2013-OCT-14

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

15743 - (SOL14700) F5 BIG-IP APM Clickjacking Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-5975

Description

A clickjacking protection bypass vulnerability is 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.

A clickjacking protection bypass vulnerability is present in some versions of F5 BIG-IP systems. The issue lies in the BIG-IP APM access policy logon page. Successful exploitation could allow an attacker to bypass clickjacking protection.

15744 - (SOL14712) F5 BIG-IP APM Access Policy Logout Page XSS Cookie Tampering Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

Description

A Cross Site-Scripting vulnerability is 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.

A Cross Site-Scripting vulnerability is present in some versions of F5 BIG-IP systems. The issue lies in the BIG-IP APM access policy logout page. Successful exploitation could allow an attacker to insert any HTML and script in the affected page.

15749 - Invensys Wonderware InTouch XML External Entities Vulnerability

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

Risk Level: Medium

CVE: CVE-2012-4709

Description

A vulnerability is present in some versions of Invensys Wonderware InTouch.

Observation

Wonderware InTouch is a software component to manage industrial systems.

A vulnerability is present in some versions of Invensys Wonderware InTouch. The vulnerability is caused by inappropriate management of XML external entities. A specially crafted XML entity could generate a denial of service or allow an attacker to access local resources.

15753 - IBM Rational ClearQuest JSON Hijacking and Cross-Site Request Forgery Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2013-0598, CVE-2013-3041

Description

Multiple vulnerabilities are present in some versions of IBM Rational ClearQuest.

Observation

IBM Rational ClearQuest is a workflow automation software package which provides bug tracking and process automation across the application development life cycle.

Multiple vulnerabilities are present in some versions of IBM Rational ClearQuest. The flaw lies in the ClearQuest HTTP requests. Successful exploitation allows remote attackers to execute arbitrary HTML in a user's browser session.

15758 - WordPress WP Ultimate Email Marketer Plugin Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2013-3263, CVE-2013-3264

Description

Multiple vulnerabilities are present in some versions of the WordPress WP Ultimate Email Marketer Plugin.

Observation

WordPress is a popular blog web application.

Multiple vulnerabilities are present in some versions of the WordPress WP Ultimate Email Marketer Plugin. The flaws lie in multiple plugin's components. Successful exploitation could allow an attacker to execute arbitrary scripts and code in the context of current logged user.

55210 - Top Weekly Malware Env - Trojan-BdCoreDumpStats (BdCoreDumpStats.exe)

Category: Windows Host Assessment -> Top Weekly Malware
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

Description

The scan detected that the host is infected by the malware: Env - Trojan-BdCoreDumpStats (BdCoreDumpStats.exe)

Observation

This malware shows the following behavior:

The files and directories below were created:
%temp%\\BdCoreDumpStats.exe

For more information on this malware, visit http://vil.nai.com/vil/default.aspx

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.

15507 - Opera Multiple Vulnerabilities Prior To 16.00

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

Risk Level: High

CVE: CVE-2013-2887, CVE-2013-2900, CVE-2013-2901, CVE-2013-2902, CVE-2013-2903, CVE-2013-2904, CVE-2013-2905

Update Details

Recommendation is updated.

15720 - (MS13-080) Cumulative Security Update for Internet Explorer (2879017)

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

Risk Level: High

CVE: CVE-2013-3872, CVE-2013-3873, CVE-2013-3874, CVE-2013-3875, CVE-2013-3882, CVE-2013-3885, CVE-2013-3886, CVE-2013-3893, CVE-2013-3897

Microsoft ID: MS13-080

Microsoft KB: 2879017

Update Details

CVE is updated.
FASLScript is updated.

2384 - HP Sendmail Implementation Connection Denial-of-Service

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

CVE: CVE-1999-0478, CVE-1999-0684

Update Details

CVE is updated.

DELETED CHECKS

15705 - (MS13-080) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3871

DISA IAVA: 2013-A-0188

Microsoft ID: MS13-080

Microsoft KB: 2879017

ADDITIONAL NOTES

15705 - was removed due to CVE-2013-3871 was not covered by Microsoft bulletin MS13-080 and FID15720 was modified as well.

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.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2012 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates