2015-NOV-23
FSL version 7.5.765

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

19291 - IBM WebSphere Application Server Apache Commons Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2015-7450

Description

A Java object deserialization vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a Java application server.

A Java object deserialization vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in Apache Commons Collections. Successful exploitation could allow an attacker to execute arbitrary code.

19300 - LibreOffice OpenOffice Bookmark DOC Document Remote Code Execution

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

Risk Level: High

CVE: CVE-2015-5214

Description

A vulnerability in some versions of LibreOffice and Apache OpenOffice could lead to remote code execution.

Observation

A vulnerability in some versions of LibreOffice and Apache OpenOffice could lead to remote code execution.

The flaw lies in the handling of a crafted DOC document. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

19306 - LibreOffice OpenOffice Long DOC Document Remote Code Execution

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

Risk Level: High

CVE: CVE-2015-5213

Description

A vulnerability in some versions of LibreOffice and Apache OpenOffice could lead to remote code execution.

Observation

A vulnerability in some versions of LibreOffice and Apache OpenOffice could lead to remote code execution.

The flaw lies in the handling of a crafted DOC document. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

19298 - Google Chrome Multiple Vulnerabilities Prior To 46.0.2490.86

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

Risk Level: High

CVE: CVE-2015-1302

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 several components, including Adobe Flash Player. Successful exploitation could allow an attacker to bypass security measures.

19299 - Google Chrome Multiple Vulnerabilities Prior To 46.0.2490.86

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-1302

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 several components, including Adobe Flash Player. Successful exploitation could allow an attacker to bypass security measures.

19301 - Unitronics VisiLogic OPLC IDE Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-6478, CVE-2015-7905

Description

Multiple vulnerabilities are present in some versions of Unitronics VisiLogic OPLC IDE.

Observation

Unitronics VisiLogic OPLC IDE allows development of PLC and HMI applications.

Multiple vulnerabilities are present in some versions of Unitronics VisiLogic OPLC IDE. The flaws lie in multiple components including an ActiveX control. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

19302 - (SYM15-011) Symantec Endpoint Protection Manager Privilege Escalation Vulnerabilities

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6554, CVE-2015-6555

Description

Multiple vulnerabilities are present in some versions of Symantec Endpoint Protection Manager.

Observation

Symantec Endpoint Protection Manager enables the management of endpoint nodes of anti-malware for Windows, Macs and Linux computers.

Multiple vulnerabilities are present in some versions of Symantec Endpoint Protection Manager. The flaws lie in the SEPM Manager console. Successful exploitation could allow an attacker to perform remote code execution with elevated privileges.

19303 - (SYM15-011) Symantec Endpoint Protection Client Privilege Escalation Vulnerability

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-8113

Description

A vulnerability is present in some versions of Symantec Endpoint Protection Client.

Observation

Symantec Endpoint Protection is an all-in-one antivirus software.

A vulnerability is present in some versions of Symantec Endpoint Protection Client. The flaw is due to improperly restricting the loading of external libraries. Successful exploitation could allow an attacker to execute arbitrary code with elevated privileges.

19194 - (CTX202404) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-7835, CVE-2015-7969, CVE-2015-7970, CVE-2015-7971, CVE-2015-7972

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in multiple components. Successful exploitation could allow an attacker to crash the host or compromise the host.

19202 - Oracle VM VirtualBox Critical Patch Update October 2015

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

Risk Level: Medium

CVE: CVE-2015-4813, CVE-2015-4856, CVE-2015-4896

Description

Multiple vulnerabilities are present in some versions of Oracle VirtualBox.

Observation

Oracle VirtualBox is a virtualization software.

Multiple vulnerabilities are present in some versions of Oracle VirtualBox. The flaws exist in the Core sub-component. Successful exploitation by a local attacker could affect availability.

19240 - IBM WebSphere Application Server Response Splitting Vulnerability

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

Risk Level: Medium

CVE: CVE-2015-2017

Description

A response splitting vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a Java application server.

A response splitting vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in Channel. Successful exploitation could allow an attacker to perform further attacks, such as Web cache poisoning, cross-site scripting and obtain sensitive information.

19305 - (CTX202482) Citrix NetScaler Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-7996, CVE-2015-7997, CVE-2015-7998

Description

Multiple vulnerabilities are 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.

Multiple vulnerabilities are present in some versions of Citrix NetScaler. The flaws lie in the Service VM (SVM) component. Successful exploitation could allow an attacker to retrieve sensitive data or to remotely execute arbitrary code.

19293 - (CTX202583) Citrix XenServer Multiple Denial of Service Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

Description

Multiple denial of service vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple denial of service vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in exception delivery which will cause CPU lockup. Successful exploitation could allow an attacker to cause denial of service.

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.

19307 - Jenkins Java Deserialization Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2015-8103

Update Details

CVE is updated

18722 - (SOL16872) F5 BIG-IP Java Runtime Environment Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2013-4002

Update Details

FASLScript is updated

18740 - (SOL16912) F5 BIG-IP BIND Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-4620

Update Details

FASLScript is updated

18743 - (SOL16909) F5 BIG-IP BIND Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-5477

Update Details

FASLScript is updated

12824 - HTTP Server Prone To Slow Denial Of Service Attack

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

Risk Level: Medium

CVE: CVE-2007-6750, CVE-2009-5111, CVE-2012-5568

Update Details

CVE is updated

18724 - (SOL16946) F5 BIG-IP Boost Memory Allocator Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2012-2677

Update Details

FASLScript is updated

130315 - Debian Linux 7.0, 8.0 DSA-3398-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8023

Update Details

Risk is updated

181671 - FreeBSD strongswan Authentication Bypass Vulnerability In The Eap-mschapv2 Plugin (3eb0ccc2-8c6a-11e5-8519-005056ac623e)

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

Risk Level: Medium

CVE: CVE-2015-8023

Update Details

Risk is updated

185058 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2811-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8023

Update Details

Risk is updated

70116 - scada.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70131 - f5.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.