2018-JAN-04
FSL version 7.5.990

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

22797 - (HPESBHF03716) HPE Intelligent Management Center Authentication Bypass Vulnerability

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

Risk Level: High

CVE: CVE-2017-5791

Description

A remote authentication bypass vulnerability is present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A remote authentication bypass vulnerability is present in some versions of HPE Intelligent Management Center. The flaw lies in an unspecified component. Successful exploitation could allow an attacker to bypass authentication and gain unauthorized access to the target system.

22806 - (HPESBHF03710) HPE Intelligent Management Center Untrusted Data Deserialization Vulnerability

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

Risk Level: High

CVE: CVE-2017-5790

Description

A vulnerability is present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A vulnerability is present in some versions of HPE Intelligent Management Center. The flaw is related with deserialization of untrusted data. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22850 - (HT208334) Apple iOS Multiple Vulnerabilities Prior To 11.2

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2017-13080, CVE-2017-13833, CVE-2017-13847, CVE-2017-13855, CVE-2017-13856, CVE-2017-13860, CVE-2017-13861, CVE-2017-13862, CVE-2017-13865, CVE-2017-13866, CVE-2017-13867, CVE-2017-13868, CVE-2017-13869, CVE-2017-13870, CVE-2017-13874, CVE-2017-13876, CVE-2017-13879, CVE-2017-7152, CVE-2017-7154, CVE-2017-7156, CVE-2017-7157, CVE-2017-7160, CVE-2017-7162

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

Apple iOS is the operating system used by Apple iPhone, iPad and iPod touch.

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system and obtain sensitive information.

22884 - (APSB17-13) Creative Cloud Desktop Application Vulnerability

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

Risk Level: High

CVE: CVE-2017-3006, CVE-2017-3007

Description

Multiple vulnerabilities are present in some versions of Adobe Creative Cloud Desktop Application.

Observation

Adobe Creative Cloud Desktop Application is the desktop client used to access Adobe Creative Cloud.

Multiple vulnerabilities are present in some versions of Adobe Creative Cloud Desktop Application. The flaws lie in multiple components. Successful exploitation could allow an attacker to bypass security restrictions and execute arbitrary code in the context of the user.

22909 - (MSPT-Jan2018) Microsoft Scripting Engine Information Disclosure Vulnerability (CVE-2018-0780)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0780

Description

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22918 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0776)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0776

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22928 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Information Disclosure Vulnerability (CVE-2018-0800)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0800

Description

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

182565 - FreeBSD OTRS Multiple Vulnerabilities (cebd05d6-ed7b-11e7-95f2-005056925db4)

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

Risk Level: High

CVE: CVE-2017-16664, CVE-2017-16854, CVE-2017-16921

Description

The scan detected that the host is missing the following update:
OTRS -- Multiple vulnerabilities (cebd05d6-ed7b-11e7-95f2-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/cebd05d6-ed7b-11e7-95f2-005056925db4.html

Affected packages:
otrs < 5.0.26

193128 - Fedora Linux 26 FEDORA-2017-6e6f4f95e6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0898, CVE-2017-10784, CVE-2017-14033

Description

The scan detected that the host is missing the following update:
FEDORA-2017-6e6f4f95e6

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 26

ruby-2.4.2-84.fc26

22939 - (MSPT-Jan2018) Microsoft Products Speculative Execution Side-Channel Vulnerabilities (CVE-2017-5753)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5753

Description

A vulnerability in some versions of several Microsoft Products could lead to information disclosure.

Observation

A vulnerability in some versions of several Microsoft Products could lead to information disclosure.

The flaw lies in the usage of indirect branch prediction and speculative execution techniques. Successful exploitation could allow an attacker to retrieve sensitive information from the target system.

22940 - (MSPT-Jan2018) Microsoft Products Speculative Execution Side-Channel Vulnerabilities (CVE-2017-5715)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5715

Description

A vulnerability in some versions of several Microsoft Products could lead to information disclosure.

Observation

A vulnerability in some versions of several Microsoft Products could lead to information disclosure.

The flaw lies in the usage of indirect branch prediction and speculative execution techniques. Successful exploitation could allow an attacker to retrieve sensitive information from the target system.

22941 - (MSPT-Jan2018) Microsoft Products Speculative Execution Side-Channel Vulnerabilities (CVE-2017-5754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5754

Description

A vulnerability in some versions of several Microsoft Products could lead to information disclosure.

Observation

A vulnerability in some versions of several Microsoft Products could lead to information disclosure.

The flaw lies in the usage of indirect branch prediction and speculative execution techniques. Successful exploitation could allow an attacker to retrieve sensitive information from the target system.

22886 - Google Chrome Multiple Vulnerabilities Prior To 63.0.3239.108

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

Risk Level: High

CVE: CVE-2017-15429

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to launch cross-site scripting attacks or cause other unspecified attacks.

22887 - Google Chrome Multiple Vulnerabilities Prior To 63.0.3239.108

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-15429

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to launch cross-site scripting attacks or cause other unspecified attacks.

22892 - (K07369970) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6151

Description

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

Observation

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

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

22898 - WECON LeviStudio HMI Heap Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2017-16717

Description

A vulnerability is present in some versions of WECON LeviStudioU.

Observation

WECON LeviStudioU is an HMI programming software.

A vulnerability is present in some versions of WECON LeviStudioU. The flaw occurs due to a buffer overflow issue. Successful exploitation could allow an attacker to execute arbitrary code and cause a denial of service condition.

22906 - (MSPT-Jan2018) Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2018-0762)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0762

Description

A vulnerability in some versions of Microsoft Internet Explorer and Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer and Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22907 - (MSPT-Jan2018) Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2018-0772)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0772

Description

A vulnerability in some versions of Microsoft Internet Explorer and Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer and Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22908 - (MSPT-Jan2018) Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2018-0768)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0768

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22916 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0770)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0770

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22917 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0775)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0775

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22919 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0777)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0777

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22920 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0778)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0778

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22921 - (MSPT-Jan2018) Microsoft Windows IPSec Denial of Service (CVE-2018-0753)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0753

Description

A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

The flaw lies in the IPSec component. Successful exploitation by a remote attacker could result in a denial of service condition.

22922 - (MSPT-Jan2018) Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2018-0769)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0769

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22924 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution Vulnerability (CVE-2018-0773)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0773

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22925 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution Vulnerability (CVE-2018-0774)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0774

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22926 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution Vulnerability (CVE-2018-0781)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0781

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

22929 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Remote Code Execution Vulnerability(CVE-2018-0758)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-0758

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

130985 - Debian Linux 9.0 DSA-4074-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12877, CVE-2017-16546, CVE-2017-17499, CVE-2017-17504, CVE-2017-17879

Description

The scan detected that the host is missing the following update:
DSA-4074-1

Observation

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

http://www.debian.org/security/2017/dsa-4074

Debian 9.0
all
imagemagick_8:6.9.7.4+dfsg-11+deb9u4

146189 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3455-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2016-9841, CVE-2017-10281, CVE-2017-10285, CVE-2017-10293, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3455-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003557.html

SuSE SLES 12 SP3
x86_64
java-1_7_1-ibm-alsa-1.7.1_sr4.15-38.8.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.15-38.8.1
java-1_7_1-ibm-plugin-1.7.1_sr4.15-38.8.1
java-1_7_1-ibm-1.7.1_sr4.15-38.8.1

SuSE SLES 12 SP2
x86_64
java-1_7_1-ibm-alsa-1.7.1_sr4.15-38.8.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.15-38.8.1
java-1_7_1-ibm-plugin-1.7.1_sr4.15-38.8.1
java-1_7_1-ibm-1.7.1_sr4.15-38.8.1

146192 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3448-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3448-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00110.html

SuSE Linux 42.2
noarch
phpMyAdmin-4.7.7-33.12.1

SuSE Linux 42.3
noarch
phpMyAdmin-4.7.7-6.1

146193 - SuSE SLES 11 SP4 SUSE-SU-2017:3440-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10165, CVE-2016-9841, CVE-2017-10281, CVE-2017-10285, CVE-2017-10293, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3440-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003555.html

SuSE SLES 11 SP4
i586
java-1_7_1-ibm-alsa-1.7.1_sr4.15-26.8.1
java-1_7_1-ibm-plugin-1.7.1_sr4.15-26.8.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.15-26.8.1
java-1_7_1-ibm-1.7.1_sr4.15-26.8.1

x86_64
java-1_7_1-ibm-alsa-1.7.1_sr4.15-26.8.1
java-1_7_1-ibm-plugin-1.7.1_sr4.15-26.8.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.15-26.8.1
java-1_7_1-ibm-1.7.1_sr4.15-26.8.1

146195 - SuSE SLES 11 SP4 SUSE-SU-2018:0003-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16642, CVE-2017-9228, CVE-2017-9229

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:0003-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-January/003559.html

SuSE SLES 11 SP4
i586
php53-xmlwriter-5.3.17-112.10.1
php53-tokenizer-5.3.17-112.10.1
php53-pgsql-5.3.17-112.10.1
php53-gd-5.3.17-112.10.1
php53-suhosin-5.3.17-112.10.1
php53-dba-5.3.17-112.10.1
php53-pear-5.3.17-112.10.1
php53-iconv-5.3.17-112.10.1
php53-pcntl-5.3.17-112.10.1
php53-bcmath-5.3.17-112.10.1
php53-ftp-5.3.17-112.10.1
php53-xsl-5.3.17-112.10.1
apache2-mod_php53-5.3.17-112.10.1
php53-json-5.3.17-112.10.1
php53-gmp-5.3.17-112.10.1
php53-sysvshm-5.3.17-112.10.1
php53-soap-5.3.17-112.10.1
php53-wddx-5.3.17-112.10.1
php53-sysvmsg-5.3.17-112.10.1
php53-ctype-5.3.17-112.10.1
php53-fastcgi-5.3.17-112.10.1
php53-curl-5.3.17-112.10.1
php53-ldap-5.3.17-112.10.1
php53-mcrypt-5.3.17-112.10.1
php53-xmlrpc-5.3.17-112.10.1
php53-gettext-5.3.17-112.10.1
php53-xmlreader-5.3.17-112.10.1
php53-openssl-5.3.17-112.10.1
php53-pspell-5.3.17-112.10.1
php53-intl-5.3.17-112.10.1
php53-bz2-5.3.17-112.10.1
php53-odbc-5.3.17-112.10.1
php53-mysql-5.3.17-112.10.1
php53-calendar-5.3.17-112.10.1
php53-dom-5.3.17-112.10.1
php53-5.3.17-112.10.1
php53-zip-5.3.17-112.10.1
php53-shmop-5.3.17-112.10.1
php53-fileinfo-5.3.17-112.10.1
php53-pdo-5.3.17-112.10.1

php53-exif-5.3.17-112.10.1
php53-sysvsem-5.3.17-112.10.1
php53-snmp-5.3.17-112.10.1
php53-zlib-5.3.17-112.10.1
php53-mbstring-5.3.17-112.10.1

x86_64
php53-xmlwriter-5.3.17-112.10.1
php53-tokenizer-5.3.17-112.10.1
php53-pgsql-5.3.17-112.10.1
php53-gd-5.3.17-112.10.1
php53-suhosin-5.3.17-112.10.1
php53-dba-5.3.17-112.10.1
php53-pear-5.3.17-112.10.1
php53-iconv-5.3.17-112.10.1
php53-pcntl-5.3.17-112.10.1
php53-bcmath-5.3.17-112.10.1
php53-ftp-5.3.17-112.10.1
php53-xsl-5.3.17-112.10.1
apache2-mod_php53-5.3.17-112.10.1
php53-json-5.3.17-112.10.1
php53-gmp-5.3.17-112.10.1
php53-sysvshm-5.3.17-112.10.1
php53-soap-5.3.17-112.10.1
php53-wddx-5.3.17-112.10.1
php53-sysvmsg-5.3.17-112.10.1
php53-ctype-5.3.17-112.10.1
php53-fastcgi-5.3.17-112.10.1
php53-curl-5.3.17-112.10.1
php53-ldap-5.3.17-112.10.1
php53-mcrypt-5.3.17-112.10.1
php53-xmlrpc-5.3.17-112.10.1
php53-gettext-5.3.17-112.10.1
php53-xmlreader-5.3.17-112.10.1
php53-openssl-5.3.17-112.10.1
php53-pspell-5.3.17-112.10.1
php53-intl-5.3.17-112.10.1
php53-bz2-5.3.17-112.10.1
php53-odbc-5.3.17-112.10.1
php53-mysql-5.3.17-112.10.1
php53-calendar-5.3.17-112.10.1
php53-dom-5.3.17-112.10.1
php53-5.3.17-112.10.1
php53-zip-5.3.17-112.10.1
php53-shmop-5.3.17-112.10.1
php53-fileinfo-5.3.17-112.10.1
php53-pdo-5.3.17-112.10.1
php53-exif-5.3.17-112.10.1
php53-sysvsem-5.3.17-112.10.1
php53-snmp-5.3.17-112.10.1
php53-zlib-5.3.17-112.10.1
php53-mbstring-5.3.17-112.10.1

193131 - Fedora Linux 26 FEDORA-2017-16a414b3c5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15595, CVE-2017-17044, CVE-2017-17045, CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566

Description

The scan detected that the host is missing the following update:
FEDORA-2017-16a414b3c5

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/2018/1/?count=200&page=2

Fedora Core 26

xen-4.8.2-9.fc26

193132 - Fedora Linux 27 FEDORA-2017-2e5a17c4cc Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2e5a17c4cc

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/2018/1/?count=200&page=1

Fedora Core 27

python33-3.3.7-2.fc27

130984 - Debian Linux 8.0, 9.0 DSA-4076-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16671, CVE-2017-16672, CVE-2017-17090, CVE-2017-17664

Description

The scan detected that the host is missing the following update:
DSA-4076-1

Observation

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

http://www.debian.org/security/2017/dsa-4076

Debian 8.0
all
asterisk_1:11.13.1~dfsg-2+deb8u5

Debian 9.0
all
asterisk_1:13.14.1~dfsg-2+deb9u3

146190 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3442-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17531

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3442-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00108.html

SuSE Linux 42.2
x86_64
global-debuginfo-6.5.1-3.3.1
global-debugsource-6.5.1-3.3.1
global-6.5.1-3.3.1

i586
global-debuginfo-6.5.1-3.3.1
global-debugsource-6.5.1-3.3.1
global-6.5.1-3.3.1

SuSE Linux 42.3
x86_64
global-debugsource-6.5.1-6.1
global-debuginfo-6.5.1-6.1
global-6.5.1-6.1

i586
global-debugsource-6.5.1-6.1
global-debuginfo-6.5.1-6.1
global-6.5.1-6.1

193115 - Fedora Linux 27 FEDORA-2017-06b373d942 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13856, CVE-2017-13866, CVE-2017-13870, CVE-2017-7156

Description

The scan detected that the host is missing the following update:
FEDORA-2017-06b373d942

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

webkitgtk4-2.18.4-1.fc27

193118 - Fedora Linux 26 FEDORA-2017-80c6b4d3be Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17512

Description

The scan detected that the host is missing the following update:
FEDORA-2017-80c6b4d3be

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 26

sensible-utils-0.0.11-1.fc26

193119 - Fedora Linux 27 FEDORA-2017-fd9462d9ef Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17531

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fd9462d9ef

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

global-6.5.7-4.fc27

193125 - Fedora Linux 27 FEDORA-2017-2fab3f12c4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17512

Description

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

FEDORA-2017-2fab3f12c4

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

sensible-utils-0.0.11-1.fc27

22824 - Cisco NX-OS Software CLI Arbitrary File Read Vulnerability (cisco-sa-20171129-nxos6)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12338

Description

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

Observation

Cisco NX-OS is a network operating system.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the CLI. Successful exploitation could allow a local attacker to read the contents of arbitrary files.

22847 - Cisco NX-OS Software CLI Command Injection Vulnerability (cisco-sa-20171129-nxos7)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12339

Description

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

Observation

Cisco NX-OS is a network operating system .

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in CLI of Cisco NX-OS System Software. Successful exploitation could allow a local attacker to bypass the security restrictions.

22871 - Cisco Nexus Series Switches Open Agent Container Code Execution Vulnerability (cisco-sa-20171129-nxos9)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12342

Description

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

Observation

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

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in OAC feature. Successful exploitation could allow an attacker to execute arbitrary code.

22872 - Mozilla Firefox Multiple Vulnerabilities Prior To 57.0.1 (CVE-2017-7843)

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

Risk Level: Medium

CVE: CVE-2017-7843

Description

A vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox. The flaw occurs when Private Browsing mode is used. Successful exploitation could allow an attacker to bypass security restrictions and perform unauthorized actions.

22873 - Mozilla Firefox Multiple Vulnerabilities Prior To 57.0.1 (CVE-2017-7843)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-7843

Description

A vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox. The flaw occurs when Private Browsing mode is used. Successful exploitation could allow an attacker to bypass security restrictions and perform unauthorized actions.

22874 - Mozilla Firefox Multiple Vulnerabilities Prior To 57.0.1 (CVE-2017-7844)

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

Risk Level: Medium

CVE: CVE-2017-7844

Description

A vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox. The flaw lies in the SVG image. Successful exploitation could allow an attacker to obtain sensitive information and perform unauthorized actions.

22875 - Mozilla Firefox Multiple Vulnerabilities Prior To 57.0.1 (CVE-2017-7844)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-7844

Description

A vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A vulnerability is present in some versions of Mozilla Firefox. The flaw lies in the SVG image. Successful exploitation could allow an attacker to obtain sensitive information and perform unauthorized actions.

22880 - IBM WebSphere Application Server Multiple Java Vulnerabilities (swg22010560)

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

Risk Level: Medium

CVE: CVE-2017-10356, CVE-2017-10388

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server.

Observation

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

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaws lie in the IBM Java SDK component. Exploitation could allow a malicious unauthenticated user to obtain sensitive information or take control of the system.

22883 - IBM WebSphere Application Server Liberty Profile Multiple Java Vulnerabilities (swg22010560)

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

Risk Level: Medium

CVE: CVE-2017-10356, CVE-2017-10388

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server Liberty Profile.

Observation

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

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server Liberty Profile. The flaws lie in the IBM Java SDK component. Exploitation could allow a malicious unauthenticated user to obtain sensitive information or take control of the system.

22888 - IBM AIX OpenSSL Multiple Vulnerabilities (openssl_advisory24)

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

Risk Level: Medium

CVE: CVE-2017-3735

Description

A vulnerability is present in some versions of IBM AIX.

Observation

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

A vulnerability is present in some versions of IBM AIX. The flaw lies in OpenSSL. It could result in an incorrect text display of the certificate.

22889 - (CTX230624) Citrix XenServer Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

A vulnerability is present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

A vulnerability is present in some versions of Citrix XenServer. The flaw is due to unspecified issue. Successful exploitation could allow a malicious administrator of a guest VM to crash the host.

22890 - McAfee Security Scan Plus Arbitrary Command Execution Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-8026

Description

A vulnerability is present in some versions of McAfee Security Scan Plus.

Observation

McAfee Security Scan Plus is a free virus scan software.

A vulnerability is present in some versions of McAfee Security Scan Plus. The flaw is due to an unspecified local command-execution issue. Successful exploitation could allow an authenticated user to gain elevated privileges via unspecified vectors.

22893 - Atlassian Confluence Server Information Disclosure Vulnerability (CONFSERVER-52222)

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

Risk Level: Medium

CVE: CVE-2017-7415

Description

An information disclosure vulnerability is present in some versions of Atlassian Confluence Server.

Observation

Atlassian Confluence Server is a Java team-collaboration software.

An information disclosure vulnerability is present in some versions of Atlassian Confluence Server. The flaw lies in the drafts diff REST resource. Successful exploitation could allow an attacker to retrieve sensitive data from the target system.

22910 - (MSPT-Jan2018) Microsoft Windows ATMFD.dll Information Disclosure (CVE-2018-0754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0754

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the ATMFD.dll component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22911 - (MSPT-Jan2018) Microsoft Windows Color Management Information Disclosure (CVE-2018-0741)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0741

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Color Management component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22912 - (MSPT-Jan2018) Microsoft Windows SMB Server Privilege Escalation (CVE-2018-0749)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0749

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the SMB Server component.Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to have valid credentials to the vulnerable system.

22913 - (MSPT-Jan2018) Microsoft Windows GDI Information Disclosure (CVE-2018-0750)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0750

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the GDI component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to log on to an affected system and run a specially crafted application.

22914 - (MSPT-Jan2018) Microsoft Windows Subsystem for Linux Privilege Escalation (CVE-2018-0743)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0743

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Subsystem for Linux component.Successful exploitation could allow a local user to execute remote code with elevated privileges.

22915 - (MSPT-Jan2018) Microsoft Windows Kernel Information Disclosure (CVE-2018-0745)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0745

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Kernel component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

22927 - (MSPT-Jan2018) Microsoft Edge Elevation of Privilege Vulnerability (CVE-2018-0803)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0803

Description

A vulnerability in some versions of Microsoft Edge could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Edge could lead to privilege escalation.

The flaw lies in the Cross Domain Policy component. Successful exploitation by a remote attacker could result in privilege escalation. The exploit requires the user to open a vulnerable website, email or document.

22930 - (MSPT-Jan2018) Microsoft Edge Memory Handling Information Disclosure Vulnerability (CVE-2018-0766)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0766

Description

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

The flaw lies in a memory handling component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22931 - (MSPT-Jan2018) Microsoft Edge Scripting Engine Information Disclosure Vulnerability (CVE-2018-0767)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0767

Description

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22932 - (MSPT-Jan2018) Microsoft Windows OpenType Font Driver Elevation of Privilege Vulnerability (CVE-2018-0788)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0788

Description

A vulnerability in some versions of Microsoft Windows could lead to elevation of privilege.

Observation

A vulnerability in some versions of Microsoft Windows could lead to elevation of privilege.

The flaw lies in the ATMFD.dll component. Successful exploitation could allow an local attacker to execute arbitrary code and take control of an affected system.

22933 - (MSPT-Jan2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0744)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0744

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges.

22936 - (MSPT-Jan2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0748)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0748

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component.Successful exploitation could allow a local user to gain elevated privileges. The exploit requires a locally authenticated attacker to run a specially crafted application.

22937 - (MSPT-Jan2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0751)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0751

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component.Successful exploitation could allow a local user to gain elevated privileges.

22938 - (MSPT-Jan2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0752)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-0752

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component.Successful exploitation could allow a local user to gain elevated privileges.

146191 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3436-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17083, CVE-2017-17084, CVE-2017-17085

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3436-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003554.html

SuSE SLES 12 SP2
x86_64
libwiretap6-2.2.11-48.15.3
wireshark-gtk-debuginfo-2.2.11-48.15.3
libwsutil7-debuginfo-2.2.11-48.15.3
wireshark-gtk-2.2.11-48.15.3
libwscodecs1-2.2.11-48.15.3
libwsutil7-2.2.11-48.15.3
wireshark-debuginfo-2.2.11-48.15.3
libwscodecs1-debuginfo-2.2.11-48.15.3
wireshark-2.2.11-48.15.3
libwireshark8-debuginfo-2.2.11-48.15.3
libwiretap6-debuginfo-2.2.11-48.15.3
libwireshark8-2.2.11-48.15.3
wireshark-debugsource-2.2.11-48.15.3

SuSE SLED 12 SP3
x86_64
libwiretap6-2.2.11-48.15.3
wireshark-gtk-debuginfo-2.2.11-48.15.3
libwsutil7-debuginfo-2.2.11-48.15.3
wireshark-gtk-2.2.11-48.15.3
libwscodecs1-2.2.11-48.15.3
libwsutil7-2.2.11-48.15.3
wireshark-debuginfo-2.2.11-48.15.3
libwscodecs1-debuginfo-2.2.11-48.15.3
wireshark-2.2.11-48.15.3

libwireshark8-debuginfo-2.2.11-48.15.3
libwiretap6-debuginfo-2.2.11-48.15.3
libwireshark8-2.2.11-48.15.3
wireshark-debugsource-2.2.11-48.15.3

SuSE SLED 12 SP2
x86_64
libwiretap6-2.2.11-48.15.3
wireshark-gtk-debuginfo-2.2.11-48.15.3
libwsutil7-debuginfo-2.2.11-48.15.3
wireshark-gtk-2.2.11-48.15.3
libwscodecs1-2.2.11-48.15.3
libwsutil7-2.2.11-48.15.3
wireshark-debuginfo-2.2.11-48.15.3
libwscodecs1-debuginfo-2.2.11-48.15.3
wireshark-2.2.11-48.15.3
libwireshark8-debuginfo-2.2.11-48.15.3
libwiretap6-debuginfo-2.2.11-48.15.3
libwireshark8-2.2.11-48.15.3
wireshark-debugsource-2.2.11-48.15.3

SuSE SLES 12 SP3
x86_64
libwiretap6-2.2.11-48.15.3
wireshark-gtk-debuginfo-2.2.11-48.15.3
libwsutil7-debuginfo-2.2.11-48.15.3
wireshark-gtk-2.2.11-48.15.3
libwscodecs1-2.2.11-48.15.3
libwsutil7-2.2.11-48.15.3
wireshark-debuginfo-2.2.11-48.15.3
libwscodecs1-debuginfo-2.2.11-48.15.3
wireshark-2.2.11-48.15.3
libwireshark8-debuginfo-2.2.11-48.15.3
libwiretap6-debuginfo-2.2.11-48.15.3
libwireshark8-2.2.11-48.15.3
wireshark-debugsource-2.2.11-48.15.3

193114 - Fedora Linux 26 FEDORA-2017-bf172b2035 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000211

Description

The scan detected that the host is missing the following update:
FEDORA-2017-bf172b2035

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 26

lynx-2.8.9-0.20.dev16.fc26

193129 - Fedora Linux 27 FEDORA-2017-66e9367f7e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17090

Description

The scan detected that the host is missing the following update:
FEDORA-2017-66e9367f7e

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

asterisk-14.7.4-1.fc27

22879 - Cisco Jabber Clients Cross-Site Scripting Vulnerability (cisco-sa-20171129-jabber)

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

Risk Level: Medium

CVE: CVE-2017-12356

Description

A cross-site scripting vulnerability is present in some versions of Cisco Jabber.

Observation

Cisco Jabber is Cisco unified communication software solution.

A cross-site scripting vulnerability is present in some versions of Cisco Jabber. The flaw lies in the web-based management interface of Cisco Jabber. Successful exploitation could allow an attacker to execute remote code.

22885 - (K14363514) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-3736

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 obtain sensitive information.

182566 - FreeBSD The Bouncy Castle Crypto APIs: CVE-2017-13098 ("ROBOT") (6a131fbf-ec76-11e7-aa65-001b216d295b)

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

Risk Level: Medium

CVE: CVE-2017-13098

Description

The scan detected that the host is missing the following update:
The Bouncy Castle Crypto APIs: CVE-2017-13098 ("ROBOT") (6a131fbf-ec76-11e7-aa65-001b216d295b)

Observation

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

http://www.vuxml.org/freebsd/6a131fbf-ec76-11e7-aa65-001b216d295b.html

Affected packages:
bouncycastle15 < 1.59

193120 - Fedora Linux 26 FEDORA-2017-7b4149911a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15612, CVE-2017-16876

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7b4149911a

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

python-mistune-0.8.3-1.fc26

193121 - Fedora Linux 27 FEDORA-2017-2eefd424bd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15612, CVE-2017-16876

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2eefd424bd

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

python-mistune-0.8.3-1.fc27

193122 - Fedora Linux 26 FEDORA-2017-38fbcdffc3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17664

Description

The scan detected that the host is missing the following update:
FEDORA-2017-38fbcdffc3

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 26

asterisk-13.18.4-1.fc26

193123 - Fedora Linux 26 FEDORA-2017-d6402c8005 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000159

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d6402c8005

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 26

evince-3.24.2-2.fc26

130982 - Debian Linux 8.0, 9.0 DSA-4077-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17784, CVE-2017-17785, CVE-2017-17786, CVE-2017-17787, CVE-2017-17788, CVE-2017-17789

Description

The scan detected that the host is missing the following update:
DSA-4077-1

Observation

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

http://www.debian.org/security/2017/dsa-4077

Debian 8.0
all
gimp_2.8.14-1+deb8u2

Debian 9.0
all
gimp_2.8.18-1+deb9u1

130983 - Debian Linux 9.0 DSA-4075-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7829, CVE-2017-7830, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

Description

The scan detected that the host is missing the following update:
DSA-4075-1

Observation

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

http://www.debian.org/security/2017/dsa-4075

Debian 9.0
all
thunderbird_1:52.5.2-2~deb9u1

146188 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3447-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3447-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2017-12/msg00109.html

SuSE Linux 42.2
i586
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-7.6.1
gdk-pixbuf-debugsource-2.34.0-7.6.1
libgdk_pixbuf-2_0-0-2.34.0-7.6.1
gdk-pixbuf-devel-debuginfo-2.34.0-7.6.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-7.6.1

gdk-pixbuf-query-loaders-2.34.0-7.6.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-7.6.1
gdk-pixbuf-devel-2.34.0-7.6.1

noarch
gdk-pixbuf-lang-2.34.0-7.6.1

x86_64
gdk-pixbuf-query-loaders-2.34.0-7.6.1
gdk-pixbuf-devel-debuginfo-32bit-2.34.0-7.6.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-7.6.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-7.6.1
gdk-pixbuf-debugsource-2.34.0-7.6.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-7.6.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-7.6.1
libgdk_pixbuf-2_0-0-2.34.0-7.6.1
gdk-pixbuf-query-loaders-32bit-2.34.0-7.6.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-7.6.1
gdk-pixbuf-devel-debuginfo-2.34.0-7.6.1
gdk-pixbuf-devel-2.34.0-7.6.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-7.6.1
gdk-pixbuf-devel-32bit-2.34.0-7.6.1

SuSE Linux 42.3
i586
gdk-pixbuf-devel-debuginfo-2.34.0-13.1
gdk-pixbuf-debugsource-2.34.0-13.1
libgdk_pixbuf-2_0-0-2.34.0-13.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-13.1
gdk-pixbuf-devel-2.34.0-13.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-13.1
gdk-pixbuf-query-loaders-2.34.0-13.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-13.1

noarch
gdk-pixbuf-lang-2.34.0-13.1

x86_64
gdk-pixbuf-query-loaders-debuginfo-2.34.0-13.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-13.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-13.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-13.1
gdk-pixbuf-query-loaders-2.34.0-13.1
gdk-pixbuf-devel-debuginfo-32bit-2.34.0-13.1
gdk-pixbuf-devel-32bit-2.34.0-13.1
gdk-pixbuf-devel-debuginfo-2.34.0-13.1
gdk-pixbuf-query-loaders-32bit-2.34.0-13.1
gdk-pixbuf-debugsource-2.34.0-13.1
gdk-pixbuf-devel-2.34.0-13.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-13.1
libgdk_pixbuf-2_0-0-2.34.0-13.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-13.1

146194 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3441-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3441-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003556.html

SuSE SLES 12 SP2
noarch
gdk-pixbuf-lang-2.34.0-19.8.1

x86_64
gdk-pixbuf-query-loaders-32bit-2.34.0-19.8.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-19.8.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-19.8.1
gdk-pixbuf-debugsource-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-2.34.0-19.8.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-19.8.1
gdk-pixbuf-query-loaders-2.34.0-19.8.1

SuSE SLED 12 SP3
x86_64
gdk-pixbuf-query-loaders-32bit-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-19.8.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-19.8.1
gdk-pixbuf-debugsource-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-2.34.0-19.8.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-19.8.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-19.8.1
gdk-pixbuf-query-loaders-2.34.0-19.8.1

noarch
gdk-pixbuf-lang-2.34.0-19.8.1

SuSE SLED 12 SP2
x86_64
gdk-pixbuf-query-loaders-32bit-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-19.8.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-19.8.1
gdk-pixbuf-debugsource-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-2.34.0-19.8.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-19.8.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-19.8.1
gdk-pixbuf-query-loaders-2.34.0-19.8.1

noarch
gdk-pixbuf-lang-2.34.0-19.8.1

SuSE SLES 12 SP3

noarch
gdk-pixbuf-lang-2.34.0-19.8.1

x86_64
gdk-pixbuf-query-loaders-32bit-2.34.0-19.8.1
gdk-pixbuf-query-loaders-debuginfo-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-debuginfo-32bit-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-debuginfo-2.34.0-19.8.1
typelib-1_0-GdkPixbuf-2_0-2.34.0-19.8.1
gdk-pixbuf-debugsource-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-2.34.0-19.8.1
gdk-pixbuf-query-loaders-debuginfo-32bit-2.34.0-19.8.1
libgdk_pixbuf-2_0-0-32bit-2.34.0-19.8.1
gdk-pixbuf-query-loaders-2.34.0-19.8.1

193116 - Fedora Linux 27 FEDORA-2017-54288fb74e 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-2017-54288fb74e

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

thunderbird-enigmail-1.9.9-1.fc27

193117 - Fedora Linux 26 FEDORA-2017-1dc71e1acd 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-2017-1dc71e1acd

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 26

shellinabox-2.20-5.fc26

193124 - Fedora Linux 27 FEDORA-2017-a95dd74301 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-2017-a95dd74301

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

shellinabox-2.20-5.fc27

193126 - Fedora Linux 26 FEDORA-2017-856a149a4c 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-2017-856a149a4c

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

thunderbird-enigmail-1.9.9-1.fc26

193127 - Fedora Linux 27 FEDORA-2017-b24ef59f94 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6328

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b24ef59f94

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

libexif-0.6.21-14.fc27

193130 - Fedora Linux 27 FEDORA-2017-cad79c7c6c 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-2017-cad79c7c6c

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/2018/1/?count=200&page=1

Fedora Core 27

phpMyAdmin-4.7.7-1.fc27

193133 - Fedora Linux 27 FEDORA-2017-c2645aa935 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427, CVE-2017-15429

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c2645aa935

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/2018/1/?count=200&page=2

Fedora Core 27

chromium-63.0.3239.108-1.fc27

193134 - Fedora Linux 26 FEDORA-2017-481515e199 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-2017-481515e199

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/2018/1/?count=200&page=2

Fedora Core 26

phpMyAdmin-4.7.7-1.fc26

193135 - Fedora Linux 27 FEDORA-2017-828f8a8fc6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000408, CVE-2017-1000409

Description

The scan detected that the host is missing the following update:
FEDORA-2017-828f8a8fc6

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/2018/1/?count=200&page=1

Fedora Core 27

glibc-2.26-21.fc27

193136 - Fedora Linux 26 FEDORA-2017-ea44f172e3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-15398, CVE-2017-15399, CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427, CVE-2017-15429, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ea44f172e3

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/2018/1/?count=200&page=2

Fedora Core 26

chromium-63.0.3239.108-1.fc26

22934 - (MSPT-Jan2018) Microsoft Windows Information Disclosure Vulnerability (CVE-2018-0746)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2018-0746

Description

An information disclosure vulnerability is present in some versions of Microsoft Windows.

Observation

Windows is a popular operating system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows kernel handles memory address. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

22935 - (MSPT-Jan2018) Windows Information Disclosure Vulnerability (CVE-2018-0747)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2018-0747

Description

An information disclosure vulnerability is present in some versions of Microsoft Windows.

Observation

Windows is a popular operating system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows kernel handles memory address. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

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.

22742 - (APSB17-33) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2017-11213, CVE-2017-11215, CVE-2017-11225, CVE-2017-3112, CVE-2017-3114

Update Details

Risk is updated

22743 - (APSB17-33) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-11213, CVE-2017-11215, CVE-2017-11225, CVE-2017-3112, CVE-2017-3114

Update Details

Risk is updated

141778 - Red Hat Enterprise Linux RHSA-2017-3222 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11213, CVE-2017-11215, CVE-2017-11225, CVE-2017-3112, CVE-2017-3114

Update Details

Risk is updated

146164 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3355-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17458

Update Details

Risk is updated

182523 - FreeBSD Flash Player Multiple Vulnerabilities (52f10525-caff-11e7-b590-6451062f0f7a)

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

Risk Level: High

CVE: CVE-2017-11213, CVE-2017-11215, CVE-2017-11225, CVE-2017-3112, CVE-2017-3114

Update Details

Risk is updated

22856 - (HT208331) Apple macOS Multiple Vulnerabilities Prior To 10.13.2

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000254, CVE-2017-10140, CVE-2017-13833, CVE-2017-13844, CVE-2017-13847, CVE-2017-13848, CVE-2017-13855, CVE-2017-13858, CVE-2017-13860, CVE-2017-13862, CVE-2017-13865, CVE-2017-13867, CVE-2017-13868, CVE-2017-13869, CVE-2017-13871, CVE-2017-13872, CVE-2017-13875, CVE-2017-13876, CVE-2017-13878, CVE-2017-13883, CVE-2017-3735, CVE-2017-9798

Update Details

CVE is updated

22861 - Microsoft Office 2016 Click-To-Run December 2017 Updates

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

Risk Level: High

CVE: CVE-2017-11934, CVE-2017-11935, CVE-2017-11939

Update Details

Risk is updated

88906 - Slackware Linux 14.2 SSA:2017-353-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17405

Update Details

Risk is updated

130958 - Debian Linux 8.0, 9.0 DSA-4052-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14176

Update Details

Risk is updated

130975 - Debian Linux 8.0, 9.0 DSA-4066-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16854, CVE-2017-16921

Update Details

Risk is updated

146158 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3271-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17459

Update Details

Risk is updated

182559 - FreeBSD ruby Command Injection Vulnerability In Net::FTP (dd644964-e10e-11e7-8097-0800271d4b9c)

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

Risk Level: High

CVE: CVE-2017-17405

Update Details

Risk is updated

88900 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-332-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14746, CVE-2017-15275

Update Details
Risk is updated

96041 - Fedora Linux 27 FEDORA-2017-791c5d52be Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14746, CVE-2017-15275

Update Details
Risk is updated

130952 - Debian Linux 8.0, 9.0 DSA-4043-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14746, CVE-2017-15275

Update Details
Risk is updated

130973 - Debian Linux 8.0, 9.0 DSA-4067-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-17432

Update Details
Risk is updated

182562 - FreeBSD rsync Multiple Vulnerabilities (72fff788-e561-11e7-8097-0800271d4b9c)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-16548, CVE-2017-17433, CVE-2017-17434

Update Details
FASLScript is updated

185966 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3486-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-14746, CVE-2017-15275

Update Details

Risk is updated

192997 - Fedora Linux 26 FEDORA-2017-366046c758 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Update Details

Risk is updated

193099 - Fedora Linux 26 FEDORA-2017-ba6b6e71f7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-8824

Update Details

Risk is updated

193107 - Fedora Linux 27 FEDORA-2017-129969aa8a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-8824

Update Details

Risk is updated

22876 - (HT208328) Apple iCloud Vulnerabilities Prior To 7.2

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

Risk Level: Medium

CVE: CVE-2017-13856, CVE-2017-13864, CVE-2017-13866, CVE-2017-13870, CVE-2017-7156, CVE-2017-7157

Update Details

Risk is updated

130961 - Debian Linux 8.0, 9.0 DSA-4054-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8819, CVE-2017-8820, CVE-2017-8821, CVE-2017-8822, CVE-2017-8823

Update Details

Risk is updated

130981 - Debian Linux 8.0, 9.0 DSA-4071-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17512

Update Details

Risk is updated

146116 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3203-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8819, CVE-2017-8820, CVE-2017-8821, CVE-2017-8822, CVE-2017-8823

Update Details

Risk is updated

182550 - FreeBSD node.js Data Confidentiality/Integrity Vulnerability, December 2017 (bea84a7a-e0c9-11e7-b4f3-11baa0c2df21)

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

Risk Level: Medium

CVE: CVE-2017-15896, CVE-2017-15897, CVE-2017-3738

Update Details

Risk is updated

182554 - FreeBSD global Gozilla Vulnerability (48cca164-e269-11e7-be51-6599c735afc8)

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

Risk Level: Medium

CVE: CVE-2017-17531

Update Details

Risk is updated

193004 - Fedora Linux 26 FEDORA-2017-9ea11e444d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000405

Update Details

Risk is updated

193018 - Fedora Linux 27 FEDORA-2017-b0c1f44130 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000405

Update Details

Risk is updated

193090 - Fedora Linux 26 FEDORA-2017-bce9e03721 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-8819, CVE-2017-8820, CVE-2017-8821, CVE-2017-8822, CVE-2017-8823

Update Details
Risk is updated

193095 - Fedora Linux 27 FEDORA-2017-bc2edc421d Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-8819, CVE-2017-8820, CVE-2017-8821, CVE-2017-8822, CVE-2017-8823

Update Details
Risk is updated

193111 - Fedora Linux 27 FEDORA-2017-f7cb245861 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17712

Update Details
Risk is updated

193112 - Fedora Linux 26 FEDORA-2017-7810b7c59f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17712, CVE-2017-17741

Update Details
Risk is updated

130654 - Debian Linux 8.0 DSA-3741-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-1254

Update Details
Risk is updated

130954 - Debian Linux 8.0 DSA-4046-1 Update Is Not Installed

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

CVE: CVE-2017-8028

Update Details

Risk is updated

130971 - Debian Linux 9.0 DSA-4055-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17439

Update Details

Risk is updated

145139 - SuSE Linux 13.2 openSUSE-SU-2016:3281-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1254

Update Details

Risk is updated

146150 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3268-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17439

Update Details

Risk is updated

182497 - FreeBSD irssi Multiple Vulnerabilities (85e2c7eb-b74b-11e7-8546-5cf3fcfdd1f1)

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

Risk Level: Medium

CVE: CVE-2017-15227, CVE-2017-15228, CVE-2017-15721, CVE-2017-15722, CVE-2017-15723

Update Details

FASLScript is updated

182534 - FreeBSD asterisk DOS Vulnerability In Asterisk Chan_skinny (e91cf90c-d6dd-11e7-9d10-001999f8d30b)

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

Risk Level: Medium

CVE: CVE-2017-17090

Update Details

Risk is updated

182551 - FreeBSD tor Use-after-free In Onion Service V2 (36ef8753-d86f-11e7-ad28-0025908740c2)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-8819

Update Details
Risk is updated

191564 - Fedora Linux 24 FEDORA-2016-76b646637e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-1254

Update Details
Risk is updated

191574 - Fedora Linux 25 FEDORA-2016-95b4e9077e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-1254

Update Details
Risk is updated

193037 - Fedora Linux 27 FEDORA-2017-386e856a4f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17042

Update Details
Risk is updated

193048 - Fedora Linux 25 FEDORA-2017-ca05b30e86 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17042

Update Details
Risk is updated

193060 - Fedora Linux 26 FEDORA-2017-c6c6e9beae Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17042

Update Details

Risk is updated

88904 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-342-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3737, CVE-2017-3738

Update Details
Risk is updated

130646 - Debian Linux 8.0 DSA-3733-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-1252

Update Details
Risk is updated

130963 - Debian Linux 8.0, 9.0 DSA-4057-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000385

Update Details
Risk is updated

130974 - Debian Linux 9.0 DSA-4065-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3737, CVE-2017-3738

Update Details
Risk is updated

130979 - Debian Linux 9.0 DSA-4072-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-13098

Update Details
Risk is updated

146168 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3343-1 Update Is Not Installed

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

CVE: CVE-2017-3737, CVE-2017-3738

Update Details

Risk is updated

146173 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3345-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3737, CVE-2017-3738

Update Details

Risk is updated

182516 - FreeBSD roundcube File Disclosure Vulnerability (f622608c-c53c-11e7-a633-009c02a2ab30)

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

Risk Level: Medium

CVE: CVE-2017-16651

Update Details

FASLScript is updated

182540 - FreeBSD OpenSSL Multiple Vulnerabilities (3bb451fc-db64-11e7-ac58-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-3737, CVE-2017-3738

Update Details

Risk is updated

185521 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3156-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1252

Update Details

Risk is updated

186006 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3503-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000159

Update Details

Risk is updated

186011 - Ubuntu Linux 16.04, 17.04, 17.10 USN-3512-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3737, CVE-2017-3738

Update Details
Risk is updated

193070 - Fedora Linux 27 FEDORA-2017-9e6df1e099 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000385

Update Details
Risk is updated

193075 - Fedora Linux 26 FEDORA-2017-93b6236635 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-1000385

Update Details
Risk is updated

193088 - Fedora Linux 26 FEDORA-2017-0f3270406c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17440

Update Details
Risk is updated

193101 - Fedora Linux 27 FEDORA-2017-354b9647ba Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-17440

Update Details
Risk is updated

88903 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-333-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Low
CVE: CVE-2017-16611

Update Details

Risk is updated

182558 - FreeBSD libXfont Permission Bypass When Opening Files Through Symlinks (08a125f3-e35a-11e7-a293-54e1ad3d6335)

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

Risk Level: Low

CVE: CVE-2017-16611

Update Details

Risk is updated

186000 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3500-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16611

Update Details

Risk is updated

70014 - netbios-helpers.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.