2015-NOV-12
FSL version 7.5.762

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

19201 - (JSA10703) Juniper Junos PFE Daemon Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-7749

Description

A vulnerability in some versions of Juniper Junos could lead to a denial of service.

Observation

A vulnerability in some versions of Juniper Junos could lead to a denial of service.

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

19198 - (SB10139) McAfee ePO Multiple Java Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-2601, CVE-2015-2613, CVE-2015-2625, CVE-2015-4748, CVE-2015-4749

Description

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator.

Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator. The flaws lie in the Java components. Successful exploitation could allow an attacker to disclose information or cause a denial of service condition.

19276 - Joomla SQL Injection Vulnerabilities (20151001)

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

Risk Level: High

CVE: CVE-2015-7297, CVE-2015-7857, CVE-2015-7858

Description

Multiple SQL injection vulnerabilities are present in some versions of Joomla!.

Observation

Joomla! is a content management system.

Multiple SQL injection vulnerabilities are present in some versions of Joomla!. The flaws are due to inadequate checking of input values within multiple components. Successful exploitation by an attacker could lead to remote code execution.

19195 - (HT205317) Apple Mac EFI Security Update 2015-002

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

Risk Level: High

CVE: CVE-2015-7035

Description

A vulnerability is present in some versions of Apple OS X.

Observation

Apple OS X is an operating system used in Apple computer.

A vulnerability is present in some versions of Apple OS X. The flaw lies in Mac EFI firmware. Successful exploitation could allow an attacker to reach unused EFI functions.

19204 - (HT205379) Apple Xcode Type Conversion Vulnerability Prior To 7.1

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

Risk Level: High

CVE: CVE-2015-7030

Description

A type conversion vulnerability is present in some versions of Apple Xcode.

Observation

Apple Xcode is a development framework for MAC OS X and iOS devices.

A type conversion vulnerability is present in some versions of Apple Xcode. The flaw lies in Swift within Xcode. Successful exploitation could allow an attacker to cause an undetermined impact on the affected host.

19286 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 38.4

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

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

Observation

Mozilla Firefox ESR is an open source web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code.

19287 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 38.4

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

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

Observation

Mozilla Firefox ESR is an open source web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code.

19278 - Joomla ACL Violations Vulnerability (20151003)

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

Risk Level: Medium

CVE: CVE-2015-7899

Description

An information disclosure vulnerability is present in some versions of Joomla!.

Observation

Joomla! is a content management system.

An information disclosure vulnerability is present in some versions of Joomla!. The flaw is due to inadequate checking of ACLs within com_content component. Successful exploitation by an attacker could lead to sensitive information disclosure.

19281 - (SOL17494) F5 BIG-IP PAM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-3238

Description

A vulnerability is present in the Linux Kernel in some versions of F5 BIG-IP systems.

Observation

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

A vulnerability is present in the Linux Kernel in some versions of F5 BIG-IP systems. The flaw lies in Linux-PAM. Successful exploitation could allow local users to enumerate usernames or cause a denial of service on the affected system.

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.

70046 - macosx.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.