-2018-16853, CVE-2019-3880

Description

The scan detected that the host is missing the following update:
FEDORA-2019-019c5314a0

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

samba-4.8.11-0.fc28

195115 - Fedora Linux 30 FEDORA-2019-eba1109acd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9494, CVE-2019-9495, CVE-2019-9496, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499

Description

The scan detected that the host is missing the following update:
FEDORA-2019-eba1109acd

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=3

Fedora Core 30

hostapd-2.7-2.fc30

25043 - Joomla JQuery Method Prototype Pollution Vulnerability (20190403)

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

A vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A vulnerability is present in some versions of Joomla! CMS. The flaw lies in the $.extend method of JQuery. Successful exploitation could allow an attacker to execute arbitrary code.

25045 - Joomla Helpsites Refresh Endpoint Callable For Unauthenticated Users Vulnerability (20190402)

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

Risk Level: Medium

CVE: CVE-2019-10946

Description

A vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A vulnerability is present in some versions of Joomla! CMS. The flaw is due to the lack of access checks for "refresh list of helpsites" endpoint of com_users. Successful exploitation could allow an attacker to bypass security restrictions on the target system.

25059 - Wireshark Multiple Vulnerabilities Prior To 2.6.8

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

Risk Level: Medium

CVE: CVE-2019-10894, CVE-2019-10895, CVE-2019-10896, CVE-2019-10899, CVE-2019-10901, CVE-2019-10903

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

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

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

25062 - Oracle WebCenter Sites Critical Patch Update April 2019

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

Risk Level: Medium

CVE: CVE-2019-2578, CVE-2019-2579

Description

Multiple vulnerabilities are present in some versions of Oracle WebCenter Sites.

Observation

Oracle WebCenter Sites is a business-oriented product used to create web pages.

Multiple vulnerabilities are present in some versions of Oracle WebCenter Sites. The flaws lie in the Advanced UI component. Successful exploitation could allow an attacker to affect confidentiality of the target system.

25063 - Wireshark Multiple Vulnerabilities Prior To 2.4.14

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

Risk Level: Medium

CVE: CVE-2019-10894, CVE-2019-10895, CVE-2019-10896, CVE-2019-10899, CVE-2019-10901, CVE-2019-10903

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

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

25068 - Oracle MySQL Server Critical Patch Update April 2019

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

Risk Level: Medium

CVE: CVE-2018-3123, CVE-2019-1559, CVE-2019-2566, CVE-2019-2580, CVE-2019-2581, CVE-2019-2584, CVE-2019-2585, CVE-2019-2587, CVE-2019-2589, CVE-2019-2592, CVE-2019-2593, CVE-2019-2596, CVE-2019-2606, CVE-2019-2607, CVE-2019-2614, CVE-2019-2617, CVE-2019-2620, CVE-2019-2623, CVE-2019-2624, CVE-2019-2625, CVE-2019-2626, CVE-2019-2627, CVE-2019-2628, CVE-2019-2630, CVE-2019-2631, CVE-2019-2632, CVE-2019-2634, CVE-2019-2635, CVE-2019-2636, CVE-2019-2644, CVE-2019-2681, CVE-2019-2683, CVE-2019-2685, CVE-2019-2686, CVE-2019-2687, CVE-2019-2688, CVE-2019-2689, CVE-2019-2691, CVE-2019-2693, CVE-2019-2694, CVE-2019-2695

Description

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

Observation

Oracle MySQL Server is a popular open source database.

Multiple vulnerabilities are present in some versions of Oracle MySQL Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or have unauthorized access to the target system.

25070 - Wireshark Multiple Vulnerabilities Prior To 3.0.1

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

Risk Level: Medium

CVE: CVE-2019-10894, CVE-2019-10895, CVE-2019-10896, CVE-2019-10897, CVE-2019-10898, CVE-2019-10899, CVE-2019-10900, CVE-2019-10901, CVE-2019-10902, CVE-2019-10903

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

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

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

147874 - SuSE Linux 42.3 openSUSE-SU-2019:1292-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3880

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1292-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00208.html

SuSE Linux 42.3
i586
samba-debugsource-4.6.16+git.154.2998451b912-27.1
libsamba-hostconfig-devel-4.6.16+git.154.2998451b912-27.1
libtevent-util0-4.6.16+git.154.2998451b912-27.1
libndr0-4.6.16+git.154.2998451b912-27.1
libdcerpc-binding0-4.6.16+git.154.2998451b912-27.1
libsmbconf0-4.6.16+git.154.2998451b912-27.1
libwbclient0-debuginfo-4.6.16+git.154.2998451b912-27.1
ctdb-tests-debuginfo-4.6.16+git.154.2998451b912-27.1
libsmbldap0-4.6.16+git.154.2998451b912-27.1
libndr-krb5pac-devel-4.6.16+git.154.2998451b912-27.1
samba-winbind-4.6.16+git.154.2998451b912-27.1
libndr-standard0-debuginfo-4.6.16+git.154.2998451b912-27.1
libdcerpc-samr-devel-4.6.16+git.154.2998451b912-27.1

libsamba-passdb0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-credentials0-4.6.16+git.154.2998451b912-27.1
libndr-devel-4.6.16+git.154.2998451b912-27.1
samba-test-debuginfo-4.6.16+git.154.2998451b912-27.1
samba-python-4.6.16+git.154.2998451b912-27.1
samba-pidl-4.6.16+git.154.2998451b912-27.1
samba-debuginfo-4.6.16+git.154.2998451b912-27.1
libsmbconf-devel-4.6.16+git.154.2998451b912-27.1
ctdb-tests-4.6.16+git.154.2998451b912-27.1
libndr-nbt-devel-4.6.16+git.154.2998451b912-27.1
libnetapi-devel-4.6.16+git.154.2998451b912-27.1
libsamba-passdb-devel-4.6.16+git.154.2998451b912-27.1
samba-libs-debuginfo-4.6.16+git.154.2998451b912-27.1
libwbclient0-4.6.16+git.154.2998451b912-27.1
libndr-standard-devel-4.6.16+git.154.2998451b912-27.1
libsmbclient-devel-4.6.16+git.154.2998451b912-27.1
libtevent-util-devel-4.6.16+git.154.2998451b912-27.1
libsamba-passdb0-4.6.16+git.154.2998451b912-27.1
ctdb-4.6.16+git.154.2998451b912-27.1
libsamba-errors-devel-4.6.16+git.154.2998451b912-27.1
samba-4.6.16+git.154.2998451b912-27.1
libsamba-util0-debuginfo-4.6.16+git.154.2998451b912-27.1
libdcerpc-samr0-4.6.16+git.154.2998451b912-27.1
samba-winbind-debuginfo-4.6.16+git.154.2998451b912-27.1
samba-client-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-util0-4.6.16+git.154.2998451b912-27.1
libsamba-hostconfig0-debuginfo-4.6.16+git.154.2998451b912-27.1
libndr-krb5pac0-4.6.16+git.154.2998451b912-27.1
libndr-nbt0-4.6.16+git.154.2998451b912-27.1
samba-client-4.6.16+git.154.2998451b912-27.1
libtevent-util0-debuginfo-4.6.16+git.154.2998451b912-27.1
libdcerpc-devel-4.6.16+git.154.2998451b912-27.1
libsmbclient0-4.6.16+git.154.2998451b912-27.1
samba-test-4.6.16+git.154.2998451b912-27.1
libsamba-policy0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-credentials-devel-4.6.16+git.154.2998451b912-27.1
libdcerpc0-4.6.16+git.154.2998451b912-27.1
libndr-krb5pac0-debuginfo-4.6.16+git.154.2998451b912-27.1
samba-python-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-policy-devel-4.6.16+git.154.2998451b912-27.1
libsmbldap-devel-4.6.16+git.154.2998451b912-27.1
libsamdb0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-util-devel-4.6.16+git.154.2998451b912-27.1
samba-libs-4.6.16+git.154.2998451b912-27.1
libsamba-errors0-debuginfo-4.6.16+git.154.2998451b912-27.1
libdcerpc-binding0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamdb-devel-4.6.16+git.154.2998451b912-27.1
libsamba-credentials0-debuginfo-4.6.16+git.154.2998451b912-27.1
samba-core-devel-4.6.16+git.154.2998451b912-27.1
libsamdb0-4.6.16+git.154.2998451b912-27.1
ctdb-debuginfo-4.6.16+git.154.2998451b912-27.1
libsmbldap0-debuginfo-4.6.16+git.154.2998451b912-27.1
libnetapi0-debuginfo-4.6.16+git.154.2998451b912-27.1
libwbclient-devel-4.6.16+git.154.2998451b912-27.1
libsmbconf0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsmbclient0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-hostconfig0-4.6.16+git.154.2998451b912-27.1
libndr-standard0-4.6.16+git.154.2998451b912-27.1
libsamba-policy0-4.6.16+git.154.2998451b912-27.1
libdcerpc0-debuginfo-4.6.16+git.154.2998451b912-27.1

libndr0-debuginfo-4.6.16+git.154.2998451b912-27.1
libndr-nbt0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-errors0-4.6.16+git.154.2998451b912-27.1
libnetapi0-4.6.16+git.154.2998451b912-27.1
libdcerpc-samr0-debuginfo-4.6.16+git.154.2998451b912-27.1

noarch
samba-doc-4.6.16+git.154.2998451b912-27.1

x86_64
samba-debugsource-4.6.16+git.154.2998451b912-27.1
libsamba-hostconfig-devel-4.6.16+git.154.2998451b912-27.1
libsamba-passdb0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libtevent-util0-4.6.16+git.154.2998451b912-27.1
libndr0-4.6.16+git.154.2998451b912-27.1
libdcerpc-binding0-4.6.16+git.154.2998451b912-27.1
libsmbconf0-4.6.16+git.154.2998451b912-27.1
libnetapi0-32bit-4.6.16+git.154.2998451b912-27.1
libwbclient0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-errors0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libtevent-util0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
ctdb-tests-debuginfo-4.6.16+git.154.2998451b912-27.1
libsmbconf0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libsmbldap0-4.6.16+git.154.2998451b912-27.1
libndr-krb5pac-devel-4.6.16+git.154.2998451b912-27.1
libndr-standard0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libndr0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
samba-ceph-debuginfo-4.6.16+git.154.2998451b912-27.1
samba-winbind-4.6.16+git.154.2998451b912-27.1
libsamba-policy0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libdcerpc-samr0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libndr-standard0-debuginfo-4.6.16+git.154.2998451b912-27.1
libdcerpc-samr-devel-4.6.16+git.154.2998451b912-27.1
libsmbclient0-32bit-4.6.16+git.154.2998451b912-27.1
libsamba-passdb0-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-credentials0-4.6.16+git.154.2998451b912-27.1
libndr-devel-4.6.16+git.154.2998451b912-27.1
samba-test-debuginfo-4.6.16+git.154.2998451b912-27.1
samba-python-4.6.16+git.154.2998451b912-27.1
samba-pidl-4.6.16+git.154.2998451b912-27.1
libsmbconf0-32bit-4.6.16+git.154.2998451b912-27.1
samba-debuginfo-4.6.16+git.154.2998451b912-27.1
libsamba-util0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libsmbconf-devel-4.6.16+git.154.2998451b912-27.1
ctdb-tests-4.6.16+git.154.2998451b912-27.1
libndr-nbt-devel-4.6.16+git.154.2998451b912-27.1
libnetapi-devel-4.6.16+git.154.2998451b912-27.1
libsmbldap0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libsamba-passdb-devel-4.6.16+git.154.2998451b912-27.1
samba-libs-debuginfo-4.6.16+git.154.2998451b912-27.1
libwbclient0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libsamba-util0-32bit-4.6.16+git.154.2998451b912-27.1
samba-client-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libdcerpc-binding0-debuginfo-32bit-4.6.16+git.154.2998451b912-27.1
libwbclient0-4.6.16+git.154.2998451b912-27.1
libndr-standard-devel-4.6.16+git.154.2998451b912-27.1
libsmbclient-devel-4.6.16+git.154.2998451b912-27.1
libtevent-util-devel-4.6.16+git.154.2998451b912-27.1
libsamba-passdb0-4.6.16+git.154.2998451b912-27.1
ctdb-4.6.16+git.154.2998451b912-27.1

libsamba-errors-devel-4.6.16+git.154.2998451b912-27.1
samba-4.6.16+git.154.2998451b912-27.1
libsamba-policy0-32bit-4.6.16+git.154.2998451b912-27.1
libsamba-util0-debuginfo-4.6.16+git.154.2998451b912-27.1

147878 - SuSE Linux 42.3 openSUSE-SU-2019:1276-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9628

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1276-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00190.html

SuSE Linux 42.3
x86_64
xmltooling-schemas-1.5.6-12.1
libxmltooling-devel-1.5.6-12.1
xmltooling-debugsource-1.5.6-12.1
libxmltooling6-debuginfo-1.5.6-12.1
libxmltooling6-1.5.6-12.1

147881 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1038-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10894, CVE-2019-10895, CVE-2019-10896, CVE-2019-10899, CVE-2019-10901, CVE-2019-10903

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1038-1

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/005364.html

SuSE SLED 12 SP3
x86_64
wireshark-2.4.14-48.45.1
wireshark-gtk-2.4.14-48.45.1
libwscodecs1-2.4.14-48.45.1
libwsutil8-2.4.14-48.45.1
libwiretap7-2.4.14-48.45.1
libwsutil8-debuginfo-2.4.14-48.45.1
wireshark-debugsource-2.4.14-48.45.1
wireshark-debuginfo-2.4.14-48.45.1
wireshark-gtk-debuginfo-2.4.14-48.45.1

libwscodecs1-debuginfo-2.4.14-48.45.1
libwiretap7-debuginfo-2.4.14-48.45.1
libwireshark9-2.4.14-48.45.1
libwireshark9-debuginfo-2.4.14-48.45.1

SuSE SLED 12 SP4
x86_64
wireshark-2.4.14-48.45.1
wireshark-gtk-2.4.14-48.45.1
libwscodecs1-2.4.14-48.45.1
libwsutil8-2.4.14-48.45.1
libwiretap7-2.4.14-48.45.1
libwsutil8-debuginfo-2.4.14-48.45.1
wireshark-debugsource-2.4.14-48.45.1
wireshark-debuginfo-2.4.14-48.45.1
wireshark-gtk-debuginfo-2.4.14-48.45.1
libwscodecs1-debuginfo-2.4.14-48.45.1
libwiretap7-debuginfo-2.4.14-48.45.1
libwireshark9-2.4.14-48.45.1
libwireshark9-debuginfo-2.4.14-48.45.1

SuSE SLES 12 SP4
x86_64
wireshark-2.4.14-48.45.1
wireshark-gtk-2.4.14-48.45.1
libwscodecs1-2.4.14-48.45.1
libwsutil8-2.4.14-48.45.1
libwiretap7-2.4.14-48.45.1
libwsutil8-debuginfo-2.4.14-48.45.1
wireshark-debugsource-2.4.14-48.45.1
wireshark-debuginfo-2.4.14-48.45.1
wireshark-gtk-debuginfo-2.4.14-48.45.1
libwscodecs1-debuginfo-2.4.14-48.45.1
libwiretap7-debuginfo-2.4.14-48.45.1
libwireshark9-2.4.14-48.45.1
libwireshark9-debuginfo-2.4.14-48.45.1

SuSE SLES 12 SP3
x86_64
wireshark-2.4.14-48.45.1
wireshark-gtk-2.4.14-48.45.1
libwscodecs1-2.4.14-48.45.1
libwsutil8-2.4.14-48.45.1
libwiretap7-2.4.14-48.45.1
libwsutil8-debuginfo-2.4.14-48.45.1
wireshark-debugsource-2.4.14-48.45.1
wireshark-debuginfo-2.4.14-48.45.1
wireshark-gtk-debuginfo-2.4.14-48.45.1
libwscodecs1-debuginfo-2.4.14-48.45.1
libwiretap7-debuginfo-2.4.14-48.45.1
libwireshark9-2.4.14-48.45.1
libwireshark9-debuginfo-2.4.14-48.45.1

147882 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1111-1 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:
SUSE-SU-2019:1111-1

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/005415.html

SuSE SLED 12 SP3
x86_64
libjpeg62-debuginfo-32bit-62.2.0-31.14.2
libjpeg-turbo-1.5.3-31.14.2
libjpeg-turbo-debugsource-1.5.3-31.14.2
libjpeg8-8.1.2-31.14.2
libturbojpeg0-8.1.2-31.14.2
libjpeg62-turbo-debugsource-1.5.3-31.14.2
libjpeg-turbo-debuginfo-1.5.3-31.14.2
libjpeg8-debuginfo-32bit-8.1.2-31.14.2
libjpeg62-62.2.0-31.14.2
libjpeg8-32bit-8.1.2-31.14.2
libjpeg8-debuginfo-8.1.2-31.14.2
libturbojpeg0-debuginfo-8.1.2-31.14.2
libjpeg62-32bit-62.2.0-31.14.2
libjpeg62-debuginfo-62.2.0-31.14.2
libjpeg62-turbo-1.5.3-31.14.2

SuSE SLED 12 SP4
x86_64
libjpeg62-debuginfo-32bit-62.2.0-31.14.2
libjpeg-turbo-1.5.3-31.14.2
libjpeg-turbo-debugsource-1.5.3-31.14.2
libjpeg8-8.1.2-31.14.2
libturbojpeg0-8.1.2-31.14.2
libjpeg62-turbo-debugsource-1.5.3-31.14.2
libjpeg-turbo-debuginfo-1.5.3-31.14.2
libjpeg8-debuginfo-32bit-8.1.2-31.14.2
libjpeg62-62.2.0-31.14.2
libjpeg8-32bit-8.1.2-31.14.2
libjpeg8-debuginfo-8.1.2-31.14.2
libturbojpeg0-debuginfo-8.1.2-31.14.2
libjpeg62-32bit-62.2.0-31.14.2
libjpeg62-debuginfo-62.2.0-31.14.2
libjpeg62-turbo-1.5.3-31.14.2

SuSE SLES 12 SP4
x86_64
libjpeg62-debuginfo-32bit-62.2.0-31.14.2
libjpeg8-8.1.2-31.14.2
libjpeg-turbo-1.5.3-31.14.2
libjpeg-turbo-debugsource-1.5.3-31.14.2
libturbojpeg0-8.1.2-31.14.2
libjpeg62-turbo-debugsource-1.5.3-31.14.2
libjpeg-turbo-debuginfo-1.5.3-31.14.2
libjpeg8-debuginfo-32bit-8.1.2-31.14.2
libjpeg62-62.2.0-31.14.2
libjpeg8-32bit-8.1.2-31.14.2
libjpeg8-debuginfo-8.1.2-31.14.2

libturbojpeg0-debuginfo-8.1.2-31.14.2
libjpeg62-32bit-62.2.0-31.14.2
libjpeg62-debuginfo-62.2.0-31.14.2
libjpeg62-turbo-1.5.3-31.14.2

SuSE SLES 12 SP3
x86_64
libjpeg62-debuginfo-32bit-62.2.0-31.14.2
libjpeg8-8.1.2-31.14.2
libjpeg-turbo-1.5.3-31.14.2
libjpeg-turbo-debugsource-1.5.3-31.14.2
libturbojpeg0-8.1.2-31.14.2
libjpeg62-turbo-debugsource-1.5.3-31.14.2
libjpeg-turbo-debuginfo-1.5.3-31.14.2
libjpeg8-debuginfo-32bit-8.1.2-31.14.2
libjpeg62-62.2.0-31.14.2
libjpeg8-32bit-8.1.2-31.14.2
libjpeg8-debuginfo-8.1.2-31.14.2
libturbojpeg0-debuginfo-8.1.2-31.14.2
libjpeg62-32bit-62.2.0-31.14.2
libjpeg62-debuginfo-62.2.0-31.14.2
libjpeg62-turbo-1.5.3-31.14.2

147886 - SuSE Linux 15.0 openSUSE-SU-2019:1282-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1282-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00194.html

SuSE Linux 15.0
x86_64
python3-3.6.5-lp150.2.10.1
python3-curses-3.6.5-lp150.2.10.1
python3-tk-3.6.5-lp150.2.10.1
python3-debuginfo-3.6.5-lp150.2.10.1
python3-32bit-debuginfo-3.6.5-lp150.2.10.1
python3-32bit-3.6.5-lp150.2.10.1
python3-debugsource-3.6.5-lp150.2.10.1
python3-dbm-debuginfo-3.6.5-lp150.2.10.1
python3-curses-debuginfo-3.6.5-lp150.2.10.1
python3-dbm-3.6.5-lp150.2.10.1
python3-tk-debuginfo-3.6.5-lp150.2.10.1

i586
python3-3.6.5-lp150.2.10.1
python3-curses-3.6.5-lp150.2.10.1
python3-tk-3.6.5-lp150.2.10.1
python3-debuginfo-3.6.5-lp150.2.10.1

python3-debugsource-3.6.5-lp150.2.10.1
python3-dbm-debuginfo-3.6.5-lp150.2.10.1
python3-curses-debuginfo-3.6.5-lp150.2.10.1
python3-dbm-3.6.5-lp150.2.10.1
python3-tk-debuginfo-3.6.5-lp150.2.10.1

147894 - SuSE Linux 15.0 openSUSE-SU-2019:1284-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10861, CVE-2018-1128, CVE-2018-1129, CVE-2018-14662, CVE-2018-16846

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1284-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00198.html

SuSE Linux 15.0
x86_64
rbd-nbd-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
librados-devel-13.2.4.125+gad802694f5-lp150.2.3.1
python3-rgw-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-base-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-mds-13.2.4.125+gad802694f5-lp150.2.3.1
python3-rados-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
libradosstriper1-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-debugsource-13.2.4.125+gad802694f5-lp150.2.3.1
python3-rados-13.2.4.125+gad802694f5-lp150.2.3.1
python3-cephfs-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-fuse-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
librbd1-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-mon-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-base-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-test-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-mgr-13.2.4.125+gad802694f5-lp150.2.3.1
rbd-mirror-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
librgw2-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
librgw-devel-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-mds-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
rbd-mirror-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-radosgw-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
librgw2-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-resource-agents-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-common-13.2.4.125+gad802694f5-lp150.2.3.1
librados-devel-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
python3-rbd-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
rbd-nbd-13.2.4.125+gad802694f5-lp150.2.3.1
libcephfs2-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
librbd-devel-13.2.4.125+gad802694f5-lp150.2.3.1
rados-objclass-devel-13.2.4.125+gad802694f5-lp150.2.3.1
python3-rgw-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-mon-13.2.4.125+gad802694f5-lp150.2.3.1

ceph-fuse-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-test-13.2.4.125+gad802694f5-lp150.2.3.1
libcephfs2-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-osd-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-radosgw-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-mgr-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
librados2-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-test-debugsource-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-common-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
librados2-13.2.4.125+gad802694f5-lp150.2.3.1
rbd-fuse-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
python3-rbd-13.2.4.125+gad802694f5-lp150.2.3.1
libradosstriper-devel-13.2.4.125+gad802694f5-lp150.2.3.1
libcephfs-devel-13.2.4.125+gad802694f5-lp150.2.3.1
librbd1-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1
libradosstriper1-13.2.4.125+gad802694f5-lp150.2.3.1
ceph-osd-13.2.4.125+gad802694f5-lp150.2.3.1
rbd-fuse-13.2.4.125+gad802694f5-lp150.2.3.1
python3-cephfs-debuginfo-13.2.4.125+gad802694f5-lp150.2.3.1

147895 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1037-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3880

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1037-1

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/005365.html

SuSE SLED 12 SP3
x86_64
libsamba-errors0-4.6.16+git.154.2998451b912-3.40.3
libnetapi0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-errors0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libndr0-4.6.16+git.154.2998451b912-3.40.3
libsmbclient0-4.6.16+git.154.2998451b912-3.40.3
libnetapi0-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-krb5pac0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libdcerpc-binding0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libwbclient0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbldap0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-credentials0-4.6.16+git.154.2998451b912-3.40.3
libndr0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libndr-nbt0-32bit-4.6.16+git.154.2998451b912-3.40.3
samba-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-passdb0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbldap0-4.6.16+git.154.2998451b912-3.40.3
libwbclient0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsmbconf0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbldap0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libwbclient0-4.6.16+git.154.2998451b912-3.40.3

samba-libs-4.6.16+git.154.2998451b912-3.40.3
samba-debugsource-4.6.16+git.154.2998451b912-3.40.3
libtevent-util0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-credentials0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-hostconfig0-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-standard0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-nbt0-4.6.16+git.154.2998451b912-3.40.3
libsamdb0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-standard0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-errors0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamdb0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libndr-krb5pac0-4.6.16+git.154.2998451b912-3.40.3
libdcerpc-binding0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-passdb0-32bit-4.6.16+git.154.2998451b912-3.40.3
libwbclient0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbconf0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-credentials0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libnetapi0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-util0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-util0-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr0-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-nbt0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamdb0-4.6.16+git.154.2998451b912-3.40.3
libndr-krb5pac0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
samba-winbind-32bit-4.6.16+git.154.2998451b912-3.40.3
samba-winbind-4.6.16+git.154.2998451b912-3.40.3
libsmbclient0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-errors0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-hostconfig0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
samba-libs-32bit-4.6.16+git.154.2998451b912-3.40.3
samba-client-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libdcerpc0-32bit-4.6.16+git.154.2998451b912-3.40.3
samba-winbind-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-standard0-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-krb5pac0-32bit-4.6.16+git.154.2998451b912-3.40.3
libtevent-util0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libtevent-util0-4.6.16+git.154.2998451b912-3.40.3
samba-4.6.16+git.154.2998451b912-3.40.3
libndr0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libdcerpc-binding0-4.6.16+git.154.2998451b912-3.40.3
libsmbconf0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-nbt0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
samba-client-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-standard0-4.6.16+git.154.2998451b912-3.40.3
libsamba-hostconfig0-4.6.16+git.154.2998451b912-3.40.3
samba-winbind-debuginfo-4.6.16+git.154.2998451b912-3.40.3
samba-client-4.6.16+git.154.2998451b912-3.40.3
samba-libs-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-util0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libtevent-util0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-credentials0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-passdb0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-hostconfig0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-passdb0-4.6.16+git.154.2998451b912-3.40.3
libsmbldap0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libnetapi0-4.6.16+git.154.2998451b912-3.40.3
libsamdb0-32bit-4.6.16+git.154.2998451b912-3.40.3
libdcerpc-binding0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbclient0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbclient0-debuginfo-4.6.16+git.154.2998451b912-3.40.3

samba-client-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-util0-4.6.16+git.154.2998451b912-3.40.3
libdcerpc0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbconf0-4.6.16+git.154.2998451b912-3.40.3
libdcerpc0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
samba-libs-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libdcerpc0-4.6.16+git.154.2998451b912-3.40.3

noarch
samba-doc-4.6.16+git.154.2998451b912-3.40.3

SuSE SLED 12 SP4
x86_64
libsamba-errors0-4.6.16+git.154.2998451b912-3.40.3
libnetapi0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-errors0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libndr0-4.6.16+git.154.2998451b912-3.40.3
libsmbclient0-4.6.16+git.154.2998451b912-3.40.3
libnetapi0-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-krb5pac0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libdcerpc-binding0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libwbclient0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbldap0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-credentials0-4.6.16+git.154.2998451b912-3.40.3
libndr0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libndr-nbt0-32bit-4.6.16+git.154.2998451b912-3.40.3
samba-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-passdb0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbldap0-4.6.16+git.154.2998451b912-3.40.3
libwbclient0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsmbconf0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsmbldap0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libwbclient0-4.6.16+git.154.2998451b912-3.40.3
samba-libs-4.6.16+git.154.2998451b912-3.40.3
samba-debugsource-4.6.16+git.154.2998451b912-3.40.3
libtevent-util0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-credentials0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-hostconfig0-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-standard0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-nbt0-4.6.16+git.154.2998451b912-3.40.3
libsamdb0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libndr-standard0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libsamba-errors0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamdb0-debuginfo-4.6.16+git.154.2998451b912-3.40.3
libndr-krb5pac0-4.6.16+git.154.2998451b912-3.40.3
libdcerpc-binding0-32bit-4.6.16+git.154.2998451b912-3.40.3
libsamba-passdb0-32bit-4.6.16+git.154.2998451b912-3.40.3
libwbclient0-debuginfo-32bit-4.6.16+git.154.2998451b912-3.40.3

SuSE SLES 12 SP4
noarch
samba-doc-4.6.16+git.154.2998451b912-3.40.3

SuSE SLES 12 SP3
noarch
samba-doc-4.6.16+git.154.2998451b912-3.40.3

160554 - CentOS 7 CESA-2019-0638 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3816

Description

The scan detected that the host is missing the following update:
CESA-2019-0638

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/023295.html

CentOS 7
x86_64
libwsman-devel-2.6.3-6.git4391e5c.el7_6
openwsman-python-2.6.3-6.git4391e5c.el7_6
openwsman-perl-2.6.3-6.git4391e5c.el7_6
openwsman-client-2.6.3-6.git4391e5c.el7_6
libwsman1-2.6.3-6.git4391e5c.el7_6
openwsman-ruby-2.6.3-6.git4391e5c.el7_6
openwsman-server-2.6.3-6.git4391e5c.el7_6

i686
openwsman-server-2.6.3-6.git4391e5c.el7_6
openwsman-client-2.6.3-6.git4391e5c.el7_6
libwsman-devel-2.6.3-6.git4391e5c.el7_6
libwsman1-2.6.3-6.git4391e5c.el7_6

178744 - Gentoo Linux GLSA-201904-24 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-201904-24

Observation

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

https://security.gentoo.org/glsa/201904-24

Affected packages:
media-libs/ming < 0.20181112

178745 - Gentoo Linux GLSA-201904-25 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-201904-25

Observation

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

https://security.gentoo.org/glsa/201904-25

Affected packages:
app-emulation/qemu < 3.1.0-r4

182970 - FreeBSD buildbot CRLF Injection In Buildbot Login And Logout Redirect Code (5536ea5f-6814-11e9-a8f7-0050562a4d7b)

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

Risk Level: Medium

CVE: CVE-2019-7313

Description

The scan detected that the host is missing the following update:
buildbot -- CRLF injection in Buildbot login and logout redirect code (5536ea5f-6814-11e9-a8f7-0050562a4d7b)

Observation

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

http://www.vuxml.org/freebsd/5536ea5f-6814-11e9-a8f7-0050562a4d7b.html

Affected packages:
py27-buildbot < 1.8.0
py35-buildbot < 1.8.0
py36-buildbot < 1.8.0
py37-buildbot < 1.8.0

186677 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3957-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2566, CVE-2019-2581, CVE-2019-2592, CVE-2019-2614, CVE-2019-2627, CVE-2019-2628, CVE-2019-2632, CVE-2019-2683

Description

The scan detected that the host is missing the following update:
USN-3957-1

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/004867.html

Ubuntu 16.04

mysql-server-5.7_5.7.26-0ubuntu0.16.04.1

Ubuntu 18.10

mysql-server-5.7_5.7.26-0ubuntu0.18.10.1

Ubuntu 19.04

mysql-server-5.7_5.7.26-0ubuntu0.19.04.1

Ubuntu 18.04

mysql-server-5.7_5.7.26-0ubuntu0.18.04.1

195086 - Fedora Linux 28 FEDORA-2019-432b3dff25 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6251

Description

The scan detected that the host is missing the following update:
FEDORA-2019-432b3dff25

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=4

Fedora Core 28

webkit2gtk3-2.24.1-1.fc28

195089 - Fedora Linux 28 FEDORA-2019-3ee6a7adf2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14773, CVE-2018-14774

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3ee6a7adf2

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

php-symfony-2.8.51-1.fc28

195098 - Fedora Linux 28 FEDORA-2019-2a7f472198 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14773, CVE-2018-14774

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2a7f472198

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

php-symfony3-3.4.26-1.fc28

195103 - Fedora Linux 29 FEDORA-2019-04a42e480b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10906

Description

The scan detected that the host is missing the following update:
FEDORA-2019-04a42e480b

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 29

python-jinja2-2.10.1-1.fc29

195106 - Fedora Linux 29 FEDORA-2019-74f7603660 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6251

Description

The scan detected that the host is missing the following update:
FEDORA-2019-74f7603660

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

wpewebkit-2.24.1-1.fc29

195107 - Fedora Linux 30 FEDORA-2019-e41e19457b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10906

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e41e19457b

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=3

Fedora Core 30

python-jinja2-2.10.1-1.fc30

195108 - Fedora Linux 28 FEDORA-2019-4f978cacb4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10906

Description

The scan detected that the host is missing the following update:
FEDORA-2019-4f978cacb4

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

python-jinja2-2.10.1-1.fc28

195110 - Fedora Linux 28 FEDORA-2019-8560719e80 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20060

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8560719e80

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

python-urllib3-1.24.2-1.fc28

195113 - Fedora Linux 30 FEDORA-2019-6afaa38e7b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20060

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6afaa38e7b

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

python-urllib3-1.24.2-1.fc30

195114 - Fedora Linux 30 FEDORA-2019-77433fc7f3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6251

Description

The scan detected that the host is missing the following update:
FEDORA-2019-77433fc7f3

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

wpewebkit-2.24.1-1.fc30

196303 - Red Hat Enterprise Linux RHSA-2019-0902 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9636

Description

The scan detected that the host is missing the following update:
RHSA-2019-0902

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/msg00034.html

RHEL6S
x86_64
rh-python35-python-libs-3.5.1-12.el6
rh-python35-python-debuginfo-3.5.1-12.el6
rh-python35-python-debug-3.5.1-12.el6
rh-python35-python-tools-3.5.1-12.el6
rh-python35-python-3.5.1-12.el6
rh-python35-python-devel-3.5.1-12.el6
rh-python35-python-tkinter-3.5.1-12.el6
rh-python35-python-test-3.5.1-12.el6

RHEL6WS
x86_64
rh-python35-python-libs-3.5.1-12.el6
rh-python35-python-debuginfo-3.5.1-12.el6
rh-python35-python-debug-3.5.1-12.el6
rh-python35-python-tools-3.5.1-12.el6
rh-python35-python-3.5.1-12.el6
rh-python35-python-devel-3.5.1-12.el6
rh-python35-python-tkinter-3.5.1-12.el6
rh-python35-python-test-3.5.1-12.el6

RHEL7S
x86_64
rh-python35-python-test-3.5.1-12.el7
rh-python35-python-debuginfo-3.5.1-12.el7
rh-python35-python-3.5.1-12.el7
rh-python35-python-debug-3.5.1-12.el7
rh-python35-python-tools-3.5.1-12.el7
rh-python35-python-tkinter-3.5.1-12.el7
rh-python35-python-devel-3.5.1-12.el7
rh-python35-python-libs-3.5.1-12.el7

RHEL7WS
x86_64
rh-python35-python-test-3.5.1-12.el7
rh-python35-python-debuginfo-3.5.1-12.el7
rh-python35-python-3.5.1-12.el7
rh-python35-python-debug-3.5.1-12.el7
rh-python35-python-tools-3.5.1-12.el7
rh-python35-python-tkinter-3.5.1-12.el7
rh-python35-python-devel-3.5.1-12.el7
rh-python35-python-libs-3.5.1-12.el7

25067 - Oracle VM VirtualBox Critical Patch Update April 2019

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2019-2574, CVE-2019-2656, CVE-2019-2657, CVE-2019-2678, CVE-2019-2679, CVE-2019-2680, CVE-2019-2690, CVE-2019-2696, CVE-2019-2703, CVE-2019-2721, CVE-2019-2722, CVE-2019-2723

Description

Multiple vulnerabilities are present in some versions of Oracle VM VirtualBox.

Observation

Oracle VM VirtualBox is a virtualization software.

Multiple vulnerabilities are present in some versions of Oracle VM VirtualBox. The flaws exist in core component. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or do unauthorized modifications on the target system.

25073 - IBM AIX OpenSSL Vulnerability (openssl_advisory30)

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

Risk Level: Medium

CVE: CVE-2019-1559

Description

A vulnerability is present in some versions of OpenSSL used by IBM AIX.

Observation

AIX is a Unix-like operating system developed by IBM.

A vulnerability is present in some versions of OpenSSL used by IBM AIX. The flaw is due to improper handling of a zero-length record with valid padding. Successful exploitation could allow an attacker to obtain sensitive information.

147880 - SuSE Linux 42.3 openSUSE-SU-2019:1294-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3840, CVE-2019-3886

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1294-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00207.html

SuSE Linux 42.3
x86_64
libvirt-daemon-driver-storage-scsi-3.3.0-24.1
libvirt-daemon-driver-libxl-3.3.0-24.1
libvirt-libs-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-logical-3.3.0-24.1
libvirt-client-debuginfo-32bit-3.3.0-24.1
libvirt-nss-3.3.0-24.1

libvirt-daemon-driver-storage-core-3.3.0-24.1
libvirt-daemon-driver-storage-3.3.0-24.1
libvirt-client-debuginfo-3.3.0-24.1
libvirt-daemon-hooks-3.3.0-24.1
libvirt-daemon-driver-interface-3.3.0-24.1
libvirt-devel-3.3.0-24.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-iscsi-3.3.0-24.1
libvirt-daemon-driver-qemu-3.3.0-24.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-mpath-3.3.0-24.1
libvirt-daemon-driver-lxc-3.3.0-24.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-24.1
libvirt-daemon-3.3.0-24.1
libvirt-daemon-xen-3.3.0-24.1
libvirt-admin-debuginfo-3.3.0-24.1
libvirt-nss-debuginfo-3.3.0-24.1
libvirt-debugsource-3.3.0-24.1
libvirt-daemon-driver-uml-3.3.0-24.1
libvirt-daemon-driver-nwfilter-3.3.0-24.1
libvirt-daemon-driver-network-debuginfo-3.3.0-24.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-24.1
libvirt-daemon-lxc-3.3.0-24.1
libvirt-daemon-driver-vbox-3.3.0-24.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-24.1
libvirt-doc-3.3.0-24.1
libvirt-daemon-driver-secret-3.3.0-24.1
libvirt-lock-sanlock-debuginfo-3.3.0-24.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-disk-3.3.0-24.1
libvirt-admin-3.3.0-24.1
libvirt-daemon-driver-network-3.3.0-24.1
libvirt-daemon-uml-3.3.0-24.1
libvirt-daemon-driver-vbox-debuginfo-3.3.0-24.1
libvirt-3.3.0-24.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-24.1
libvirt-daemon-qemu-3.3.0-24.1
libvirt-lock-sanlock-3.3.0-24.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-24.1
libvirt-daemon-config-nwfilter-3.3.0-24.1
libvirt-daemon-config-network-3.3.0-24.1
libvirt-daemon-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-24.1
libvirt-daemon-driver-uml-debuginfo-3.3.0-24.1
libvirt-daemon-driver-nodedev-3.3.0-24.1
libvirt-libs-3.3.0-24.1
libvirt-daemon-vbox-3.3.0-24.1
libvirt-devel-32bit-3.3.0-24.1
libvirt-client-3.3.0-24.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-24.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-rbd-3.3.0-24.1

i586
libvirt-daemon-driver-storage-scsi-3.3.0-24.1
libvirt-libs-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-logical-3.3.0-24.1

libvirt-nss-3.3.0-24.1
libvirt-daemon-driver-storage-core-3.3.0-24.1
libvirt-daemon-driver-storage-3.3.0-24.1
libvirt-client-debuginfo-3.3.0-24.1
libvirt-daemon-hooks-3.3.0-24.1
libvirt-daemon-driver-interface-3.3.0-24.1
libvirt-devel-3.3.0-24.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-iscsi-3.3.0-24.1
libvirt-daemon-driver-qemu-3.3.0-24.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-mpath-3.3.0-24.1
libvirt-daemon-driver-lxc-3.3.0-24.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-24.1
libvirt-daemon-3.3.0-24.1
libvirt-admin-debuginfo-3.3.0-24.1
libvirt-nss-debuginfo-3.3.0-24.1
libvirt-debugsource-3.3.0-24.1
libvirt-daemon-driver-uml-3.3.0-24.1
libvirt-daemon-driver-nwfilter-3.3.0-24.1
libvirt-daemon-driver-network-debuginfo-3.3.0-24.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-24.1
libvirt-daemon-lxc-3.3.0-24.1
libvirt-daemon-driver-vbox-3.3.0-24.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-24.1
libvirt-doc-3.3.0-24.1
libvirt-daemon-driver-secret-3.3.0-24.1
libvirt-lock-sanlock-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-disk-3.3.0-24.1
libvirt-admin-3.3.0-24.1
libvirt-daemon-driver-network-3.3.0-24.1
libvirt-daemon-uml-3.3.0-24.1
libvirt-daemon-driver-vbox-debuginfo-3.3.0-24.1
libvirt-3.3.0-24.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-24.1
libvirt-daemon-qemu-3.3.0-24.1
libvirt-lock-sanlock-3.3.0-24.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-24.1
libvirt-daemon-config-nwfilter-3.3.0-24.1
libvirt-daemon-config-network-3.3.0-24.1
libvirt-daemon-debuginfo-3.3.0-24.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-24.1
libvirt-daemon-driver-uml-debuginfo-3.3.0-24.1
libvirt-daemon-driver-nodedev-3.3.0-24.1
libvirt-libs-3.3.0-24.1
libvirt-daemon-vbox-3.3.0-24.1
libvirt-client-3.3.0-24.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-24.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-24.1

147893 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:1042-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3840, CVE-2019-3886

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1042-1

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/005368.html

SuSE SLED 12 SP3
x86_64
libvirt-daemon-driver-nodedev-3.3.0-5.30.1
libvirt-daemon-config-nwfilter-3.3.0-5.30.1
libvirt-client-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-logical-3.3.0-5.30.1
libvirt-daemon-driver-nwfilter-3.3.0-5.30.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-5.30.1
libvirt-admin-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-network-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-qemu-3.3.0-5.30.1
libvirt-daemon-3.3.0-5.30.1
libvirt-daemon-driver-lxc-3.3.0-5.30.1
libvirt-daemon-lxc-3.3.0-5.30.1
libvirt-daemon-config-network-3.3.0-5.30.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-mpath-3.3.0-5.30.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-interface-3.3.0-5.30.1
libvirt-libs-3.3.0-5.30.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-5.30.1
libvirt-debugsource-3.3.0-5.30.1
libvirt-daemon-driver-storage-3.3.0-5.30.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-scsi-3.3.0-5.30.1
libvirt-daemon-driver-secret-3.3.0-5.30.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-network-3.3.0-5.30.1
libvirt-libs-debuginfo-3.3.0-5.30.1
libvirt-client-3.3.0-5.30.1
libvirt-daemon-driver-storage-disk-3.3.0-5.30.1
libvirt-daemon-xen-3.3.0-5.30.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-core-3.3.0-5.30.1
libvirt-daemon-driver-storage-rbd-3.3.0-5.30.1
libvirt-daemon-debuginfo-3.3.0-5.30.1
libvirt-daemon-qemu-3.3.0-5.30.1
libvirt-admin-3.3.0-5.30.1
libvirt-daemon-driver-libxl-3.3.0-5.30.1
libvirt-daemon-driver-storage-iscsi-3.3.0-5.30.1
libvirt-3.3.0-5.30.1
libvirt-doc-3.3.0-5.30.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-5.30.1

SuSE SLES 12 SP3

x86_64
libvirt-daemon-driver-nodedev-3.3.0-5.30.1
libvirt-daemon-config-nwfilter-3.3.0-5.30.1
libvirt-client-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-libxl-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-logical-3.3.0-5.30.1
libvirt-daemon-driver-nwfilter-3.3.0-5.30.1
libvirt-daemon-driver-storage-logical-debuginfo-3.3.0-5.30.1
libvirt-admin-debuginfo-3.3.0-5.30.1
libvirt-lock-sanlock-3.3.0-5.30.1
libvirt-daemon-driver-storage-scsi-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-network-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-qemu-3.3.0-5.30.1
libvirt-daemon-3.3.0-5.30.1
libvirt-daemon-driver-interface-3.3.0-5.30.1
libvirt-nss-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-lxc-3.3.0-5.30.1
libvirt-daemon-lxc-3.3.0-5.30.1
libvirt-daemon-config-network-3.3.0-5.30.1
libvirt-daemon-driver-nwfilter-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-mpath-3.3.0-5.30.1
libvirt-daemon-driver-interface-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-disk-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-mpath-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-nodedev-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-core-3.3.0-5.30.1
libvirt-daemon-driver-secret-debuginfo-3.3.0-5.30.1
libvirt-debugsource-3.3.0-5.30.1
libvirt-daemon-driver-storage-3.3.0-5.30.1
libvirt-daemon-driver-libxl-3.3.0-5.30.1
libvirt-daemon-driver-lxc-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-core-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-scsi-3.3.0-5.30.1
libvirt-daemon-driver-secret-3.3.0-5.30.1
libvirt-daemon-driver-storage-rbd-debuginfo-3.3.0-5.30.1
libvirt-lock-sanlock-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-network-3.3.0-5.30.1
libvirt-libs-debuginfo-3.3.0-5.30.1
libvirt-client-3.3.0-5.30.1
libvirt-nss-3.3.0-5.30.1
libvirt-daemon-driver-storage-disk-3.3.0-5.30.1
libvirt-daemon-xen-3.3.0-5.30.1
libvirt-daemon-driver-storage-iscsi-debuginfo-3.3.0-5.30.1
libvirt-daemon-driver-storage-rbd-3.3.0-5.30.1
libvirt-daemon-debuginfo-3.3.0-5.30.1
libvirt-daemon-hooks-3.3.0-5.30.1
libvirt-admin-3.3.0-5.30.1
libvirt-libs-3.3.0-5.30.1
libvirt-daemon-driver-storage-iscsi-3.3.0-5.30.1
libvirt-3.3.0-5.30.1
libvirt-daemon-qemu-3.3.0-5.30.1
libvirt-doc-3.3.0-5.30.1
libvirt-daemon-driver-qemu-debuginfo-3.3.0-5.30.1

195090 - Fedora Linux 30 FEDORA-2019-e640b27e7e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11372, CVE-2019-11373

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e640b27e7e

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

libmediainfo-18.12-3.fc30

195093 - Fedora Linux 29 FEDORA-2019-95eb49ef49 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11026, CVE-2019-9903

Description

The scan detected that the host is missing the following update:
FEDORA-2019-95eb49ef49

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

poppler-0.67.0-18.fc29

195094 - Fedora Linux 30 FEDORA-2019-1ddce0c095 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11026

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1ddce0c095

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

poppler-0.73.0-9.fc30

89020 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-116-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5743

Description

The scan detected that the host is missing the following update:
SSA:2019-116-01

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.433443

Slackware 14.0
x86_64
bind-9.11.6_P1-x86_64-1

Slackware 14.2
x86_64
bind-9.11.6_P1-x86_64-1

i586
bind-9.11.6_P1-i586-1

Slackware 14.1
x86_64
bind-9.11.6_P1-x86_64-1

147867 - SuSE Linux 15.0 openSUSE-SU-2019:1288-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3840

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1288-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00202.html

SuSE Linux 15.0
x86_64
libvirt-daemon-driver-network-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-scsi-4.0.0-lp150.7.10.4
libvirt-daemon-driver-lxc-4.0.0-lp150.7.10.4
libvirt-client-32bit-debuginfo-4.0.0-lp150.7.10.4
libvirt-devel-32bit-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-mpath-4.0.0-lp150.7.10.4
libvirt-daemon-hooks-4.0.0-lp150.7.10.4

libvirt-daemon-lxc-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-iscsi-4.0.0-lp150.7.10.4
libvirt-daemon-xen-4.0.0-lp150.7.10.4
libvirt-daemon-driver-vbox-4.0.0-lp150.7.10.4
libvirt-client-debuginfo-4.0.0-lp150.7.10.4
libvirt-doc-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-mpath-debuginfo-4.0.0-lp150.7.10.4
libvirt-nss-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-config-network-4.0.0-lp150.7.10.4
libvirt-lock-sanlock-4.0.0-lp150.7.10.4
libvirt-4.0.0-lp150.7.10.4
wireshark-plugin-libvirt-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-logical-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-qemu-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-logical-4.0.0-lp150.7.10.4
libvirt-daemon-driver-libxl-4.0.0-lp150.7.10.4
libvirt-devel-4.0.0-lp150.7.10.4
libvirt-daemon-config-nwfilter-4.0.0-lp150.7.10.4
libvirt-daemon-vbox-4.0.0-lp150.7.10.4
wireshark-plugin-libvirt-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-uml-4.0.0-lp150.7.10.4
libvirt-lock-sanlock-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-interface-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-scsi-debuginfo-4.0.0-lp150.7.10.4
libvirt-client-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-disk-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-4.0.0-lp150.7.10.4
libvirt-daemon-driver-lxc-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-disk-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-nwfilter-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-uml-4.0.0-lp150.7.10.4
libvirt-daemon-driver-interface-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-rbd-debuginfo-4.0.0-lp150.7.10.4
libvirt-libs-4.0.0-lp150.7.10.4
libvirt-daemon-driver-nodedev-debuginfo-4.0.0-lp150.7.10.4
libvirt-admin-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-rbd-4.0.0-lp150.7.10.4
libvirt-daemon-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-iscsi-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-libxl-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-core-4.0.0-lp150.7.10.4
libvirt-daemon-driver-vbox-debuginfo-4.0.0-lp150.7.10.4
libvirt-libs-debuginfo-4.0.0-lp150.7.10.4
libvirt-admin-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-nwfilter-4.0.0-lp150.7.10.4
libvirt-debugsource-4.0.0-lp150.7.10.4
libvirt-daemon-driver-nodedev-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-core-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-uml-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-qemu-4.0.0-lp150.7.10.4
libvirt-daemon-qemu-4.0.0-lp150.7.10.4
libvirt-daemon-driver-network-debuginfo-4.0.0-lp150.7.10.4
libvirt-nss-4.0.0-lp150.7.10.4
libvirt-daemon-driver-secret-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-4.0.0-lp150.7.10.4
libvirt-daemon-driver-secret-4.0.0-lp150.7.10.4

i586
libvirt-daemon-driver-network-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-scsi-4.0.0-lp150.7.10.4

libvirt-daemon-driver-lxc-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-mpath-4.0.0-lp150.7.10.4
libvirt-daemon-hooks-4.0.0-lp150.7.10.4
libvirt-daemon-lxc-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-iscsi-4.0.0-lp150.7.10.4
libvirt-daemon-driver-vbox-4.0.0-lp150.7.10.4
libvirt-client-debuginfo-4.0.0-lp150.7.10.4
libvirt-doc-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-mpath-debuginfo-4.0.0-lp150.7.10.4
libvirt-nss-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-config-network-4.0.0-lp150.7.10.4
libvirt-lock-sanlock-4.0.0-lp150.7.10.4
libvirt-4.0.0-lp150.7.10.4
wireshark-plugin-libvirt-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-logical-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-qemu-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-logical-4.0.0-lp150.7.10.4
libvirt-devel-4.0.0-lp150.7.10.4
libvirt-daemon-config-nwfilter-4.0.0-lp150.7.10.4
libvirt-daemon-vbox-4.0.0-lp150.7.10.4
wireshark-plugin-libvirt-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-uml-4.0.0-lp150.7.10.4
libvirt-lock-sanlock-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-interface-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-scsi-debuginfo-4.0.0-lp150.7.10.4
libvirt-client-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-disk-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-4.0.0-lp150.7.10.4
libvirt-daemon-driver-lxc-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-disk-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-nwfilter-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-uml-4.0.0-lp150.7.10.4
libvirt-daemon-driver-interface-4.0.0-lp150.7.10.4
libvirt-libs-4.0.0-lp150.7.10.4
libvirt-daemon-driver-nodedev-debuginfo-4.0.0-lp150.7.10.4
libvirt-admin-4.0.0-lp150.7.10.4
libvirt-daemon-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-iscsi-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-core-4.0.0-lp150.7.10.4
libvirt-daemon-driver-vbox-debuginfo-4.0.0-lp150.7.10.4
libvirt-libs-debuginfo-4.0.0-lp150.7.10.4
libvirt-admin-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-nwfilter-4.0.0-lp150.7.10.4
libvirt-debugsource-4.0.0-lp150.7.10.4
libvirt-daemon-driver-nodedev-4.0.0-lp150.7.10.4
libvirt-daemon-driver-storage-core-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-uml-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-driver-qemu-4.0.0-lp150.7.10.4
libvirt-daemon-qemu-4.0.0-lp150.7.10.4
libvirt-daemon-driver-network-debuginfo-4.0.0-lp150.7.10.4
libvirt-nss-4.0.0-lp150.7.10.4
libvirt-daemon-driver-secret-debuginfo-4.0.0-lp150.7.10.4
libvirt-daemon-4.0.0-lp150.7.10.4
libvirt-daemon-driver-secret-4.0.0-lp150.7.10.4

147871 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:1088-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-14526

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1088-1

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/005409.html

SuSE SLED 12 SP3
x86_64
wpa_supplicant-2.6-15.10.1
wpa_supplicant-debuginfo-2.6-15.10.1
wpa_supplicant-debugsource-2.6-15.10.1

SuSE SLED 12 SP4
x86_64
wpa_supplicant-2.6-15.10.1
wpa_supplicant-debuginfo-2.6-15.10.1
wpa_supplicant-debugsource-2.6-15.10.1

SuSE SLES 12 SP4
x86_64
wpa_supplicant-2.6-15.10.1
wpa_supplicant-debuginfo-2.6-15.10.1
wpa_supplicant-debugsource-2.6-15.10.1

SuSE SLES 12 SP3
x86_64
wpa_supplicant-2.6-15.10.1
wpa_supplicant-debuginfo-2.6-15.10.1
wpa_supplicant-debugsource-2.6-15.10.1

182967 - FreeBSD drupal Drupal Core - Moderately Critical (2bad8b5d-66fb-11e9-9815-78acc0a3b880)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
drupal -- Drupal core - Moderately critical (2bad8b5d-66fb-11e9-9815-78acc0a3b880)

Observation

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

http://www.vuxml.org/freebsd/2bad8b5d-66fb-11e9-9815-78acc0a3b880.html

Affected packages:
drupal7 < 7.66
drupal8 < 8.6.15

182968 - FreeBSD Gitlab Multiple Vulnerabilities (1138b39e-6abb-11e9-a685-001b217b3468)

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

Risk Level: Low

CVE: CVE-2019-11544, CVE-2019-11545, CVE-2019-11546, CVE-2019-11547, CVE-2019-11548, CVE-2019-11549

Description

The scan detected that the host is missing the following update:
Gitlab -- Multiple vulnerabilities (1138b39e-6abb-11e9-a685-001b217b3468)

Observation

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

http://www.vuxml.org/freebsd/1138b39e-6abb-11e9-a685-001b217b3468.html

Affected packages:
11.10.0 <= gitlab-ce < 11.10.2
11.9.0 <= gitlab-ce < 11.9.10
6.0.0 <= gitlab-ce < 11.8.9

182971 - FreeBSD Dovecot Multiple Vulnerabilities (3f98ccb3-6b8a-11e9-9b5c-a4badb296695)

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

Risk Level: Low

CVE: CVE-2019-11494, CVE-2019-11499

Description

The scan detected that the host is missing the following update:
Dovecot -- Multiple vulnerabilities (3f98ccb3-6b8a-11e9-9b5c-a4badb296695)

Observation

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

http://www.vuxml.org/freebsd/3f98ccb3-6b8a-11e9-9b5c-a4badb296695.html

Affected packages:
2.3.0 <= dovecot < 2.3.6

186673 - Ubuntu Linux 18.10, 19.04 USN-3961-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-11494, CVE-2019-11499

Description

The scan detected that the host is missing the following update:
USN-3961-1

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/004871.html

Ubuntu 19.04

dovecot-core_2.3.4.1-1ubuntu2.2
dovecot-submissiond_2.3.4.1-1ubuntu2.2

Ubuntu 18.10

dovecot-core_2.3.2.1-1ubuntu3.4
dovecot-submissiond_2.3.2.1-1ubuntu3.4

186674 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3956-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5743

Description

The scan detected that the host is missing the following update:
USN-3956-1

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/004866.html

Ubuntu 16.04

bind9_9.10.3.dfsg.P4-8ubuntu1.14

Ubuntu 18.10

bind9_9.11.4+dfsg-3ubuntu5.3

Ubuntu 19.04

bind9_9.11.5.P1+dfsg-1ubuntu2.3

Ubuntu 18.04

bind9_9.11.3+dfsg-1ubuntu1.7

195091 - Fedora Linux 30 FEDORA-2019-f5d6a7ce74 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-f5d6a7ce74

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

php-symfony4-4.2.7-2.fc30

195095 - Fedora Linux 30 FEDORA-2019-e84f6c34da Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-9500

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e84f6c34da

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=4

Fedora Core 30

kernel-headers-5.0.9-300.fc30
kernel-tools-5.0.9-300.fc30
kernel-5.0.9-301.fc30

195097 - Fedora Linux 30 FEDORA-2019-7322053e74 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3843

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7322053e74

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

systemd-241-8.git9ef65cb.fc30

195100 - Fedora Linux 30 FEDORA-2019-67e684044e 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-2019-67e684044e

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

libqb-1.0.5-1.fc30

195102 - Fedora Linux 30 FEDORA-2019-0ef4149687 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-2019-0ef4149687

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

php-symfony-2.8.51-1.fc30

195105 - Fedora Linux 29 FEDORA-2019-f8db687840 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-f8db687840

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

php-symfony-2.8.51-1.fc29

195109 - Fedora Linux 29 FEDORA-2019-a3ca65028c 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-a3ca65028c

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

php-symfony3-3.4.26-1.fc29

195111 - Fedora Linux 29 FEDORA-2019-32067d8b15 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-2019-32067d8b15

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

php-symfony4-4.1.12-1.fc29

195112 - Fedora Linux 30 FEDORA-2019-8635280de5 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-2019-8635280de5

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

php-symfony3-3.4.26-1.fc30

195116 - Fedora Linux 30 FEDORA-2019-7b1733dc68 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-2019-7b1733dc68

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

dbus-broker-20-4.fc30

131338 - Debian Linux 9.0 DSA-4435-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7317

Description

The scan detected that the host is missing the following update:
DSA-4435-1

Observation

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

http://www.debian.org/security/2019/dsa-4435

Debian 9.0
all
libpng-tools_1.6.28-1+deb9u1
libpng16-16_1.6.28-1+deb9u1
libpng-dev_1.6.28-1+deb9u1
libpng16-16-udeb_1.6.28-1+deb9u1

147879 - SuSE Linux 42.3 openSUSE-SU-2019:1274-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20815, CVE-2019-3812, CVE-2019-8934, CVE-2019-9824

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1274-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00189.html

SuSE Linux 42.3
i586
qemu-linux-user-debuginfo-2.9.1-59.1
qemu-linux-user-debugsource-2.9.1-59.1
qemu-linux-user-2.9.1-59.1

noarch
qemu-ipxe-1.0.0+-59.1
qemu-sgabios-8-59.1
qemu-seabios-1.10.2-59.1
qemu-vgabios-1.10.2-59.1

x86_64
qemu-s390-2.9.1-59.1
qemu-tools-debuginfo-2.9.1-59.1
qemu-ppc-debuginfo-2.9.1-59.1
qemu-arm-debuginfo-2.9.1-59.1
qemu-2.9.1-59.1
qemu-arm-2.9.1-59.1
qemu-block-dmg-2.9.1-59.1
qemu-linux-user-2.9.1-59.1
qemu-ksm-2.9.1-59.1
qemu-block-ssh-debuginfo-2.9.1-59.1
qemu-testsuite-2.9.1-59.2
qemu-block-ssh-2.9.1-59.1
qemu-block-iscsi-2.9.1-59.1
qemu-block-dmg-debuginfo-2.9.1-59.1
qemu-block-rbd-debuginfo-2.9.1-59.1
qemu-lang-2.9.1-59.1
qemu-block-rbd-2.9.1-59.1
qemu-tools-2.9.1-59.1
qemu-guest-agent-debuginfo-2.9.1-59.1
qemu-x86-debuginfo-2.9.1-59.1
qemu-extra-debuginfo-2.9.1-59.1
qemu-x86-2.9.1-59.1
qemu-linux-user-debugsource-2.9.1-59.1
qemu-ppc-2.9.1-59.1
qemu-block-curl-debuginfo-2.9.1-59.1
qemu-guest-agent-2.9.1-59.1
qemu-linux-user-debuginfo-2.9.1-59.1
qemu-block-curl-2.9.1-59.1
qemu-block-iscsi-debuginfo-2.9.1-59.1
qemu-extra-2.9.1-59.1
qemu-s390-debuginfo-2.9.1-59.1
qemu-kvm-2.9.1-59.1
qemu-debugsource-2.9.1-59.1

186670 - Ubuntu Linux 18.04, 18.10 USN-3962-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7317

Description

The scan detected that the host is missing the following update:
USN-3962-1

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/004872.html

Ubuntu 18.10

libpng16-16_1.6.34-2ubuntu0.1

Ubuntu 18.04

libpng16-16_1.6.34-1ubuntu0.18.04.2

195088 - Fedora Linux 29 FEDORA-2019-fa61af95b3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3500

Description

The scan detected that the host is missing the following update:
FEDORA-2019-fa61af95b3

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

aria2-1.34.0-4.fc29

195096 - Fedora Linux 28 FEDORA-2019-8b8c774b84 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3500

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8b8c774b84

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

aria2-1.34.0-4.fc28

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.

186571 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3887-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-7304

Update Details

Risk is updated

184834 - Ubuntu Linux 14.04, 14.10, 15.04 USN-2618-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1326

Update Details

Risk is updated

192536 - Fedora Linux 25 FEDORA-2017-4ede204115 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1326

Update Details

Risk is updated

24056 - (K74374841) F5 BIG-IP Linux kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2018-5391

Update Details

Documentation is updated FASLScript is updated

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

Update Details

Risk is updated

50314 - Ubuntu Linux 10.04, 10.10, 11.04 USN-1196-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-3145

Update Details

Risk is updated

81962 - Fedora Linux 16 FEDORA-2011-11871 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-3145

Update Details

Risk is updated

142716 - SuSE SLES 11 SP1, 11 SP2, SLED 11 SP1, 11 SP2 SUSE-SU-2012:0682-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-3145

Update Details

Risk is updated

182936 - FreeBSD mozilla Multiple Vulnerabilities (05da6b56-3e66-4306-9ea3-89fafe939726)

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

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

Update Details

Risk is updated

182965 - FreeBSD Istio Security Vulnerabilities (484d3f5e-653a-11e9-b0e3-1c39475b9f84)

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

Risk Level: High

CVE: CVE-2019-9900, CVE-2019-9901

Update Details

Risk is updated

185024 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2782-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1341

Update Details

Risk is updated

22989 - WECON LeviStudio Multiple Buffer Overflow Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-16737, CVE-2017-16739

Update Details

Recommendation is updated

24931 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 60.6.1

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

Risk Level: Medium

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

Update Details

Risk is updated

24981 - Mozilla Firefox Vulnerabilities Prior To 66.0.1

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

Risk Level: Medium

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

Update Details

Risk is updated

25055 - Oracle Java SE Critical Patch Update April 2019

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

Risk Level: Medium

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2697, CVE-2019-2698, CVE-2019-2699

Update Details

Risk is updated

89012 - Slackware Linux 14.2 SSA:2019-081-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-9810, CVE-2019-9813

Update Details
Risk is updated

131321 - Debian Linux 9.0 DSA-4417-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-9810, CVE-2019-9813

Update Details
Risk is updated

147807 - SuSE Linux 42.3 openSUSE-SU-2019:1152-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-9810, CVE-2019-9813

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-9810, CVE-2019-9813

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-9810, CVE-2019-9813

Update Details
Risk is updated

160549 - CentOS 7 CESA-2019-0791 Update Is Not Installed

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

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details

Risk is updated

160550 - CentOS 6 CESA-2019-0790 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details

Risk is updated

160551 - CentOS 7 CESA-2019-0775 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details

Risk is updated

160552 - CentOS 6 CESA-2019-0774 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details

Risk is updated

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

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

Risk Level: Medium

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

Update Details

Risk is updated

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

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

Risk Level: Medium

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

Update Details

Risk is updated

163846 - Oracle Enterprise Linux ELSA-2019-0775 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details
Risk is updated

163847 - Oracle Enterprise Linux ELSA-2019-0791 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details
Risk is updated

163849 - Oracle Enterprise Linux ELSA-2019-0790 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details
Risk is updated

163851 - Oracle Enterprise Linux ELSA-2019-0774 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details
Risk is updated

182610 - FreeBSD Bugzilla Security Issues (22283b8c-13c5-11e8-a861-20cf30e32f6d)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5123

Update Details
Risk is updated

182842 - FreeBSD Gitlab Multiple Vulnerabilities (d889d32c-ecd9-11e8-9416-001b217b3468)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-18643, CVE-2018-19359

Update Details

Risk is updated

193346 - Fedora Linux 26 FEDORA-2018-b79f325c48 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5123

Update Details
Risk is updated

193358 - Fedora Linux 27 FEDORA-2018-1e0e37e148 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5123

Update Details
Risk is updated

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

Update Details
Risk is updated

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

Update Details
Risk is updated

196296 - Red Hat Enterprise Linux RHSA-2019-0791 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details
Risk is updated

196297 - Red Hat Enterprise Linux RHSA-2019-0775 Update Is Not Installed

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

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details

Risk is updated

196301 - Red Hat Enterprise Linux RHSA-2019-0774 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details

Risk is updated

196302 - Red Hat Enterprise Linux RHSA-2019-0790 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2698

Update Details

Risk is updated

33146 - Oracle Solaris 148104-29 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5107, CVE-2012-0814, CVE-2018-20685

Update Details

CVE is updated

33147 - Oracle Solaris 148105-29 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5107, CVE-2012-0814, CVE-2018-20685

Update Details

CVE is updated

135236 - Oracle Solaris 11.4.8.5.0 Update Is Not Installed (CVE-2019-2704)

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

Risk Level: Medium

CVE: CVE-2019-2704

Update Details

Risk is updated

182959 - FreeBSD dovecot Json Encoder Crash (a64aa22f-61ec-11e9-85b9-a4badb296695)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-10691

Update Details
Risk is updated

186614 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3917-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-7303

Update Details
Risk is updated

186666 - Ubuntu Linux 18.10, 19.04 USN-3951-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-10691

Update Details
Risk is updated

186087 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3552-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5124

Update Details
Risk is updated

182014 - FreeBSD tiff Buffer Overflow (0ab66088-4aa5-11e6-a7bd-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-5314, CVE-2016-5320, CVE-2016-5875

Update Details
CVE is updated

195084 - Fedora Linux 30 FEDORA-2019-ac2a21ff07 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

135237 - Oracle Solaris 11.4.6.4.0 Update Is Not Installed (CVE-2019-2577)

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

Risk Level: Low

CVE: CVE-2019-2577

Update Details

Risk is updated

70086 - oracle.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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