2017-OCT-16
FSL version 7.5.967

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

22547 - Cisco IOS Software DHCP Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-12240

Description

A remote code execution vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A remote code execution vulnerability is present in some versions of Cisco IOS. The flaw lies in the DHCP relay subsystem. Successful exploitation could allow a remote attacker to run arbitrary code on the system or to cause a denial of service condition.

22585 - (K82747025) F5 BIG-IP Graphicsmagick Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5118

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 WebAcceleration profile configured with the Image Optimization settings. Successful exploitation could allow a remote attacker to execute arbitrary code on target system.

22576 - (HT208144) Apple macOS Multiple Vulnerabilities Prior To 10.13

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

Risk Level: High

CVE: CVE-2016-9042, CVE-2016-9063, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2017-0381, CVE-2017-1000373, CVE-2017-10989, CVE-2017-11103, CVE-2017-6451, CVE-2017-6452, CVE-2017-6455, CVE-2017-6458, CVE-2017-6459, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464, CVE-2017-7074, CVE-2017-7077, CVE-2017-7078, CVE-2017-7080, CVE-2017-7082, CVE-2017-7083, CVE-2017-7084, CVE-2017-7086, CVE-2017-7114, CVE-2017-7119, CVE-2017-7121, CVE-2017-7122, CVE-2017-7123, CVE-2017-7124, CVE-2017-7125, CVE-2017-7126, CVE-2017-7127, CVE-2017-7128, CVE-2017-7129, CVE-2017-7130, CVE-2017-7138, CVE-2017-7141, CVE-2017-7143, CVE-2017-9233

Description

Multiple vulnerabilities are present in some versions of Apple macOS.

Observation

Apple macOS is the operating system developed by Apple.

Multiple vulnerabilities are present in some versions of Apple macOS. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or remotely execute arbitrary code on the target system.

22607 - (APSB17-32) Vulnerability In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2017-11292

Description

A vulnerability is present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

A vulnerability is present in some versions of Adobe Flash Player. The flaw is due to a type confusion issue. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

The update provided by Adobe bulletin APSB17-32 resolves the issue. The target system is missing this update.

22608 - (APSB17-32) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-11292

Description

A vulnerability is present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

A vulnerability is present in some versions of Adobe Flash Player. The flaw is due to a type confusion issue. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

The update provided by Adobe bulletin APSB17-32 resolves the issue. The target system is missing this update.

22482 - (VMSA-2017-0015.2) VMware Fusion Out Of Bounds Write Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4924

Description

A vulnerability present in some versions of VMware Fusion.

Observation

VMware Fusion is a popular virtualization platform.

A vulnerability present in some versions of VMware Fusion. The flaw is related with the SVGA device. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

22528 - (HT208142) Apple iCloud Vulnerabilities Prior To 7.0

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

Risk Level: High

CVE: CVE-2017-7081, CVE-2017-7087, CVE-2017-7089, CVE-2017-7090, CVE-2017-7091, CVE-2017-7092, CVE-2017-7093, CVE-2017-7094, CVE-2017-7095, CVE-2017-7096, CVE-2017-7098, CVE-2017-7099, CVE-2017-7100, CVE-2017-7102, CVE-2017-7104, CVE-2017-7106, CVE-2017-7107, CVE-2017-7109, CVE-2017-7111, CVE-2017-7117, CVE-2017-7120, CVE-2017-7127

Description

Multiple vulnerabilities are present in some versions of Apple iCloud.

Observation

Apple iCloud is a manager for the Apple's cloud-based storage service.

Multiple vulnerabilities are present in some versions of Apple iCloud. The flaw lies in WebKit and SQLite components. Successful exploitation could allow an attacker to execute remote arbitrary code, cause cross site scripting or obtain sensitive information.

22566 - Mozilla Firefox Multiple Vulnerabilities Prior To 56

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

Risk Level: High

CVE: CVE-2017-7793, CVE-2017-7805, CVE-2017-7810, CVE-2017-7811, CVE-2017-7812, CVE-2017-7813, CVE-2017-7814, CVE-2017-7815, CVE-2017-7816, CVE-2017-7818, CVE-2017-7819, CVE-2017-7820, CVE-2017-7821, CVE-2017-7822, CVE-2017-7823, CVE-2017-7824, CVE-2017-7825

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, conduct spoofing attacks, retrieve sensitive data, remotely execute arbitrary code on the target system or cause a denial of service condition.

22567 - Mozilla Firefox Multiple Vulnerabilities Prior To 56

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-7793, CVE-2017-7805, CVE-2017-7810, CVE-2017-7811, CVE-2017-7812, CVE-2017-7813, CVE-2017-7814, CVE-2017-7815, CVE-2017-7816, CVE-2017-7818, CVE-2017-7819, CVE-2017-7820, CVE-2017-7821, CVE-2017-7822, CVE-2017-7823, CVE-2017-7824, CVE-2017-7825

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, conduct spoofing attacks, retrieve sensitive data, remotely execute arbitrary code on the target system or cause a denial of service condition.

22583 - NVIDIA GeForce Experience Vulnerability 09-2017

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

Risk Level: High

CVE: CVE-2017-6266, CVE-2017-6267, CVE-2017-6268, CVE-2017-6269, CVE-2017-6270, CVE-2017-6271, CVE-2017-6272, CVE-2017-6277

Description

Multiple vulnerabilities are present in some versions of the NVIDIA GeForce Experience.

Observation

NVIDIA is a technology company which manufactures graphics processing units.

Multiple vulnerabilities are present in some versions of the NVIDIA GeForce Experience. The flaws occur within the kernel mode layer. Successful exploitation could allow an attacker to escalate privileges or cause a denial of service condition.

22590 - Cisco IOS Software Internet Key Exchange Denial Of Service Vulnerability

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

Risk Level: High

CVE: CVE-2017-12237

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw lies in the Internet Key Exchange Version 2 (IKEv2) module. Successful exploitation could allow a remote attacker to cause a denial of service condition.

22594 - Cisco IOS Software Network Address Translation Denial Of Service Vulnerability (CSCvc57217)

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

Risk Level: High

CVE: CVE-2017-12231

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 occurs due to improper handling of H.323 messages. Successful exploitation by a remote attacker could result in a denial of service condition.

22595 - Apache Tomcat Vulnerability Prior To 8.0.47

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

Risk Level: High

CVE: CVE-2017-12617

Description

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

Observation

Apache Tomcat is a container for the Java Servlet and Java Server Pages Web applications.

A remote code vulnerability is present in some versions of Apache Tomcat. The flaw is due to insufficient validation of user input. Successful exploitation could allow an attacker to execute remote code on the target system.

22602 - Apache Tomcat Vulnerability Prior To 9.0.1

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

Risk Level: High

CVE: CVE-2017-12617

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is a container for the Java Servlet and Java Server Pages Web applications.

A vulnerability is present in some versions of Apache Tomcat. The flaw lies in how the software handles HTTP PUT requests. Successful exploitation could allow an attacker to upload a specially crafter JSP file and execute remote code.

22529 - (CTX227928) Citrix NetScaler ADC Authentication Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-14602

Description

A vulnerability is present in some versions of Citrix NetScaler.

Observation

Citrix NetScaler is a widely used product that helps enterprises to protect, control and improve their services.

A vulnerability is present in some versions of Citrix NetScaler. The flaw lies in the management interface. Successful exploitation could allow an attacker to escalate privileges.

22556 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.4

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

Risk Level: Medium

CVE: CVE-2017-7793, CVE-2017-7814, CVE-2017-7818, CVE-2017-7823, CVE-2017-7824, CVE-2017-7825

Description

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

Observation

Mozilla Firefox ESR is a popular web browser.

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

22557 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.4

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-7793, CVE-2017-7814, CVE-2017-7818, CVE-2017-7823, CVE-2017-7824, CVE-2017-7825

Description

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

Observation

Mozilla Firefox ESR is a popular web browser.

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

22579 - Novell iManager Vulnerability Prior To 3.0.4

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

Risk Level: Medium

CVE: CVE-2016-9276

Description

A vulnerability is present in some versions of Novell (NetIQ) iManager.

Observation

Novell iManager is a web-based administration console.

A vulnerability is present in some versions of Novell (NetIQ) iManager. The flaw lies in Libdwarf. Successful exploitation could allow an attacker to cause a denial of service.

22588 - IBM WebSphere Portal Path Traversal Vulnerability (swg22008586)

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

Risk Level: Medium

CVE: CVE-2017-1577

Description

A path traversal vulnerability is present in some versions of IBM WebSphere Portal.

Observation

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

A path traversal vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in directory-traversal sequences. Successful exploitation could allow a remote attacker to disclose sensitive information.

22589 - (K08440897) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-0774

Description

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

Observation

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

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

22599 - Cisco IOS Software Plug-and-Play PKI API Certificate Validation Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-12228

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.

22580 - Cisco IOS Catalyst 6800 Series Switches VPLS Denial of Service Vulnerability

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

Risk Level: Low

CVE: CVE-2017-12238

Description

A vulnerability is present in some versions of Cisco IOS used in Cisco Catalyst Switches.

Observation

Cisco IOS is an operating system used in Cisco device.

A vulnerability is present in some versions of Cisco IOS used in Cisco Catalyst Switches. The vulnerability is due to a memory management issue. Successful exploitation could allow an adjacent attacker to cause a denial of service condition.

22598 - (VMSA-2017-0015.2) VMware Fusion NULL Pointer Dereference Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2017-4925

Description

A vulnerability is present in some versions of VMware Fusion.

Observation

VMware Fusion is a popular virtualization platform.

A vulnerability is present in some versions of VMware Fusion. The flaw lies in how guest RPC requests are handled. Successful exploitation could allow an attacker to cause a denial of service condition.

14519 - Cisco IOS Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

An obsolete version of Cisco IOS is detected on the target.

Observation

Cisco IOS is an industry-standard router OS developed by Cisco Systems.

An obsolete version of Cisco IOS is detected on the target. The vendor no longer provides support or patches for obsolete versions of the product. Use of vulnerable obsolete software may expose the target system to malicious attacks.

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.

913 - CSSearch Remote Command Execution

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

Risk Level: High

CVE: CVE-2002-0495, CVE-2002-1750

Update Details

FASLScript is updated

14411 - PHP Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14412 - Fedora Obsolete Version Detection

Category: SSH Module -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14413 - VMware ESX Obsolete Version Detection

Category: SSH Module -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14506 - Adobe Acrobat Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14541 - HP Systems Insight Manager Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14917 - Adobe ColdFusion Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

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.