2014-NOV-18
FSL version 7.5.648

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

17292 - Oracle Database Server Critical Patch Update October 2014

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

Risk Level: High

CVE: CVE-2014-0050, CVE-2014-2478, CVE-2014-4289, CVE-2014-4290, CVE-2014-4291, CVE-2014-4292, CVE-2014-4293, CVE-2014-4294, CVE-2014-4295, CVE-2014-4296, CVE-2014-4297, CVE-2014-4298, CVE-2014-4299, CVE-2014-4300, CVE-2014-4301, CVE-2014-4310, CVE-2014-6452, CVE-2014-6453, CVE-2014-6454, CVE-2014-6455, CVE-2014-6467, CVE-2014-6483, CVE-2014-6537, CVE-2014-6538, CVE-2014-6542, CVE-2014-6544, CVE-2014-6545, CVE-2014-6546, CVE-2014-6547, CVE-2014-6560, CVE-2014-6563

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is a industrial standard database software.

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

17293 - Oracle Database Server Critical Patch Update October 2014

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0050, CVE-2014-2478, CVE-2014-4289, CVE-2014-4290, CVE-2014-4291, CVE-2014-4292, CVE-2014-4293, CVE-2014-4294, CVE-2014-4295, CVE-2014-4296, CVE-2014-4297, CVE-2014-4298, CVE-2014-4299, CVE-2014-4300, CVE-2014-4301, CVE-2014-4310, CVE-2014-6452, CVE-2014-6453, CVE-2014-6454, CVE-2014-6455, CVE-2014-6467, CVE-2014-6483, CVE-2014-6537, CVE-2014-6538, CVE-2014-6542, CVE-2014-6544, CVE-2014-6545, CVE-2014-6546, CVE-2014-6547, CVE-2014-6560, CVE-2014-6563

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is a industrial standard database software.

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

17429 - WordPress Media File Renamer Plugin Cross-Site Scripting Vulnerability

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

Risk Level: High

CVE: CVE-2014-2040

Description

Multiple cross-site scripting vulnerabilities are present in some versions of Media File Renamer Plugin for WordPress.

Observation

WordPress is a popular blog web application.

Multiple cross-site scripting vulnerabilities are present in some versions of Media File Renamer Plugin for WordPress. The flaws lie in multiple parameters which are not being properly sanitized by the plugin. Successful exploitation could allow an attacker to execute arbitrary web code.

17358 - (MS14-068) Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)

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

Risk Level: High

CVE: CVE-2014-6324

Description

A privilege escalation vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operating system.

A privilege escalation vulnerability is present in some versions of Microsoft Windows. The flaw lies in Microsoft Kerberos KDC. Successful exploitation could allow an attacker to escalate privileges.

Microsoft has provided MS14-068 to address this issue. The host appears to be missing this patch.

17411 - ABB RobotStudio/Test Signal Viewer DLL Hijack Remote Code Execution

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

Risk Level: High

CVE: CVE-2014-5430

Description

A vulnerability in some versions of ABB RobotStudio and ABB Test Signal Viewer could lead to remote code execution.

Observation

A vulnerability in some versions of ABB RobotStudio and ABB Test Signal Viewer could lead to remote code execution.

The flaw lies in a third-party component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17417 - Microsys Promotic Visual Basic Code Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of Microsys Promotic could lead to remote code execution.

Observation

A vulnerability in some versions of Microsys Promotic could lead to remote code execution.

The flaw is due to an unspecified defect. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17340 - D-Link Multiple Products OpenSSL SSL/TLS Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-2014-0224

Description

A vulnerability is present in some versions of D-Link DSR-500 and DSR-1000.

Observation

D-Link DSR-500 and DSR-1000 are network router devices.

A vulnerability is present in some versions of D-Link DSR-500 and DSR-1000. The flaw lies in OpenSSL component. Successful exploitation could allow an attacker to bypass security restriction and obtain sensitive information.

17315 - Oracle JRockit Critical Patch Update October 2014

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

Risk Level: Medium

CVE: CVE-2014-6457, CVE-2014-6512, CVE-2014-6517, CVE-2014-6558

Description

Multiple vulnerabilities are present in some versions of Oracle JRockit.

Observation

Oracle JRockit is Middleware for Oracle Fusion.

Multiple vulnerabilities are present in some versions of Oracle JRockit. The flaws lie in the Oracle JRockit components. Successful exploitation by a remote attacker could affect confidentiality, integrity and availability.

17323 - (HT6541) Apple iOS Multiple Vulnerabilities Prior To 8.1

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Medium

CVE: CVE-2014-3566, CVE-2014-4428, CVE-2014-4448, CVE-2014-4449, CVE-2014-4450

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 multiple components. Successful exploitation could allow an attacker to disclose potentially sensitive information and bypass certain security restrictions.

17350 - IBM WebSphere Portal CKEditor Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2014-5191

Description

A vulnerability in some versions of IBM WebSphere Portal could lead to cross-site scripting.

Observation

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

A vulnerability in some versions of IBM WebSphere Portal could lead to cross-site scripting. The flaw lies in the CKEditor. Successful exploitation could allow a remote attacker to inject arbitrary web script or HTML code.

17361 - (MS14-068) Microsoft Windows Kerberos Checksum Privilege Escalation (3011780)

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

Risk Level: Medium

CVE: CVE-2014-6324

Description

A privilege escalation vulnerability is present in some versions of Microsoft Windows.

Observation

A privilege escalation vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Kerberos component. Successful exploitation could allow an attacker to execute commands with elevated privileges.

17343 - (SOL15685) F5 BIG-IP Linux Kernel Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3940, CVE-2014-4027

Description

Multiple denial of service vulnerabilities are present 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.

Multiple denial of service vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in the Linux kernel. Successful exploitation could allow an attacker to cause a denial of service condition.

17410 - IBM Tivoli Storage Manager Client ReFS File Unauthorized Access Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-5371

Description

A security bypass vulnerability is present in some versions of IBM Tivoli Storage Manager Client.

Observation

IBM Tivoli Storage Manager (TSM) is an enterprise class backup and recovery software.

A security bypass vulnerability is present in some versions of IBM Tivoli Storage Manager Client. The flaw is caused due to TSM Windows client not properly preserving file permissions when performing archive, backup, restore, and retrieve operations to ReFS. Successful exploitation could allow an attacker to bypass security and gain unauthorized access to restored or retrieved files.

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.

9944 - SquirrelMail spellchecker plug-in Remote Shell Command Execution Vulnerability

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

Risk Level: High

CVE: CVE-2002-1650

Update Details

FASLScript is updated

17039 - BlackBerry OS OpenSSL Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Blackberry

Risk Level: Medium

CVE: CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

Update Details

Recommendation is updated

17281 - SSLv3 Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3566

Update Details

Recommendation is updated

70086 - oracle.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript 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

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.