2017-OCT-17
FSL version 7.5.968

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

22614 - Windows Wireless WPA Group Key Reinstallation Vulnerability (CVE-2017-13080)

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

Risk Level: High

CVE: CVE-2017-13080

Description

A vulnerability is present in some versions of Microsoft Windows.

Observation

Windows is a popular operating system developed by Microsoft.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Windows implementation of wireless networking. Successful exploitation could allow an attacker to inspect and intercept traffic between the target computer and wireless access point.

22596 - Cisco ASA Software Direct Authentication Denial Of Service Vulnerability (CSCvd59063)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-12246

Description

A vulnerability is present in some versions of Cisco Adaptive Security Appliance (ASA).

Observation

Cisco Adaptive Security Appliance is a firewall device.

A vulnerability is present in some versions of Cisco Adaptive Security Appliance (ASA). The flaw lies in the implementation of the direct authentication feature. Successful exploitation could allow an attacker to cause a denial of service condition.

22600 - Novell eDirectory Multiple Vulnerabilities Prior To 9.0.4

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2009-3555, CVE-2017-9277, CVE-2017-9285

Description

Multiple vulnerabilities are present in some versions of Novell (NetIQ) eDirectory.

Observation

Novell (NetIQ) eDirectory is an X.500 compatible directory service software for centrally managing access to network resources.

Multiple vulnerabilities are present in some versions of Novell (NetIQ) eDirectory. The flaws lie in multiple components. Successful exploitation could allow a malicious user to cause a denial-of-service or other unspecified impact.

22601 - Apache Tomcat Vulnerability Prior To 7.0.82

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 is related with the use of the HTTP PUT request. Successful exploitation could allow an attacker to execute remote code on the target system.

22584 - Cisco IOS ISG G2 Denial Of Service Vulnerability (CSCvc03809)

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

Risk Level: Medium

CVE: CVE-2017-12232

Description

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

Observation

Cisco IOS is an operating system used in Cisco device.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw lies in the ISR G2 Routers running this software, and is due to a misclassification of Ethernet frames. Successful exploitation could allow an attacker to cause a denial of service condition.

22603 - (K53084033) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2016-2178

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 many components. Successful exploitation could allow a local attacker to gain sensitive information.

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.