2019-APR-22
FSL version 7.6.107

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

25055 - Oracle Java SE Critical Patch Update April 2019

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

Risk Level: High

CVE: CVE-2019-2602, CVE-2019-2684, CVE-2019-2697, CVE-2019-2698, CVE-2019-2699

Description

Multiple vulnerabilities are present in some versions of Oracle Java SE.

Observation

Oracle Java SE is used to run Java applications.

Multiple vulnerabilities are present in some versions of Oracle Java SE. The flaws lie in multiple components. Successful exploitation could allow an attacker to affect the confidentiality, integrity and availability of the targeted system.

24926 - IBM DB2 Privilege Escalation Vulnerability (ibm10875860)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-4094

Description

A vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw is due to loading libraries from an untrusted path. Successful exploitation could allow a local attacker to gain full access to the DB2 instance account.

25021 - Apache Tomcat Vulnerability Prior To 8.5.38

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

Risk Level: High

CVE: CVE-2019-0199

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

A vulnerability is present in some versions of Apache Tomcat. The flaw lies in HTTP/2 implementation. Successful exploitation could cause an attacker to cause a denial of service condition.

25037 - Cisco IOS Software Network-Based Application Recognition Denial Of Service Vulnerabilities (cisco-sa-20190327-nbar)

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

Risk Level: High

CVE: CVE-2019-1738, CVE-2019-1739, CVE-2019-1740

Description

Multiple vulnerabilities are present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

Multiple vulnerabilities are present in some versions of Cisco IOS. The flaws lie in Network-Based Application Recognition (NBAR) feature. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

25044 - (SB10278) McAfee Web Gateway Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-18311, CVE-2018-5742, CVE-2019-6454, CVE-2019-9169

Description

Multiple vulnerabilities are present in some versions of McAfee Web Gateway.

Observation

McAfee Web Gateway is a web based security control system designed to prevent web application attacks.

Multiple vulnerabilities are present in some versions of McAfee Web Gateway. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service or execute arbitrary code.

25047 - Cisco IOS Software ISDN Interface Denial of Service Vulnerability (cisco-sa-20190327-isdn)

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

Risk Level: High

CVE: CVE-2019-1752

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 ISDN functions. Successful exploitation could allow a remote attacker to cause a denial of service condition.

25020 - (HT209599) Apple iOS Multiple Vulnerabilities Prior To 12.2

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Medium

CVE: CVE-2019-6201, CVE-2019-6203, CVE-2019-6204, CVE-2019-6207, CVE-2019-6222, CVE-2019-6237, CVE-2019-7284, CVE-2019-7285, CVE-2019-7292, CVE-2019-7293, CVE-2019-8502, CVE-2019-8503, CVE-2019-8504, CVE-2019-8505, CVE-2019-8506, CVE-2019-8510, CVE-2019-8511, CVE-2019-8512, CVE-2019-8514, CVE-2019-8515, CVE-2019-8516, CVE-2019-8517, CVE-2019-8518, CVE-2019-8521, CVE-2019-8523, CVE-2019-8524, CVE-2019-8527, CVE-2019-8528, CVE-2019-8529, CVE-2019-8530, CVE-2019-8535, CVE-2019-8536, CVE-2019-8538, CVE-2019-8540, CVE-2019-8541, CVE-2019-8542, CVE-2019-8544, CVE-2019-8545, CVE-2019-8546, CVE-2019-8549, CVE-2019-8550, CVE-2019-8551, CVE-2019-8552, CVE-2019-8553, CVE-2019-8554, CVE-2019-8556, CVE-2019-8558, CVE-2019-8559, CVE-2019-8562, CVE-2019-8563, CVE-2019-8565, CVE-2019-8566, CVE-2019-8567, CVE-2019-8906

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 many components. Successful exploitation could allow an attacker to cause remote code execution, privilege escalation on the target or may lead to a denial of service.

25042 - Cisco IOS Software Hot Standby Router Protocol Information Leak Vulnerability (cisco-sa-20190327-ios-infoleak)

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

Risk Level: Low

CVE: CVE-2019-1761

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 insufficient memory initialization. Successful exploitation could allow an attacker to obtain sensitive information.

25053 - Cisco IOS Software Information Disclosure Vulnerability (cisco-sa-20190327-info)

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

Risk Level: Low

CVE: CVE-2019-1762

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw lies in Secure Storage feature. Successful exploitation could allow an attacker to retrieve sensitive information from the target 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.

24056 - (K74374841) F5 BIG-IP Linux kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2018-5391

Update Details

Observation is updated

182926 - FreeBSD Gitlab Multiple Vulnerabilities (11292460-3f2f-11e9-adcb-001b217b3468)

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

Risk Level: High

CVE: CVE-2019-9170, CVE-2019-9171, CVE-2019-9172, CVE-2019-9174, CVE-2019-9175, CVE-2019-9176, CVE-2019-9178, CVE-2019-9179, CVE-2019-9217, CVE-2019-9219, CVE-2019-9220, CVE-2019-9221, CVE-2019-9222, CVE-2019-9223, CVE-2019-9224, CVE-2019-9225, CVE-2019-9485

Update Details

Risk is updated

131333 - Debian Linux 9.0 DSA-4430-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499

Update Details

Risk is updated

195067 - Fedora Linux 30 FEDORA-2019-ca49dfd42f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-9494, CVE-2019-9495, CVE-2019-9496, CVE-2019-9497, CVE-2019-9498

Update Details

Risk 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.