2019-APR-24
FSL version 7.6.108

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

24891 - (VMSA-2019-0001) VMware vSphere Integrated Containers Mishandled File Descriptor Vulnerability

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

Risk Level: High

CVE: CVE-2019-5736

Description

A vulnerability is present in some versions of VMware vSphere Integrated Containers.

Observation

VMware vSphere Integrated Container (VIC) is a platform that helps to deploy and manage containers within virtual machines.

A vulnerability is present in some versions of VMware vSphere Integrated Containers. The flaw is due to file-descriptor mishandling. Successful exploitation could allow an attacker to retrieve sensitive data, execute arbitrary code or cause a denial of service condition on the target system.

25058 - Cisco IOS Software NAT64 Denial Of Service Vulnerability (cisco-sa-20190327-nat64)

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

Risk Level: High

CVE: CVE-2019-1751

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 lies in Network Address Translation 64 (NAT64) functions. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

25019 - WordPress Multiple Vulnerabilities Prior To 5.1.1

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of WordPress.

Observation

WordPress is a popular blog application.

Multiple vulnerabilities are present in some versions of WordPress. The flaws lie in multiple components. Successful exploitation could allow an attacker to lead to a cross-site scripting attacks, obtain sensitive information, or bypass certain security restrictions.

25046 - Joomla Directory Traversal In com_media Vulnerability (20190401)

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

Risk Level: High

CVE: CVE-2019-10945

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 com_media. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

25048 - Apache Tomcat Vulnerability Prior To 8.5.40

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.

25051 - Cisco IOS Software IP Service Level Agreement Denial Of Service Vulnerability (cisco-sa-20190327-ipsla-dos)

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

Risk Level: High

CVE: CVE-2019-1737

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 in processing of IP Service Level Agreement (SLA) packets. Successful exploitation could allow an attacker to cause a denial of service condition in the target system.

25054 - IBM AIX Java Multiple Vulnerabilities (java_jan2019_advisory)

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

Risk Level: High

CVE: CVE-2018-11212, CVE-2018-12547, CVE-2018-12549, CVE-2018-1890, CVE-2019-2422, CVE-2019-2426, CVE-2019-2449

Description

Multiple vulnerabilities are present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lie in Java SDK component. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

25056 - Oracle WebCenter Portal Critical Patch Update April 2019

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

Risk Level: High

CVE: CVE-2016-1000031, CVE-2018-19362

Description

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

Observation

Oracle WebCenter Portal is a web platform that helps organizations in fast and easy creation of intranets, extranets, composite applications and self-service portals.

Multiple vulnerabilities are present in some versions of Oracle WebCenter Portal. The flaws lie in several components. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

25061 - Oracle HTTP Server Critical Patch Update April 2019

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

Risk Level: High

CVE: CVE-2019-3822

Description

A vulnerability is present in some versions of Oracle HTTP Server.

Observation

Oracle HTTP Server is a web server based on the Apache HTTP Server

A vulnerability is present in some versions of Oracle HTTP Server. The flaw lies in the Web Listener component. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

147850 - SuSE Linux 42.3 openSUSE-SU-2019:1226-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19665, CVE-2018-19961, CVE-2018-19962, CVE-2018-19965, CVE-2018-19966, CVE-2018-19967, CVE-2019-6778, CVE-2019-9824

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1226-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00140.html

SuSE Linux 42.3
x86_64
xen-doc-html-4.9.4_02-37.1
xen-libs-debuginfo-32bit-4.9.4_02-37.1
xen-libs-4.9.4_02-37.1
xen-tools-debuginfo-4.9.4_02-37.1
xen-libs-debuginfo-4.9.4_02-37.1
xen-tools-domU-debuginfo-4.9.4_02-37.1
xen-libs-32bit-4.9.4_02-37.1
xen-debugsource-4.9.4_02-37.1
xen-4.9.4_02-37.1
xen-tools-domU-4.9.4_02-37.1
xen-tools-4.9.4_02-37.1
xen-devel-4.9.4_02-37.1

i586
xen-libs-4.9.4_02-37.1
xen-libs-debuginfo-4.9.4_02-37.1
xen-tools-domU-debuginfo-4.9.4_02-37.1
xen-debugsource-4.9.4_02-37.1
xen-tools-domU-4.9.4_02-37.1
xen-devel-4.9.4_02-37.1

147851 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0996-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16839

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0996-1

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/005352.html

SuSE SLED 12 SP3
x86_64
libcurl4-7.37.0-37.37.1
curl-debugsource-7.37.0-37.37.1
libcurl4-32bit-7.37.0-37.37.1
curl-debuginfo-7.37.0-37.37.1
libcurl4-debuginfo-32bit-7.37.0-37.37.1
curl-7.37.0-37.37.1

libcurl4-debuginfo-7.37.0-37.37.1

SuSE SLES 12 SP3
x86_64
libcurl4-7.37.0-37.37.1
curl-debugsource-7.37.0-37.37.1
libcurl4-32bit-7.37.0-37.37.1
curl-debuginfo-7.37.0-37.37.1
libcurl4-debuginfo-32bit-7.37.0-37.37.1
curl-7.37.0-37.37.1
libcurl4-debuginfo-7.37.0-37.37.1

147853 - SuSE Linux 42.3 openSUSE-SU-2019:1220-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3814, CVE-2019-7524

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1220-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00134.html

SuSE Linux 42.3
x86_64
dovecot22-backend-mysql-2.2.31-2.12.1
dovecot22-backend-sqlite-debuginfo-2.2.31-2.12.1
dovecot22-backend-pgsql-debuginfo-2.2.31-2.12.1
dovecot22-backend-mysql-debuginfo-2.2.31-2.12.1
dovecot22-2.2.31-2.12.1
dovecot22-fts-debuginfo-2.2.31-2.12.1
dovecot22-devel-2.2.31-2.12.1
dovecot22-backend-sqlite-2.2.31-2.12.1
dovecot22-fts-solr-debuginfo-2.2.31-2.12.1
dovecot22-debuginfo-2.2.31-2.12.1
dovecot22-fts-2.2.31-2.12.1
dovecot22-fts-lucene-2.2.31-2.12.1
dovecot22-backend-pgsql-2.2.31-2.12.1
dovecot22-debugsource-2.2.31-2.12.1
dovecot22-fts-squat-2.2.31-2.12.1
dovecot22-fts-squat-debuginfo-2.2.31-2.12.1
dovecot22-fts-solr-2.2.31-2.12.1
dovecot22-fts-lucene-debuginfo-2.2.31-2.12.1

i586
dovecot22-backend-mysql-2.2.31-2.12.1
dovecot22-backend-sqlite-debuginfo-2.2.31-2.12.1
dovecot22-backend-pgsql-debuginfo-2.2.31-2.12.1
dovecot22-backend-mysql-debuginfo-2.2.31-2.12.1
dovecot22-2.2.31-2.12.1
dovecot22-fts-debuginfo-2.2.31-2.12.1
dovecot22-devel-2.2.31-2.12.1
dovecot22-backend-sqlite-2.2.31-2.12.1

dovecot22-fts-solr-debuginfo-2.2.31-2.12.1
dovecot22-debuginfo-2.2.31-2.12.1
dovecot22-fts-2.2.31-2.12.1
dovecot22-fts-lucene-2.2.31-2.12.1
dovecot22-backend-pgsql-2.2.31-2.12.1
dovecot22-debugsource-2.2.31-2.12.1
dovecot22-fts-squat-2.2.31-2.12.1
dovecot22-fts-squat-debuginfo-2.2.31-2.12.1
dovecot22-fts-solr-2.2.31-2.12.1
dovecot22-fts-lucene-debuginfo-2.2.31-2.12.1

147857 - SuSE Linux 42.3 openSUSE-SU-2019:1258-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1258-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00172.html

SuSE Linux 42.3
i586
apache2-debugsource-2.4.23-49.1
apache2-utils-2.4.23-49.1
apache2-devel-2.4.23-49.1
apache2-event-2.4.23-49.1
apache2-debuginfo-2.4.23-49.1
apache2-event-debuginfo-2.4.23-49.1
apache2-utils-debuginfo-2.4.23-49.1
apache2-worker-debuginfo-2.4.23-49.1
apache2-prefork-debuginfo-2.4.23-49.1
apache2-example-pages-2.4.23-49.1
apache2-2.4.23-49.1
apache2-worker-2.4.23-49.1
apache2-prefork-2.4.23-49.1

noarch
apache2-doc-2.4.23-49.1

x86_64
apache2-debugsource-2.4.23-49.1
apache2-utils-2.4.23-49.1
apache2-devel-2.4.23-49.1
apache2-event-2.4.23-49.1
apache2-debuginfo-2.4.23-49.1
apache2-event-debuginfo-2.4.23-49.1
apache2-utils-debuginfo-2.4.23-49.1
apache2-worker-debuginfo-2.4.23-49.1
apache2-prefork-debuginfo-2.4.23-49.1
apache2-example-pages-2.4.23-49.1
apache2-2.4.23-49.1

apache2-worker-2.4.23-49.1
apache2-prefork-2.4.23-49.1

147859 - SuSE Linux 42.3 openSUSE-SU-2019:1256-1 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-2019-9641

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1256-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00169.html

SuSE Linux 42.3
i586
php5-gettext-5.5.14-115.1
php5-mcrypt-5.5.14-115.1
php5-gettext-debuginfo-5.5.14-115.1
php5-devel-5.5.14-115.1
php5-bcmath-debuginfo-5.5.14-115.1
php5-curl-debuginfo-5.5.14-115.1
php5-shmop-debuginfo-5.5.14-115.1
php5-intl-5.5.14-115.1
php5-suhosin-debuginfo-5.5.14-115.1
php5-snmp-5.5.14-115.1
php5-xmlrpc-debuginfo-5.5.14-115.1
php5-dom-5.5.14-115.1
php5-phar-5.5.14-115.1
php5-xmlreader-5.5.14-115.1
php5-wddx-5.5.14-115.1
php5-curl-5.5.14-115.1
php5-ctype-5.5.14-115.1
php5-sysvshm-debuginfo-5.5.14-115.1
php5-5.5.14-115.1
php5-zlib-debuginfo-5.5.14-115.1
php5-pgsql-debuginfo-5.5.14-115.1
php5-posix-5.5.14-115.1
php5-bcmath-5.5.14-115.1
php5-zlib-5.5.14-115.1
php5-sysvmsg-5.5.14-115.1
php5-mcrypt-debuginfo-5.5.14-115.1
php5-imap-5.5.14-115.1
php5-readline-5.5.14-115.1
php5-fastcgi-debuginfo-5.5.14-115.1
php5-pcntl-5.5.14-115.1
php5-tidy-5.5.14-115.1
php5-iconv-5.5.14-115.1
php5-sockets-debuginfo-5.5.14-115.1
php5-zip-5.5.14-115.1
php5-gd-debuginfo-5.5.14-115.1
php5-fpm-5.5.14-115.1
php5-snmp-debuginfo-5.5.14-115.1

php5-exif-5.5.14-115.1
php5-suhosin-5.5.14-115.1
php5-enchant-debuginfo-5.5.14-115.1
apache2-mod_php5-5.5.14-115.1
php5-mysql-debuginfo-5.5.14-115.1
php5-odbc-debuginfo-5.5.14-115.1
php5-gmp-5.5.14-115.1
php5-mbstring-5.5.14-115.1
php5-mysql-5.5.14-115.1
php5-gmp-debuginfo-5.5.14-115.1
php5-ldap-5.5.14-115.1
php5-opcache-debuginfo-5.5.14-115.1
php5-gd-5.5.14-115.1
php5-sqlite-debuginfo-5.5.14-115.1
php5-openssl-5.5.14-115.1
php5-ftp-debuginfo-5.5.14-115.1
php5-intl-debuginfo-5.5.14-115.1
php5-xsl-debuginfo-5.5.14-115.1
php5-pgsql-5.5.14-115.1
php5-enchant-5.5.14-115.1
php5-pcntl-debuginfo-5.5.14-115.1
php5-debuginfo-5.5.14-115.1
php5-debugsource-5.5.14-115.1
php5-xsl-5.5.14-115.1
php5-bz2-debuginfo-5.5.14-115.1
php5-dba-5.5.14-115.1
php5-openssl-debuginfo-5.5.14-115.1
php5-xmlreader-debuginfo-5.5.14-115.1
php5-bz2-5.5.14-115.1
php5-mbstring-debuginfo-5.5.14-115.1
php5-imap-debuginfo-5.5.14-115.1
php5-opcache-5.5.14-115.1
php5-soap-debuginfo-5.5.14-115.1
php5-dom-debuginfo-5.5.14-115.1
php5-tidy-debuginfo-5.5.14-115.1
php5-calendar-5.5.14-115.1
php5-fastcgi-5.5.14-115.1
php5-fpm-debuginfo-5.5.14-115.1
php5-tokenizer-debuginfo-5.5.14-115.1
php5-xmlrpc-5.5.14-115.1
php5-firebird-debuginfo-5.5.14-115.1
php5-ftp-5.5.14-115.1
php5-pspell-debuginfo-5.5.14-115.1
php5-xmlwriter-debuginfo-5.5.14-115.1
php5-mssql-5.5.14-115.1
php5-iconv-debuginfo-5.5.14-115.1
php5-sqlite-5.5.14-115.1
php5-fileinfo-debuginfo-5.5.14-115.1
php5-soap-5.5.14-115.1
php5-json-5.5.14-115.1
php5-firebird-5.5.14-115.1
php5-dba-debuginfo-5.5.14-115.1
php5-ldap-debuginfo-5.5.14-115.1
apache2-mod_php5-debuginfo-5.5.14-115.1
php5-phar-debuginfo-5.5.14-115.1
php5-odbc-5.5.14-115.1
php5-mssql-debuginfo-5.5.14-115.1
php5-readline-debuginfo-5.5.14-115.1
php5-exif-debuginfo-5.5.14-115.1
php5-posix-debuginfo-5.5.14-115.1

php5-ctype-debuginfo-5.5.14-115.1
php5-sysvsem-5.5.14-115.1
php5-sysvshm-5.5.14-115.1
php5-tokenizer-5.5.14-115.1
php5-fileinfo-5.5.14-115.1
php5-sockets-5.5.14-115.1
php5-json-debuginfo-5.5.14-115.1
php5-pdo-5.5.14-115.1
php5-wddx-debuginfo-5.5.14-115.1
php5-sysvmsg-debuginfo-5.5.14-115.1
php5-pspell-5.5.14-115.1
php5-sysvsem-debuginfo-5.5.14-115.1
php5-xmlwriter-5.5.14-115.1
php5-shmop-5.5.14-115.1
php5-zip-debuginfo-5.5.14-115.1
php5-pdo-debuginfo-5.5.14-115.1
php5-calendar-debuginfo-5.5.14-115.1

noarch
php5-pear-5.5.14-115.1

x86_64
php5-gettext-5.5.14-115.1
php5-mcrypt-5.5.14-115.1
php5-gettext-debuginfo-5.5.14-115.1
php5-devel-5.5.14-115.1
php5-bcmath-debuginfo-5.5.14-115.1
php5-curl-debuginfo-5.5.14-115.1
php5-shmop-debuginfo-5.5.14-115.1
php5-intl-5.5.14-115.1
php5-suhosin-debuginfo-5.5.14-115.1
php5-snmp-5.5.14-115.1
php5-xmlrpc-debuginfo-5.5.14-115.1
php5-dom-5.5.14-115.1
php5-phar-5.5.14-115.1
php5-xmlreader-5.5.14-115.1
php5-wddx-5.5.14-115.1
php5-curl-5.5.14-115.1
php5-ctype-5.5.14-115.1
php5-sysvshm-debuginfo-5.5.14-115.1
php5-5.5.14-115.1
php5-zlib-debuginfo-5.5.14-115.1
php5-pgsql-debuginfo-5.5.14-115.1
php5-posix-5.5.14-115.1
php5-bcmath-5.5.14-115.1
php5-zlib-5.5.14-115.1
php5-sysvmsg-5.5.14-115.1
php5-mcrypt-debuginfo-5.5.14-115.1
php5-imap-5.5.14-115.1
php5-readline-5.5.14-115.1
php5-fastcgi-debuginfo-5.5.14-115.1
php5-pcntl-5.5.14-115.1
php5-tidy-5.5.14-115.1
php5-iconv-5.5.14-115.1
php5-sockets-debuginfo-5.5.14-115.1
php5-zip-5.5.14-115.1
php5-gd-debuginfo-5.5.14-115.1
php5-fpm-5.5.14-115.1
php5-snmp-debuginfo-5.5.14-115.1
php5-exif-5.5.14-115.1

php5-suhosin-5.5.14-115.1
php5-enchant-debuginfo-5.5.14-115.1
apache2-mod_php5-5.5.14-115.1
php5-mysql-debuginfo-5.5.14-115.1
php5-odbc-debuginfo-5.5.14-115.1
php5-gmp-5.5.14-115.1
php5-mbstring-5.5.14-115.1
php5-mysql-5.5.14-115.1
php5-gmp-debuginfo-5.5.14-115.1
php5-ldap-5.5.14-115.1
php5-opcache-debuginfo-5.5.14-115.1
php5-gd-5.5.14-115.1
php5-sqlite-debuginfo-5.5.14-115.1
php5-openssl-5.5.14-115.1
php5-ftp-debuginfo-5.5.14-115.1
php5-intl-debuginfo-5.5.14-115.1
php5-xsl-debuginfo-5.5.14-115.1
php5-pgsql-5.5.14-115.1
php5-enchant-5.5.14-115.1
php5-pcntl-debuginfo-5.5.14-115.1
php5-debuginfo-5.5.14-115.1
php5-debugsource-5.5.14-115.1
php5-xsl-5.5.14-115.1
php5-bz2-debuginfo-5.5.14-115.1
php5-dba-5.5.14-115.1
php5-openssl-debuginfo-5.5.14-115.1
php5-xmlreader-debuginfo-5.5.14-115.1
php5-bz2-5.5.14-115.1
php5-mbstring-debuginfo-5.5.14-115.1
php5-imap-debuginfo-5.5.14-115.1
php5-opcache-5.5.14-115.1
php5-soap-debuginfo-5.5.14-115.1
php5-dom-debuginfo-5.5.14-115.1
php5-tidy-debuginfo-5.5.14-115.1
php5-calendar-5.5.14-115.1
php5-fastcgi-5.5.14-115.1
php5-fpm-debuginfo-5.5.14-115.1
php5-tokenizer-debuginfo-5.5.14-115.1
php5-xmlrpc-5.5.14-115.1
php5-firebird-debuginfo-5.5.14-115.1
php5-ftp-5.5.14-115.1
php5-pspell-debuginfo-5.5.14-115.1
php5-xmlwriter-debuginfo-5.5.14-115.1
php5-mssql-5.5.14-115.1
php5-iconv-debuginfo-5.5.14-115.1
php5-sqlite-5.5.14-115.1
php5-fileinfo-debuginfo-5.5.14-115.1
php5-soap-5.5.14-115.1
php5-json-5.5.14-115.1
php5-firebird-5.5.14-115.1
php5-dba-debuginfo-5.5.14-115.1
php5-ldap-debuginfo-5.5.14-115.1
apache2-mod_php5-debuginfo-5.5.14-115.1
php5-phar-debuginfo-5.5.14-115.1
php5-odbc-5.5.14-115.1
php5-mssql-debuginfo-5.5.14-115.1
php5-readline-debuginfo-5.5.14-115.1
php5-exif-debuginfo-5.5.14-115.1
php5-posix-debuginfo-5.5.14-115.1
php5-ctype-debuginfo-5.5.14-115.1

php5-sysvsem-5.5.14-115.1
php5-sysvshm-5.5.14-115.1
php5-tokenizer-5.5.14-115.1
php5-fileinfo-5.5.14-115.1
php5-sockets-5.5.14-115.1
php5-json-debuginfo-5.5.14-115.1
php5-pdo-5.5.14-115.1
php5-wddx-debuginfo-5.5.14-115.1
php5-sysvmsg-debuginfo-5.5.14-115.1
php5-pspell-5.5.14-115.1
php5-sysvsem-debuginfo-5.5.14-115.1
php5-xmlwriter-5.5.14-115.1
php5-shmop-5.5.14-115.1
php5-zip-debuginfo-5.5.14-115.1
php5-pdo-debuginfo-5.5.14-115.1
php5-calendar-debuginfo-5.5.14-115.1

147860 - SuSE Linux 15.0 openSUSE-SU-2019:1236-1 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-2019:1236-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00150.html

SuSE Linux 15.0
x86_64
wget-debugsource-1.19.5-lp150.7.1
wget-debuginfo-1.19.5-lp150.7.1
wget-1.19.5-lp150.7.1

i586
wget-debugsource-1.19.5-lp150.7.1
wget-debuginfo-1.19.5-lp150.7.1
wget-1.19.5-lp150.7.1

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

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
CESA-2019-0791

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/023276.html

CentOS 7
x86_64
java-1.7.0-openjdk-headless-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el7_6

noarch
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.el7_6

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

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
CESA-2019-0790

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/023277.html

CentOS 6
i686
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el6_10

noarch
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.el6_10

x86_64
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el6_10

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

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

Risk Level: High

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

Description

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

CESA-2019-0775

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/023274.html

CentOS 7
i686
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el7_6

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-zip-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el7_6

x86_64
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el7_6

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

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
CESA-2019-0774

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/023275.html

CentOS 6
i686
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el6_10

x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10

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

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2019-0775

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/008654.html
http://oss.oracle.com/pipermail/el-errata/2019-April/008659.html

OEL7
x86_64
java-1.8.0-openjdk-javadoc-zip-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el7_6

java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el7_6

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

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2019-0791

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/008665.html
http://oss.oracle.com/pipermail/el-errata/2019-April/008666.html

OEL7
x86_64
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.0.1.el7_6
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.0.1.el7_6
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.0.1.el7_6
java-1.7.0-openjdk-headless-1.7.0.221-2.6.18.0.0.1.el7_6
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.0.1.el7_6
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.0.1.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.221-2.6.18.0.0.1.el7_6

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

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2019-0790

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/008664.html

OEL6
x86_64
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.0.1.el6_10
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.0.1.el6_10

java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.0.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.0.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.0.1.el6_10

i386
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.0.1.el6_10
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.0.1.el6_10
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.0.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.0.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.0.1.el6_10

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

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2019-0774

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/008656.html

OEL6
x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10

i386
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10

171089 - Amazon Linux AMI ALAS-2019-1194 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5953

Description

The scan detected that the host is missing the following update:
ALAS-2019-1194

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1194.html

Amazon Linux AMI
x86_64
wget-debuginfo-1.18-5.30.amzn1
wget-1.18-5.30.amzn1

i686
wget-debuginfo-1.18-5.30.amzn1
wget-1.18-5.30.amzn1

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: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2019-0791

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/msg00021.html

RHEL7D
x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-headless-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el7_6

noarch
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.el7_6

RHEL7S
noarch
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.el7_6

x86_64
java-1.7.0-openjdk-headless-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el7_6

RHEL7WS
x86_64
java-1.7.0-openjdk-headless-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.221-2.6.18.0.el7_6
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el7_6

noarch
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.el7_6

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: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2019-0775

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/msg00016.html

RHEL7D
x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-zip-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el7_6

java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el7_6

RHEL7S
noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-zip-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el7_6

x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6

RHEL7WS
x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6

noarch
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-zip-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el7_6
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el7_6

196300 - Red Hat Enterprise Linux RHSA-2019-0782 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-11307, CVE-2018-12022, CVE-2018-12023, CVE-2018-14718, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2018-19360, CVE-2018-19361, CVE-2018-19362

Description

The scan detected that the host is missing the following update:
RHSA-2019-0782

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/msg00019.html

RHEL7S
noarch
rh-maven35-jackson-databind-javadoc-2.7.6-2.5.el7
rh-maven35-jackson-databind-2.7.6-2.5.el7

RHEL7WS
noarch
rh-maven35-jackson-databind-javadoc-2.7.6-2.5.el7
rh-maven35-jackson-databind-2.7.6-2.5.el7

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: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2019-0774

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/msg00017.html

RHEL6D
i386
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el6_10

x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el6_10

java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10

RHEL6S
i386
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-javadoc-1.8.0.212.b04-0.el6_10

x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-devel-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-demo-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-src-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debug-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10

RHEL6WS
x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el6_10

i386
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-1.8.0.212.b04-0.el6_10
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el6_10

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: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2019-0790

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/msg00020.html

RHEL6D
i386
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el6_10

noarch
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.el6_10

x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el6_10

RHEL6S
i386
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el6_10

noarch
java-1.7.0-openjdk-javadoc-1.7.0.221-2.6.18.0.el6_10

x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-demo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-src-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el6_10

RHEL6WS
x86_64
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el6_10

i386
java-1.7.0-openjdk-debuginfo-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-devel-1.7.0.221-2.6.18.0.el6_10
java-1.7.0-openjdk-1.7.0.221-2.6.18.0.el6_10

147861 - SuSE Linux 15.0 openSUSE-SU-2019:1261-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1261-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00177.html

SuSE Linux 15.0
x86_64
libSDL2-2_0-0-debuginfo-2.0.8-lp150.2.3.1
libSDL2-devel-32bit-2.0.8-lp150.2.3.1
libSDL2-2_0-0-32bit-2.0.8-lp150.2.3.1
libSDL2-devel-2.0.8-lp150.2.3.1
SDL2-debugsource-2.0.8-lp150.2.3.1
libSDL2-2_0-0-2.0.8-lp150.2.3.1
libSDL2-2_0-0-32bit-debuginfo-2.0.8-lp150.2.3.1

i586
libSDL2-devel-2.0.8-lp150.2.3.1
libSDL2-2_0-0-debuginfo-2.0.8-lp150.2.3.1
libSDL2-2_0-0-2.0.8-lp150.2.3.1
SDL2-debugsource-2.0.8-lp150.2.3.1

147862 - SuSE Linux 15.0 openSUSE-SU-2019:1239-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19870, CVE-2018-19872

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1239-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00152.html

SuSE Linux 15.0
i586
libQt5Sql5-unixODBC-debuginfo-5.9.4-lp150.11.1
libQt5Concurrent5-debuginfo-5.9.4-lp150.11.1
libQt5Gui5-5.9.4-lp150.11.1
libQt5Sql5-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-common-devel-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-common-devel-5.9.4-lp150.11.1
libQt5OpenGL-devel-5.9.4-lp150.11.1
libQt5KmsSupport-devel-static-5.9.4-lp150.11.1
libQt5Test-devel-5.9.4-lp150.11.1
libQt5DBus-devel-5.9.4-lp150.11.1
libQt5Sql5-unixODBC-5.9.4-lp150.11.1
libQt5Bootstrap-devel-static-5.9.4-lp150.11.1

libQt5Core-devel-5.9.4-lp150.11.1
libQt5Xml5-5.9.4-lp150.11.1
libQt5DBus-devel-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-sqlite-5.9.4-lp150.11.1
libQt5Gui-devel-5.9.4-lp150.11.1
libQt5DBus5-5.9.4-lp150.11.1
libQt5Sql5-mysql-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-examples-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-platformtheme-gtk3-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-sqlite-debuginfo-5.9.4-lp150.11.1
libQt5Network5-debuginfo-5.9.4-lp150.11.1
libQt5Xml5-debuginfo-5.9.4-lp150.11.1
libQt5PlatformHeaders-devel-5.9.4-lp150.11.1
libQt5Sql5-5.9.4-lp150.11.1
libQt5PrintSupport5-5.9.4-lp150.11.1
libQt5Widgets5-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-mysql-5.9.4-lp150.11.1
libQt5Network-devel-5.9.4-lp150.11.1
libQt5OpenGLExtensions-devel-static-5.9.4-lp150.11.1
libqt5-qtbase-debugsource-5.9.4-lp150.11.1
libQt5Xml-devel-5.9.4-lp150.11.1
libqt5-qtbase-examples-5.9.4-lp150.11.1
libqt5-qtbase-platformtheme-gtk3-5.9.4-lp150.11.1
libQt5Sql-devel-5.9.4-lp150.11.1
libQt5OpenGL5-5.9.4-lp150.11.1
libQt5Test5-debuginfo-5.9.4-lp150.11.1
libQt5Widgets5-5.9.4-lp150.11.1
libQt5Core5-debuginfo-5.9.4-lp150.11.1
libQt5Concurrent5-5.9.4-lp150.11.1
libQt5Widgets-devel-5.9.4-lp150.11.1
libQt5PrintSupport-devel-5.9.4-lp150.11.1
libQt5Test5-5.9.4-lp150.11.1
libQt5PlatformSupport-devel-static-5.9.4-lp150.11.1
libQt5Gui5-debuginfo-5.9.4-lp150.11.1
libQt5Concurrent-devel-5.9.4-lp150.11.1
libQt5Sql5-postgresql-debuginfo-5.9.4-lp150.11.1
libQt5Core5-5.9.4-lp150.11.1
libQt5PrintSupport5-debuginfo-5.9.4-lp150.11.1
libQt5Network5-5.9.4-lp150.11.1
libQt5OpenGL5-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-devel-5.9.4-lp150.11.1
libQt5DBus5-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-postgresql-5.9.4-lp150.11.1

noarch
libQt5PlatformSupport-private-headers-devel-5.9.4-lp150.11.1
libQt5Sql-private-headers-devel-5.9.4-lp150.11.1
libqt5-qtbase-private-headers-devel-5.9.4-lp150.11.1
libQt5Core-private-headers-devel-5.9.4-lp150.11.1
libQt5Network-private-headers-devel-5.9.4-lp150.11.1
libQt5DBus-private-headers-devel-5.9.4-lp150.11.1
libQt5OpenGL-private-headers-devel-5.9.4-lp150.11.1
libQt5Test-private-headers-devel-5.9.4-lp150.11.1
libQt5Widgets-private-headers-devel-5.9.4-lp150.11.1
libQt5PrintSupport-private-headers-devel-5.9.4-lp150.11.1
libQt5Gui-private-headers-devel-5.9.4-lp150.11.1
libQt5KmsSupport-private-headers-devel-5.9.4-lp150.11.1

x86_64
libQt5PrintSupport-devel-32bit-5.9.4-lp150.11.1

libQt5Widgets-devel-32bit-5.9.4-lp150.11.1
libQt5PlatformHeaders-devel-5.9.4-lp150.11.1
libQt5Core5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-debuginfo-5.9.4-lp150.11.1
libQt5Xml-devel-5.9.4-lp150.11.1
libQt5Test-devel-32bit-5.9.4-lp150.11.1
libQt5Network-devel-32bit-5.9.4-lp150.11.1
libQt5Core5-5.9.4-lp150.11.1
libQt5Gui5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5OpenGL-devel-5.9.4-lp150.11.1
libQt5OpenGL-devel-32bit-5.9.4-lp150.11.1
libQt5PrintSupport5-32bit-5.9.4-lp150.11.1
libQt5Sql5-sqlite-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-devel-5.9.4-lp150.11.1
libQt5Sql-devel-5.9.4-lp150.11.1
libQt5OpenGLExtensions-devel-static-32bit-5.9.4-lp150.11.1
libqt5-qtbase-common-devel-5.9.4-lp150.11.1
libQt5Sql5-mysql-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-examples-32bit-5.9.4-lp150.11.1
libQt5Test5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5DBus5-5.9.4-lp150.11.1
libQt5Test5-5.9.4-lp150.11.1
libQt5KmsSupport-devel-static-5.9.4-lp150.11.1
libQt5Gui5-debuginfo-5.9.4-lp150.11.1
libQt5Xml5-debuginfo-5.9.4-lp150.11.1
libQt5PlatformSupport-devel-static-5.9.4-lp150.11.1
libQt5Concurrent5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Bootstrap-devel-static-5.9.4-lp150.11.1
libQt5Gui5-32bit-5.9.4-lp150.11.1
libQt5Concurrent-devel-32bit-5.9.4-lp150.11.1
libQt5Widgets5-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-postgresql-5.9.4-lp150.11.1
libQt5Sql5-postgresql-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-mysql-32bit-5.9.4-lp150.11.1
libQt5Sql5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5PrintSupport5-5.9.4-lp150.11.1
libQt5PrintSupport-devel-5.9.4-lp150.11.1
libQt5Network5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5DBus-devel-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Core5-32bit-5.9.4-lp150.11.1
libQt5Sql5-sqlite-32bit-debuginfo-5.9.4-lp150.11.1
libQt5OpenGL5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Network5-debuginfo-5.9.4-lp150.11.1
libQt5Widgets5-5.9.4-lp150.11.1
libQt5Widgets5-32bit-5.9.4-lp150.11.1
libQt5Xml5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Core-devel-5.9.4-lp150.11.1
libqt5-qtbase-platformtheme-gtk3-debuginfo-5.9.4-lp150.11.1
libQt5Widgets5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-32bit-5.9.4-lp150.11.1
libqt5-qtbase-platformtheme-gtk3-5.9.4-lp150.11.1
libQt5Sql5-postgresql-debuginfo-5.9.4-lp150.11.1
libQt5Gui-devel-5.9.4-lp150.11.1
libQt5Widgets-devel-5.9.4-lp150.11.1
libQt5OpenGL5-5.9.4-lp150.11.1
libQt5Concurrent5-debuginfo-5.9.4-lp150.11.1
libQt5Xml5-32bit-5.9.4-lp150.11.1
libQt5Xml5-5.9.4-lp150.11.1
libQt5DBus-devel-32bit-5.9.4-lp150.11.1
libQt5Concurrent5-32bit-5.9.4-lp150.11.1

libQt5Concurrent-devel-5.9.4-lp150.11.1
libQt5Network5-5.9.4-lp150.11.1
libQt5OpenGLExtensions-devel-static-5.9.4-lp150.11.1
libQt5DBus5-32bit-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-examples-5.9.4-lp150.11.1
libQt5Test5-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-sqlite-5.9.4-lp150.11.1
libqt5-qtbase-common-devel-debuginfo-5.9.4-lp150.11.1
libQt5OpenGL5-debuginfo-5.9.4-lp150.11.1
libQt5Bootstrap-devel-static-32bit-5.9.4-lp150.11.1
libQt5Sql5-mysql-32bit-debuginfo-5.9.4-lp150.11.1
libQt5PlatformSupport-devel-static-32bit-5.9.4-lp150.11.1
libQt5Test5-32bit-5.9.4-lp150.11.1
libQt5Sql5-unixODBC-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Sql-devel-32bit-5.9.4-lp150.11.1
libQt5Concurrent5-5.9.4-lp150.11.1
libQt5Sql5-postgresql-32bit-5.9.4-lp150.11.1
libQt5PrintSupport5-32bit-debuginfo-5.9.4-lp150.11.1
libQt5DBus-devel-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-unixODBC-debuginfo-5.9.4-lp150.11.1
libQt5Test-devel-5.9.4-lp150.11.1
libQt5PrintSupport5-debuginfo-5.9.4-lp150.11.1
libqt5-qtbase-examples-debuginfo-5.9.4-lp150.11.1
libQt5OpenGL5-32bit-5.9.4-lp150.11.1
libQt5DBus5-debuginfo-5.9.4-lp150.11.1
libQt5Sql5-unixODBC-32bit-5.9.4-lp150.11.1
libQt5Sql5-mysql-5.9.4-lp150.11.1
libQt5Sql5-unixODBC-5.9.4-lp150.11.1
libqt5-qtbase-examples-32bit-debuginfo-5.9.4-lp150.11.1
libQt5Gui5-5.9.4-lp150.11.1
libQt5DBus-devel-5.9.4-lp150.11.1
libQt5Sql5-sqlite-32bit-5.9.4-lp150.11.1
libQt5Network5-32bit-5.9.4-lp150.11.1
libQt5Network-devel-5.9.4-lp150.11.1

147864 - SuSE Linux 15.0 openSUSE-SU-2019:1223-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1223-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00141.html

SuSE Linux 15.0
x86_64
libSDL-devel-1.2.15-lp150.2.3.1
libSDL-1_2-0-1.2.15-lp150.2.3.1
libSDL-1_2-0-32bit-debuginfo-1.2.15-lp150.2.3.1
libSDL-1_2-0-32bit-1.2.15-lp150.2.3.1

libSDL-devel-32bit-1.2.15-lp150.2.3.1
libSDL-1_2-0-debuginfo-1.2.15-lp150.2.3.1
SDL-debugsource-1.2.15-lp150.2.3.1

i586
libSDL-devel-1.2.15-lp150.2.3.1
SDL-debugsource-1.2.15-lp150.2.3.1
libSDL-1_2-0-1.2.15-lp150.2.3.1
libSDL-1_2-0-debuginfo-1.2.15-lp150.2.3.1

147865 - SuSE Linux 42.3 openSUSE-SU-2019:1222-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20346, CVE-2018-20506

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1222-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00138.html

SuSE Linux 42.3
i586
sqlite3-3.8.10.2-11.3.1
sqlite3-devel-3.8.10.2-11.3.1
libsqlite3-0-debuginfo-3.8.10.2-11.3.1
sqlite3-debugsource-3.8.10.2-11.3.1
sqlite3-debuginfo-3.8.10.2-11.3.1
libsqlite3-0-3.8.10.2-11.3.1

noarch
sqlite3-doc-3.8.10.2-11.3.1

x86_64
sqlite3-3.8.10.2-11.3.1
sqlite3-devel-3.8.10.2-11.3.1
libsqlite3-0-debuginfo-3.8.10.2-11.3.1
libsqlite3-0-debuginfo-32bit-3.8.10.2-11.3.1
sqlite3-debugsource-3.8.10.2-11.3.1
libsqlite3-0-32bit-3.8.10.2-11.3.1
sqlite3-debuginfo-3.8.10.2-11.3.1
libsqlite3-0-3.8.10.2-11.3.1

182956 - FreeBSD libssh2 Multiple Issues (6e58e1e9-2636-413e-9f84-4c0e21143628)

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

Risk Level: Medium

CVE: CVE-2019-3858, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862

Description

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

libssh2 -- multiple issues (6e58e1e9-2636-413e-9f84-4c0e21143628)

Observation

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

http://www.vuxml.org/freebsd/6e58e1e9-2636-413e-9f84-4c0e21143628.html

Affected packages:
libssh2 < 1.8.1

182962 - FreeBSD FreeBSD EAP-pwd Missing Commit Validation (2da3cb25-6571-11e9-8e67-206a8a720317)

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

Risk Level: Medium

CVE: CVE-2019-9497, CVE-2019-9498, CVE-2019-9499

Description

The scan detected that the host is missing the following update:
FreeBSD -- EAP-pwd missing commit validation (2da3cb25-6571-11e9-8e67-206a8a720317)

Observation

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

http://www.vuxml.org/freebsd/2da3cb25-6571-11e9-8e67-206a8a720317.html

Affected packages:
12.0 <= FreeBSD < 12.0_3
11.2 <= FreeBSD < 11.2_9
wpa_supplicant < 2.8
hostapd < 2.8

186665 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3953-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11034, CVE-2019-11035

Description

The scan detected that the host is missing the following update:
USN-3953-1

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/004860.html

Ubuntu 16.04

php7.0-fpm_7.0.33-0ubuntu0.16.04.4
libapache2-mod-php7.0_7.0.33-0ubuntu0.16.04.4
php7.0-cgi_7.0.33-0ubuntu0.16.04.4
php7.0-cli_7.0.33-0ubuntu0.16.04.4

Ubuntu 18.10

php7.2-cli_7.2.17-0ubuntu0.18.10.1
libapache2-mod-php7.2_7.2.17-0ubuntu0.18.10.1
php7.2-cgi_7.2.17-0ubuntu0.18.10.1
php7.2-fpm_7.2.17-0ubuntu0.18.10.1

Ubuntu 19.04

libapache2-mod-php7.2_7.2.17-0ubuntu0.19.04.1
php7.2-fpm_7.2.17-0ubuntu0.19.04.1
php7.2-cli_7.2.17-0ubuntu0.19.04.1
php7.2-cgi_7.2.17-0ubuntu0.19.04.1

Ubuntu 18.04

php7.2-cgi_7.2.17-0ubuntu0.18.04.1
php7.2-cli_7.2.17-0ubuntu0.18.04.1
php7.2-fpm_7.2.17-0ubuntu0.18.04.1
libapache2-mod-php7.2_7.2.17-0ubuntu0.18.04.1

195076 - Fedora Linux 28 FEDORA-2019-235c682f35 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10536, CVE-2018-10537, CVE-2018-10538, CVE-2018-10539, CVE-2018-10540, CVE-2018-19840, CVE-2018-19841

Description

The scan detected that the host is missing the following update:
FEDORA-2019-235c682f35

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

wavpack-5.1.0-12.fc28

195082 - Fedora Linux 28 FEDORA-2019-d03bae77f5 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-d03bae77f5

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

hostapd-2.7-2.fc28

195083 - Fedora Linux 29 FEDORA-2019-f409af9fbe 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-f409af9fbe

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

hostapd-2.7-2.fc29

196295 - Red Hat Enterprise Linux RHSA-2019-0809 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12180

Description

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

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/msg00028.html

RHEL7S
noarch
OVMF-20180508-3.gitee3198e672e2.el7_6.1

196298 - Red Hat Enterprise Linux RHSA-2019-0818 Update Is Not Installed

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

RHSA-2019-0818

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/msg00026.html

RHEL7D
x86_64
kernel-debuginfo-common-x86_64-3.10.0-957.12.1.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-debuginfo-3.10.0-957.12.1.el7
kernel-tools-debuginfo-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
python-perf-debuginfo-3.10.0-957.12.1.el7
bpftool-3.10.0-957.12.1.el7
kernel-debug-debuginfo-3.10.0-957.12.1.el7
perf-debuginfo-3.10.0-957.12.1.el7
kernel-headers-3.10.0-957.12.1.el7
python-perf-3.10.0-957.12.1.el7
kernel-tools-libs-devel-3.10.0-957.12.1.el7
perf-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

RHEL7S
noarch
kernel-doc-3.10.0-957.12.1.el7
kernel-abi-whitelists-3.10.0-957.12.1.el7

x86_64
kernel-debuginfo-common-x86_64-3.10.0-957.12.1.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-debuginfo-3.10.0-957.12.1.el7
kernel-tools-debuginfo-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
python-perf-debuginfo-3.10.0-957.12.1.el7
bpftool-3.10.0-957.12.1.el7
kernel-debug-debuginfo-3.10.0-957.12.1.el7
perf-debuginfo-3.10.0-957.12.1.el7
kernel-headers-3.10.0-957.12.1.el7
python-perf-3.10.0-957.12.1.el7
kernel-tools-libs-devel-3.10.0-957.12.1.el7
perf-3.10.0-957.12.1.el7

RHEL7WS
x86_64
kernel-debuginfo-common-x86_64-3.10.0-957.12.1.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-debuginfo-3.10.0-957.12.1.el7
kernel-tools-debuginfo-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
python-perf-debuginfo-3.10.0-957.12.1.el7
bpftool-3.10.0-957.12.1.el7
kernel-debug-debuginfo-3.10.0-957.12.1.el7
perf-debuginfo-3.10.0-957.12.1.el7
kernel-headers-3.10.0-957.12.1.el7
python-perf-3.10.0-957.12.1.el7
kernel-tools-libs-devel-3.10.0-957.12.1.el7
perf-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

24927 - IBM HTTP Server Security Bypass Vulnerability (ibm10869064)

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

Risk Level: Medium

CVE: CVE-2018-17199

Description

A vulnerability is present in some versions of IBM HTTP Server.

Observation

IBM HTTP Server is an Apache-based web server.

A vulnerability is present in some versions of IBM HTTP Server. The flaw is due to improper checking of session expiry time. Successful exploitation could allow an attacker to bypass security restrictions.

25012 - IBM WebSphere Application Server Denial of Service Vulnerability (ibm10869570)

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

Risk Level: Medium

CVE: CVE-2019-4046

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 is due to improper handling of request headers. Successful exploitation could allow an attacker to cause a denial of service.

25016 - IBM WebSphere Application Server Liberty Denial of Service Vulnerability (ibm10869570)

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

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

Observation

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

A vulnerability is present in some versions of IBM WebSphere Application Server Liberty. The flaw is due to improper handling of request headers. Successful exploitation could allow a remote attacker to cause denial of service condition on the target system.

25032 - Cisco IOS Software Network Plug-and-Play Agent Certificate Validation Vulnerability (cisco-sa-20190327-pnp-cert)

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

Risk Level: Medium

CVE: CVE-2019-1748

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 certificate validation. Successful exploitation could allow an attacker to supply a crafted certificate and conduct man-in-the-middle attacks to retrieve sensitive information from the affected device.

25041 - (K18549143) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2019-1559

Description

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

Observation

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

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

25060 - (JSA10920) Juniper Junos OS Jdhcpd Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0031

Description

A denial of service vulnerability is present in some versions of Juniper Junos OS.

Observation

Juniper Junos OS is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos OS. The flaw lies in the jdhcpd service. Successful exploitation could allow a remote attacker to cause a denial of service condition in the target system.

147855 - SuSE Linux 15.0 openSUSE-SU-2019:1259-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19865

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1259-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00175.html

SuSE Linux 15.0
x86_64
libqt5-qtvirtualkeyboard-debuginfo-5.9.4-lp150.2.3.1
libqt5-qtvirtualkeyboard-devel-5.9.4-lp150.2.3.1
libqt5-qtvirtualkeyboard-examples-debuginfo-5.9.4-lp150.2.3.1
libqt5-qtvirtualkeyboard-debugsource-5.9.4-lp150.2.3.1
libqt5-qtvirtualkeyboard-examples-5.9.4-lp150.2.3.1
libqt5-qtvirtualkeyboard-5.9.4-lp150.2.3.1

147856 - SuSE Linux 15.0 openSUSE-SU-2019:1237-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20482, CVE-2019-9923

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1237-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00148.html

SuSE Linux 15.0
i586
tar-debugsource-1.30-lp150.7.1
tar-rmt-debuginfo-1.30-lp150.7.1
tar-rmt-1.30-lp150.7.1
tar-1.30-lp150.7.1
tar-tests-1.30-lp150.7.1
tar-debuginfo-1.30-lp150.7.1

tar-tests-debuginfo-1.30-lp150.7.1

noarch
tar-lang-1.30-lp150.7.1
tar-backup-scripts-1.30-lp150.7.1
tar-doc-1.30-lp150.7.1

x86_64
tar-debugsource-1.30-lp150.7.1
tar-rmt-debuginfo-1.30-lp150.7.1
tar-rmt-1.30-lp150.7.1
tar-1.30-lp150.7.1
tar-tests-1.30-lp150.7.1
tar-debuginfo-1.30-lp150.7.1
tar-tests-debuginfo-1.30-lp150.7.1

147858 - SuSE Linux 15.0 openSUSE-SU-2019:1235-1 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-2019:1235-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00151.html

SuSE Linux 15.0
x86_64
libxmltooling-devel-1.6.4-lp150.2.3.1
libxmltooling7-debuginfo-1.6.4-lp150.2.3.1
libxmltooling7-1.6.4-lp150.2.3.1
xmltooling-debugsource-1.6.4-lp150.2.3.1
xmltooling-schemas-1.6.4-lp150.2.3.1

160548 - CentOS 7 CESA-2019-0778 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
CESA-2019-0778

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/023273.html

CentOS 7
x86_64
java-11-openjdk-javadoc-zip-debug-11.0.3.7-0.el7_6
java-11-openjdk-devel-11.0.3.7-0.el7_6
java-11-openjdk-devel-debug-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.3.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.3.7-0.el7_6
java-11-openjdk-headless-11.0.3.7-0.el7_6
java-11-openjdk-debug-11.0.3.7-0.el7_6
java-11-openjdk-jmods-11.0.3.7-0.el7_6
java-11-openjdk-headless-debug-11.0.3.7-0.el7_6
java-11-openjdk-src-11.0.3.7-0.el7_6
java-11-openjdk-src-debug-11.0.3.7-0.el7_6
java-11-openjdk-11.0.3.7-0.el7_6

i686
java-11-openjdk-javadoc-zip-debug-11.0.3.7-0.el7_6
java-11-openjdk-devel-11.0.3.7-0.el7_6
java-11-openjdk-devel-debug-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.3.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.3.7-0.el7_6
java-11-openjdk-headless-11.0.3.7-0.el7_6
java-11-openjdk-debug-11.0.3.7-0.el7_6
java-11-openjdk-jmods-11.0.3.7-0.el7_6
java-11-openjdk-headless-debug-11.0.3.7-0.el7_6
java-11-openjdk-src-11.0.3.7-0.el7_6
java-11-openjdk-src-debug-11.0.3.7-0.el7_6
java-11-openjdk-11.0.3.7-0.el7_6

163848 - Oracle Enterprise Linux ELSA-2019-4619 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13305

Description

The scan detected that the host is missing the following update:
ELSA-2019-4619

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/008662.html
http://oss.oracle.com/pipermail/el-errata/2019-April/008663.html

OEL7
x86_64
kernel-uek-debug-devel-4.1.12-124.26.10.el7uek
kernel-uek-devel-4.1.12-124.26.10.el7uek

kernel-uek-firmware-4.1.12-124.26.10.el7uek
kernel-uek-doc-4.1.12-124.26.10.el7uek
kernel-uek-debug-4.1.12-124.26.10.el7uek
kernel-uek-4.1.12-124.26.10.el7uek

OEL6
x86_64
kernel-uek-devel-4.1.12-124.26.10.el6uek
kernel-uek-debug-devel-4.1.12-124.26.10.el6uek
kernel-uek-firmware-4.1.12-124.26.10.el6uek
kernel-uek-debug-4.1.12-124.26.10.el6uek
kernel-uek-doc-4.1.12-124.26.10.el6uek
kernel-uek-4.1.12-124.26.10.el6uek

163850 - Oracle Enterprise Linux ELSA-2019-0778 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ELSA-2019-0778

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/008657.html

OEL7
x86_64
java-11-openjdk-javadoc-debug-11.0.3.7-0.0.1.el7_6
java-11-openjdk-demo-debug-11.0.3.7-0.0.1.el7_6
java-11-openjdk-devel-debug-11.0.3.7-0.0.1.el7_6
java-11-openjdk-devel-11.0.3.7-0.0.1.el7_6
java-11-openjdk-headless-debug-11.0.3.7-0.0.1.el7_6
java-11-openjdk-src-11.0.3.7-0.0.1.el7_6
java-11-openjdk-debug-11.0.3.7-0.0.1.el7_6
java-11-openjdk-11.0.3.7-0.0.1.el7_6
java-11-openjdk-jmods-debug-11.0.3.7-0.0.1.el7_6
java-11-openjdk-javadoc-11.0.3.7-0.0.1.el7_6
java-11-openjdk-src-debug-11.0.3.7-0.0.1.el7_6
java-11-openjdk-javadoc-zip-11.0.3.7-0.0.1.el7_6
java-11-openjdk-demo-11.0.3.7-0.0.1.el7_6
java-11-openjdk-jmods-11.0.3.7-0.0.1.el7_6
java-11-openjdk-headless-11.0.3.7-0.0.1.el7_6
java-11-openjdk-javadoc-zip-debug-11.0.3.7-0.0.1.el7_6

178737 - Gentoo Linux GLSA-201904-23 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-201904-23

Observation

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

https://security.gentoo.org/glsa/201904-23

Affected packages:
dev-libs/glib < 2.56.4

178738 - Gentoo Linux GLSA-201904-18 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-18

Observation

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

https://security.gentoo.org/glsa/201904-18

Affected packages:
sys-libs/libseccomp < 2.4.0

178739 - Gentoo Linux GLSA-201904-22 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-201904-22

Observation

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

https://security.gentoo.org/glsa/201904-22

Affected packages:
mail-filter/opendkim < 2.10.3-r8

178740 - Gentoo Linux GLSA-201904-20 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-20

Observation

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

https://security.gentoo.org/glsa/201904-20

Affected packages:
www-servers/apache < 2.4.39

178741 - Gentoo Linux GLSA-201904-21 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-21

Observation

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

https://security.gentoo.org/glsa/201904-21

Affected packages:
dev-db/sqlite < 3.25.3

178742 - Gentoo Linux GLSA-201904-17 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201904-17

Observation

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

https://security.gentoo.org/glsa/201904-17

Affected packages:
sys-devel/patch < 2.7.6-r3

178743 - Gentoo Linux GLSA-201904-19 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-201904-19

Observation

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

https://security.gentoo.org/glsa/201904-19

Affected packages:
net-mail/dovecot < 2.3.5.1

182961 - FreeBSD FreeBSD SAE Confirm Missing State Validation (98b71436-656d-11e9-8e67-206a8a720317)

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

Risk Level: Medium

CVE: CVE-2019-9496

Description

The scan detected that the host is missing the following update:
FreeBSD -- SAE confirm missing state validation (98b71436-656d-11e9-8e67-206a8a720317)

Observation

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

http://www.vuxml.org/freebsd/98b71436-656d-11e9-8e67-206a8a720317.html

Affected packages:
12.0 <= FreeBSD < 12.0_3
11.2 <= FreeBSD < 11.2_9
wpa_supplicant < 2.8
hostapd < 2.8

182963 - FreeBSD GnuTLS Double Free, Invalid Pointer Access (fb30db8f-62af-11e9-b0de-001cc0382b2f)

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
GnuTLS -- double free, invalid pointer access (fb30db8f-62af-11e9-b0de-001cc0382b2f)

Observation

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

http://www.vuxml.org/freebsd/fb30db8f-62af-11e9-b0de-001cc0382b2f.html

Affected packages:
gnutls < 3.6.7

186663 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3952-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16877, CVE-2018-16878, CVE-2019-3885

Description

The scan detected that the host is missing the following update:
USN-3952-1

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/004859.html

Ubuntu 16.04

pacemaker_1.1.14-2ubuntu1.6

Ubuntu 18.10

pacemaker_1.1.18-2ubuntu1.18.10.1

Ubuntu 19.04

pacemaker_1.1.18-2ubuntu1.19.04.1

Ubuntu 18.04

pacemaker_1.1.18-0ubuntu1.1

195071 - Fedora Linux 30 FEDORA-2019-e4c8de3fb7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16877, CVE-2018-16878, CVE-2019-3885

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e4c8de3fb7

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

pacemaker-2.0.1-2.fc30

195077 - Fedora Linux 29 FEDORA-2019-a6c56f9756 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-a6c56f9756

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

python-urllib3-1.24.2-1.fc29

195080 - Fedora Linux 29 FEDORA-2019-77b2d840ef Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16056, CVE-2018-16057, CVE-2018-16058, CVE-2018-19622, CVE-2018-19623, CVE-2018-19624, CVE-2018-19625, CVE-2018-19626, CVE-2018-19627, CVE-2018-19628, 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, CVE-2019-5716, CVE-2019-5717, CVE-2019-5718, CVE-2019-5719

Description

The scan detected that the host is missing the following update:
FEDORA-2019-77b2d840ef

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

wireshark-3.0.1-1.fc29

196293 - Red Hat Enterprise Linux RHSA-2019-0806 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-2019-0806

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/msg00023.html

RHEL6S
x86_64
python27-python-libs-2.7.13-4.el6
python27-python-debug-2.7.13-4.el6
python27-tkinter-2.7.13-4.el6
python27-python-2.7.13-4.el6
python27-python-debuginfo-2.7.13-4.el6
python27-python-devel-2.7.13-4.el6
python27-python-tools-2.7.13-4.el6
python27-python-test-2.7.13-4.el6

RHEL6WS
x86_64
python27-python-libs-2.7.13-4.el6
python27-python-debug-2.7.13-4.el6
python27-tkinter-2.7.13-4.el6
python27-python-2.7.13-4.el6
python27-python-debuginfo-2.7.13-4.el6
python27-python-devel-2.7.13-4.el6
python27-python-tools-2.7.13-4.el6
python27-python-test-2.7.13-4.el6

RHEL7S
ppc64le
python27-python-devel-2.7.13-6.el7
python27-python-debug-2.7.13-6.el7
python27-python-debuginfo-2.7.13-6.el7
python27-python-test-2.7.13-6.el7
python27-python-2.7.13-6.el7
python27-python-libs-2.7.13-6.el7
python27-python-tools-2.7.13-6.el7
python27-tkinter-2.7.13-6.el7

RHEL7WS
x86_64
python27-python-devel-2.7.13-6.el7
python27-python-debug-2.7.13-6.el7
python27-python-debuginfo-2.7.13-6.el7
python27-python-test-2.7.13-6.el7
python27-python-2.7.13-6.el7
python27-python-libs-2.7.13-6.el7
python27-python-tools-2.7.13-6.el7
python27-tkinter-2.7.13-6.el7

196299 - Red Hat Enterprise Linux RHSA-2019-0778 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

Description

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

RHSA-2019-0778

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/msg00018.html

RHEL7D
x86_64
java-11-openjdk-javadoc-zip-debug-11.0.3.7-0.el7_6
java-11-openjdk-devel-11.0.3.7-0.el7_6
java-11-openjdk-devel-debug-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.3.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.3.7-0.el7_6
java-11-openjdk-headless-11.0.3.7-0.el7_6
java-11-openjdk-debug-11.0.3.7-0.el7_6
java-11-openjdk-debuginfo-11.0.3.7-0.el7_6
java-11-openjdk-jmods-11.0.3.7-0.el7_6
java-11-openjdk-headless-debug-11.0.3.7-0.el7_6
java-11-openjdk-src-11.0.3.7-0.el7_6
java-11-openjdk-src-debug-11.0.3.7-0.el7_6
java-11-openjdk-11.0.3.7-0.el7_6

RHEL7S
x86_64
java-11-openjdk-javadoc-zip-debug-11.0.3.7-0.el7_6
java-11-openjdk-devel-11.0.3.7-0.el7_6
java-11-openjdk-devel-debug-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.3.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.3.7-0.el7_6
java-11-openjdk-headless-11.0.3.7-0.el7_6
java-11-openjdk-debug-11.0.3.7-0.el7_6
java-11-openjdk-debuginfo-11.0.3.7-0.el7_6
java-11-openjdk-jmods-11.0.3.7-0.el7_6
java-11-openjdk-headless-debug-11.0.3.7-0.el7_6
java-11-openjdk-src-11.0.3.7-0.el7_6
java-11-openjdk-src-debug-11.0.3.7-0.el7_6
java-11-openjdk-11.0.3.7-0.el7_6

RHEL7WS
x86_64
java-11-openjdk-javadoc-zip-debug-11.0.3.7-0.el7_6
java-11-openjdk-devel-11.0.3.7-0.el7_6
java-11-openjdk-devel-debug-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.3.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-debug-11.0.3.7-0.el7_6
java-11-openjdk-demo-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-11.0.3.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.3.7-0.el7_6
java-11-openjdk-headless-11.0.3.7-0.el7_6

java-11-openjdk-debug-11.0.3.7-0.el7_6
java-11-openjdk-debuginfo-11.0.3.7-0.el7_6
java-11-openjdk-jmods-11.0.3.7-0.el7_6
java-11-openjdk-headless-debug-11.0.3.7-0.el7_6
java-11-openjdk-src-11.0.3.7-0.el7_6
java-11-openjdk-src-debug-11.0.3.7-0.el7_6
java-11-openjdk-11.0.3.7-0.el7_6

25057 - Cisco IOS Software Smart Call Home Certificate Validation Vulnerability (cisco-sa-20190327-call-home-cert)

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

Risk Level: Medium

CVE: CVE-2019-1757

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 lies in Cisco Smart Call Home feature. Successful exploitation could allow an unauthenticated, remote attacker to retrieve sensitive information from the target system.

89019 - Slackware Linux 14.2 SSA:2019-107-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14048, CVE-2018-14550, CVE-2019-7317

Description

The scan detected that the host is missing the following update:
SSA:2019-107-01

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.369646

Slackware 14.2
x86_64
libpng-1.6.37-x86_64-1

i586
libpng-1.6.37-i586-1

131337 - Debian Linux 9.0 DSA-4434-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11358

Description

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

DSA-4434-1

Observation

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

http://www.debian.org/security/2019/dsa-4434

Debian 9.0
all
drupal7_7.52-2+deb9u8

147849 - SuSE Linux 15.0 openSUSE-SU-2019:1225-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6888

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1225-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00137.html

SuSE Linux 15.0
i586
flac-debuginfo-1.3.2-lp150.2.3.1
libFLAC8-1.3.2-lp150.2.3.1
libFLAC8-debuginfo-1.3.2-lp150.2.3.1
libFLAC++6-1.3.2-lp150.2.3.1
flac-1.3.2-lp150.2.3.1
flac-debugsource-1.3.2-lp150.2.3.1
libFLAC++6-debuginfo-1.3.2-lp150.2.3.1
flac-devel-1.3.2-lp150.2.3.1

noarch
flac-doc-1.3.2-lp150.2.3.1

x86_64
flac-devel-32bit-1.3.2-lp150.2.3.1
libFLAC++6-32bit-1.3.2-lp150.2.3.1
flac-1.3.2-lp150.2.3.1
flac-debugsource-1.3.2-lp150.2.3.1
libFLAC8-debuginfo-1.3.2-lp150.2.3.1
flac-debuginfo-1.3.2-lp150.2.3.1
flac-devel-1.3.2-lp150.2.3.1
libFLAC8-32bit-1.3.2-lp150.2.3.1
libFLAC++6-debuginfo-1.3.2-lp150.2.3.1
libFLAC8-32bit-debuginfo-1.3.2-lp150.2.3.1
libFLAC++6-32bit-debuginfo-1.3.2-lp150.2.3.1
libFLAC++6-1.3.2-lp150.2.3.1
libFLAC8-1.3.2-lp150.2.3.1

147852 - SuSE Linux 15.0 openSUSE-SU-2019:1224-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10689

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1224-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00143.html

SuSE Linux 15.0
x86_64
blktrace-debuginfo-1.1.0+git.20170126-lp150.2.3.1
blktrace-1.1.0+git.20170126-lp150.2.3.1
blktrace-debugsource-1.1.0+git.20170126-lp150.2.3.1

147854 - SuSE Linux 15.0 openSUSE-SU-2019:1250-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10739

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1250-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00164.html

SuSE Linux 15.0
i586
nscd-debuginfo-2.26-lp150.11.17.1
nscd-2.26-lp150.11.17.1
glibc-locale-2.26-lp150.11.17.1
glibc-devel-2.26-lp150.11.17.1
glibc-utils-src-debugsource-2.26-lp150.11.17.1
glibc-extra-2.26-lp150.11.17.1
glibc-devel-static-2.26-lp150.11.17.1
glibc-locale-base-debuginfo-2.26-lp150.11.17.1
glibc-debuginfo-2.26-lp150.11.17.1
glibc-extra-debuginfo-2.26-lp150.11.17.1
glibc-2.26-lp150.11.17.1
glibc-debugsource-2.26-lp150.11.17.1
glibc-utils-2.26-lp150.11.17.1
glibc-utils-debuginfo-2.26-lp150.11.17.1
glibc-profile-2.26-lp150.11.17.1
glibc-devel-debuginfo-2.26-lp150.11.17.1

glibc-locale-base-2.26-lp150.11.17.1

i686
glibc-debugsource-2.26-lp150.11.17.1
glibc-devel-2.26-lp150.11.17.1
glibc-locale-base-2.26-lp150.11.17.1
glibc-locale-base-debuginfo-2.26-lp150.11.17.1
glibc-devel-debuginfo-2.26-lp150.11.17.1
glibc-debuginfo-2.26-lp150.11.17.1
glibc-devel-static-2.26-lp150.11.17.1
glibc-2.26-lp150.11.17.1
glibc-locale-2.26-lp150.11.17.1
glibc-profile-2.26-lp150.11.17.1

noarch
glibc-i18ndata-2.26-lp150.11.17.1
glibc-info-2.26-lp150.11.17.1
glibc-html-2.26-lp150.11.17.1

x86_64
nscd-debuginfo-2.26-lp150.11.17.1
glibc-utils-src-debugsource-2.26-lp150.11.17.1
glibc-2.26-lp150.11.17.1
glibc-devel-static-32bit-2.26-lp150.11.17.1
glibc-locale-2.26-lp150.11.17.1
glibc-devel-32bit-2.26-lp150.11.17.1
glibc-debugsource-2.26-lp150.11.17.1
glibc-locale-base-2.26-lp150.11.17.1
nscd-2.26-lp150.11.17.1
glibc-locale-base-debuginfo-2.26-lp150.11.17.1
glibc-extra-2.26-lp150.11.17.1
glibc-profile-2.26-lp150.11.17.1
glibc-debuginfo-2.26-lp150.11.17.1
glibc-utils-debuginfo-2.26-lp150.11.17.1
glibc-32bit-2.26-lp150.11.17.1
glibc-utils-32bit-2.26-lp150.11.17.1
glibc-extra-debuginfo-2.26-lp150.11.17.1
glibc-utils-2.26-lp150.11.17.1
glibc-utils-32bit-debuginfo-2.26-lp150.11.17.1
glibc-profile-32bit-2.26-lp150.11.17.1
glibc-locale-base-32bit-2.26-lp150.11.17.1
glibc-devel-static-2.26-lp150.11.17.1
glibc-devel-debuginfo-2.26-lp150.11.17.1
glibc-32bit-debuginfo-2.26-lp150.11.17.1
glibc-devel-32bit-debuginfo-2.26-lp150.11.17.1
glibc-locale-base-32bit-debuginfo-2.26-lp150.11.17.1
glibc-devel-2.26-lp150.11.17.1

147863 - SuSE Linux 15.0 openSUSE-SU-2019:1260-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-13440

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1260-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-04/msg00176.html

SuSE Linux 15.0
x86_64
libaudiofile1-32bit-debuginfo-0.3.6-lp150.7.1
libaudiofile1-32bit-0.3.6-lp150.7.1
audiofile-debugsource-0.3.6-lp150.7.1
audiofile-devel-32bit-0.3.6-lp150.7.1
audiofile-debuginfo-0.3.6-lp150.7.1
audiofile-devel-0.3.6-lp150.7.1
audiofile-doc-0.3.6-lp150.7.1
libaudiofile1-0.3.6-lp150.7.1
libaudiofile1-debuginfo-0.3.6-lp150.7.1
audiofile-0.3.6-lp150.7.1

i586
audiofile-debugsource-0.3.6-lp150.7.1
audiofile-debuginfo-0.3.6-lp150.7.1
audiofile-devel-0.3.6-lp150.7.1
audiofile-doc-0.3.6-lp150.7.1
libaudiofile1-0.3.6-lp150.7.1
libaudiofile1-debuginfo-0.3.6-lp150.7.1
audiofile-0.3.6-lp150.7.1

171090 - Amazon Linux AMI ALAS-2018-1123 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10906

Description

The scan detected that the host is missing the following update:
ALAS-2018-1123

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1123.html

Amazon Linux AMI
x86_64
fuse-debuginfo-2.9.4-1.18.amzn1
fuse-2.9.4-1.18.amzn1
fuse-libs-2.9.4-1.18.amzn1
fuse-devel-2.9.4-1.18.amzn1

i686
fuse-debuginfo-2.9.4-1.18.amzn1
fuse-2.9.4-1.18.amzn1
fuse-libs-2.9.4-1.18.amzn1
fuse-devel-2.9.4-1.18.amzn1

182957 - FreeBSD FreeBSD EAP-pwd Side-channel Attack (60129efe-656d-11e9-8e67-206a8a720317)

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

Risk Level: Medium

CVE: CVE-2019-9495

Description

The scan detected that the host is missing the following update:
FreeBSD -- EAP-pwd side-channel attack (60129efe-656d-11e9-8e67-206a8a720317)

Observation

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

http://www.vuxml.org/freebsd/60129efe-656d-11e9-8e67-206a8a720317.html

Affected packages:
12.0 <= FreeBSD < 12.0_3
11.2 <= FreeBSD < 11.2_9
wpa_supplicant < 2.8
hostapd < 2.8

182964 - FreeBSD Ghostscript Security Bypass Vulnerability (5ed7102e-6454-11e9-9a3a-001cc0382b2f)

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
Ghostscript -- Security bypass vulnerability (5ed7102e-6454-11e9-9a3a-001cc0382b2f)

Observation

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

http://www.vuxml.org/freebsd/5ed7102e-6454-11e9-9a3a-001cc0382b2f.html

Affected packages:
ghostscript9-agpl-base < 9.27
ghostscript9-agpl-x11 < 9.27

182966 - FreeBSD FreeBSD SAE Side-channel Attacks (7e53f9cc-656d-11e9-8e67-206a8a720317)

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

Risk Level: Medium

CVE: CVE-2019-9494

Description

The scan detected that the host is missing the following update:
FreeBSD -- SAE side-channel attacks (7e53f9cc-656d-11e9-8e67-206a8a720317)

Observation

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

For more information see:

http://www.vuxml.org/freebsd/7e53f9cc-656d-11e9-8e67-206a8a720317.html

Affected packages:
12.0 <= FreeBSD < 12.0_3
11.2 <= FreeBSD < 11.2_9
wpa_supplicant < 2.8
hostapd < 2.8

186664 - Ubuntu Linux 18.10 USN-3950-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9917

Description

The scan detected that the host is missing the following update:
USN-3950-1

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/004857.html

Ubuntu 18.10

znc_1.7.1-2ubuntu0.1

195074 - Fedora Linux 29 FEDORA-2019-d5ad4a435c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9917

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d5ad4a435c

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

znc-1.7.3-1.fc29

195085 - Fedora Linux 28 FEDORA-2019-64ed5e4dfa Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9917

Description

The scan detected that the host is missing the following update:
FEDORA-2019-64ed5e4dfa

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

znc-1.7.3-1.fc28

196294 - Red Hat Enterprise Linux RHSA-2019-0832 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6133

Description

The scan detected that the host is missing the following update:
RHSA-2019-0832

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/msg00025.html

RHEL6_6S
x86_64
polkit-devel-0.96-7.el6_6.1
polkit-docs-0.96-7.el6_6.1
polkit-debuginfo-0.96-7.el6_6.1
polkit-0.96-7.el6_6.1

noarch
polkit-desktop-policy-0.96-7.el6_6.1

131336 - Debian Linux 9.0 DSA-4433-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-8320, CVE-2019-8321, CVE-2019-8322, CVE-2019-8323, CVE-2019-8324, CVE-2019-8325

Description

The scan detected that the host is missing the following update:
DSA-4433-1

Observation

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

http://www.debian.org/security/2019/dsa-4433

Debian 9.0
all
ruby2.3_2.3.3-1+deb9u6

182958 - FreeBSD FreeBSD EAP-pwd Message Reassembly Issue With Unexpected Fragment (a207bbd8-6572-11e9-8e67-206a8a720317)

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:
FreeBSD -- EAP-pwd message reassembly issue with unexpected fragment (a207bbd8-6572-11e9-8e67-206a8a720317)

Observation

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

http://www.vuxml.org/freebsd/a207bbd8-6572-11e9-8e67-206a8a720317.html

Affected packages:
12.0 <= FreeBSD < 12.0_3
11.2 <= FreeBSD < 11.2_9
wpa_supplicant < 2.8
hostapd < 2.8

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

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

Risk Level: Low

CVE: CVE-2019-10691

Description

The scan detected that the host is missing the following update:
dovecot -- json encoder crash (a64aa22f-61ec-11e9-85b9-a4badb296695)

Observation

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

http://www.vuxml.org/freebsd/a64aa22f-61ec-11e9-85b9-a4badb296695.html

Affected packages:
dovecot < 2.3.5.2

182960 - FreeBSD gitea Remote Code Execution (b747783f-5fb6-11e9-b2ac-08002705f877)

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:
gitea -- remote code execution (b747783f-5fb6-11e9-b2ac-08002705f877)

Observation

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

http://www.vuxml.org/freebsd/b747783f-5fb6-11e9-b2ac-08002705f877.html

Affected packages:
gitea < 1.7.5

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

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
Istio -- Security vulnerabilities (484d3f5e-653a-11e9-b0e3-1c39475b9f84)

Observation

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

http://www.vuxml.org/freebsd/484d3f5e-653a-11e9-b0e3-1c39475b9f84.html

Affected packages:
istio < 1.1.2

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

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

Risk Level: Low

CVE: CVE-2019-10691

Description

The scan detected that the host is missing the following update:
USN-3951-1

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/004858.html

Ubuntu 19.04

dovecot-core_2.3.4.1-1ubuntu2.1

Ubuntu 18.10

dovecot-core_2.3.2.1-1ubuntu3.3

186667 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3914-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3914-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-April/004856.html

Ubuntu 16.04

ntfs-3g_2015.3.14AR.1-1ubuntu0.3

Ubuntu 18.10

ntfs-3g_2017.3.23-2ubuntu0.18.10.2

Ubuntu 18.04

ntfs-3g_2017.3.23-2ubuntu0.18.04.2

195068 - Fedora Linux 30 FEDORA-2019-146f3a7d7f 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-2019-146f3a7d7f

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

glibd-2.1.0-1.fc30
appstream-generator-0.7.7-1.fc30
gir-to-d-0.19.0-1.fc30

195069 - Fedora Linux 28 FEDORA-2019-bbdaeae59f 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-bbdaeae59f

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

freeradius-3.0.19-1.fc28

195070 - Fedora Linux 28 FEDORA-2019-782e6e61ce Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-1002162

Description

The scan detected that the host is missing the following update:
FEDORA-2019-782e6e61ce

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

atomic-reactor-1.6.36.1-3.fc28

195072 - Fedora Linux 29 FEDORA-2019-9667df8350 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-2019-9667df8350

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

freeradius-3.0.19-1.fc29

195073 - Fedora Linux 29 FEDORA-2019-b6ec9df480 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-b6ec9df480

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

osbs-client-0.52-2.fc29

195075 - Fedora Linux 29 FEDORA-2019-b60638d04e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-1002162

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b60638d04e

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

atomic-reactor-1.6.36.1-3.fc29

195078 - Fedora Linux 28 FEDORA-2019-2fff3c6889 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-2019-2fff3c6889

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

osbs-client-0.52-2.fc28

195079 - Fedora Linux 29 FEDORA-2019-27e7b92407 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-2019-27e7b92407

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

elementary-camera-1.0.4-2.fc29
mpris-scrobbler-0.3.2-2.fc29
fuse-2.9.9-3.fc29
reportd-0.6.6-2.fc29
ephemeral-5.0.1-2.fc29
switchboard-plug-display-2.1.7-2.fc29
elementary-terminal-5.3.4-2.fc29
libxmlb-0.1.8-2.fc29
gnome-shell-extension-gsconnect-21-2.fc29
elementary-code-3.1.1-2.fc29
group-service-1.1.0-5.fc29
switchboard-plug-pantheon-shell-2.8.1-2.fc29
gnome-characters-3.30.0-3.fc29
mesa-18.3.6-3.fc29
fondo-1.2.2-4.20190324git71d97ee.fc29
geocode-glib-3.26.1-2.fc29
egl-wayland-1.1.2-3.fc29
meson-0.50.0-4.fc29
wingpanel-2.2.3-2.fc29
mate-user-admin-1.4.1-2.fc29
libmodulemd-2.2.3-3.fc29

195081 - Fedora Linux 29 FEDORA-2019-c36819bf25 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-c36819bf25

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

glpi-9.3.4-1.fc29

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ac2a21ff07

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

gnome-software-3.32.1-2.fc30
gnome-disk-utility-3.32.1-2.fc30
switchboard-plug-display-2.1.7-2.fc30
eog-3.32.1-2.fc30
gnome-initial-setup-3.32.1-2.fc30
msgpack-d-1.0.0-0.6.beta.7.fc30
gnome-maps-3.32.1-2.fc30
gir-to-d-0.18.0-4.fc30
gnome-system-monitor-3.32.1-2.fc30
elementary-code-3.1.1-2.fc30
gnome-builder-3.32.1-4.fc30
gnome-music-3.32.1-2.fc30
toolbox-0.0.8-2.fc30
dav1d-0.2.1-3.fc30
atomix-3.32.1-2.fc30
mesa-19.0.2-3.fc30
wingpanel-2.2.3-2.fc30
egl-wayland-1.1.2-3.fc30
zchunk-1.1.1-3.fc30
libinput-1.13.1-2.fc30
stdx-allocator-2.77.2-7.fc30
gnome-boxes-3.32.0.2-2.fc30
gnome-calculator-3.32.1-2.fc30
switchboard-plug-pantheon-shell-2.8.1-2.fc30
gnome-shell-extension-gsconnect-21-2.fc30
libnotify-0.7.8-2.fc30
signon-glib-2.1-4.fc30

at-spi2-core-2.32.1-2.fc30
libsoup-2.66.1-2.fc30
ephemeral-5.0.1-2.fc30
gamemode-1.2-4.fc30
elementary-camera-1.0.4-2.fc30
systemd-241-7.gita2eaa1c.fc30
fondo-1.2.2-4.20190324git71d97ee.fc30
simple-scan-3.32.2-2.fc30
libxmlb-0.1.8-2.fc30
gnome-books-3.32.0-3.fc30
dsymbol-20181014gitec28618-8.fc30
libplacebo-1.18.0-2.fc30
reportd-0.6.6-2.fc30
libdazzle-3.32.1-2.fc30
polari-3.32.0-3.fc30
fwupd-1.2.7-2.fc30
gnome-weather-3.32.1-2.fc30
fuse-2.9.9-3.fc30
elementary-terminal-5.3.4-2.fc30
meson-0.50.0-4.fc30
mate-user-admin-1.4.1-2.fc30
libdparse-0.9.9-7.fc30
file-roller-3.32.1-2.fc30
gnome-characters-3.32.1-2.fc30
gvfs-1.40.1-2.fc30
dbus-broker-20-3.fc30
containers-0.8.0-8.alpha.9.fc30
libmodulemd-2.2.3-3.fc30
gobject-introspection-1.60.1-2.fc30
group-service-1.1.0-5.fc30
mpris-scrobbler-0.3.2-2.fc30
gnome-desktop3-3.32.1-2.fc30
glib-networking-2.60.1-2.fc30
shotwell-0.31.0-2.fc30
glib2-2.60.1-2.fc30
bijiben-3.32.1-2.fc30
gnome-bluetooth-3.32.1-2.fc30
geocode-glib-3.26.1-2.fc30
gnome-control-center-3.32.1-2.fc30

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

24187 - (HPESBHF03866) HPE Integrated Lights-Out Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2018-7105

Update Details

CVE is updated

195014 - Fedora Linux 28 FEDORA-2019-3348cb4934 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000877, CVE-2018-1000878, CVE-2018-1000879, CVE-2018-1000880, CVE-2019-1000019, CVE-2019-1000020, CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Update Details

CVE is updated

21165 - (K17075474) F5 BIG-IP Glibc Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-4429

Update Details

FASLScript is updated

147115 - SuSE Linux 15.0 openSUSE-SU-2018:2895-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

CVE is updated

147136 - SuSE SLES 12 SP3 SUSE-SU-2018:2838-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

CVE is updated

147151 - SuSE SLES 11 SP4 SUSE-SU-2018:2789-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

CVE is updated

147583 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0179-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6519

Update Details

CVE is updated

147597 - SuSE Linux 42.3 openSUSE-SU-2019:0128-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6519

Update Details

CVE is updated

147610 - SuSE SLES 11 SP4 SUSE-SU-2019:13947-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6519

Update Details

CVE is updated

147660 - SuSE Linux 15.0 openSUSE-SU-2019:0197-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6519

Update Details

CVE is updated

194708 - Fedora Linux 29 FEDORA-2019-2e385f97e2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11333, CVE-2017-14160, CVE-2017-14632, CVE-2017-14633, CVE-2018-10392, CVE-2018-10393, CVE-2018-5146

Update Details

CVE 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

Update Details

CVE is updated

194501 - Fedora Linux 29 FEDORA-2018-e5e93f4c7b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

CVE is updated

194530 - Fedora Linux 28 FEDORA-2018-b74b9ac8d1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

CVE is updated

70050 - vmware.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70088 - ibm.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.