2013-OCT-16

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

15750 - BlackBerry 10 OS / PlayBook OS WebKit JavaScriptCore Component Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Blackberry

Risk Level: High

CVE: CVE-2013-0999

Description

A vulnerability is present in some versions of BlackBerry OS.

Observation

BlackBerry OS is a popular mobile phone operating system.

A vulnerability is present in some versions of BlackBerry OS. The flaw lies in WebKit. Successful exploitation of the vulnerability could allow an attacker to execute remote code on the affected device.

15759 - Cogent DataHub Two Vulnerabilities

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

Risk Level: High

Description

Two vulnerabilities are present in some versions of Cogent DataHub.

Observation

Cogent DataHub is a popular real-time data solutions.

Two vulnerabilities are present in some versions of Cogent DataHub. The flaws are due to unspecified errors. Successful exploitation by a remote attacker could result in a denial of service or the overwrite of certain files.

15792 - Oracle Java SE Critical Patch Update October 2013

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

Risk Level: High

CVE: CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5775, CVE-2013-5776, CVE-2013-5777, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5787, CVE-2013-5788, CVE-2013-5789, CVE-2013-5790, CVE-2013-5797, CVE-2013-5800, CVE-2013-5801, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5805, CVE-2013-5806, CVE-2013-5809, CVE-2013-5810, CVE-2013-5812, CVE-2013-5814, CVE-2013-5817, CVE-2013-5818, CVE-2013-5819, CVE-2013-5820, CVE-2013-5823, CVE-2013-5824, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5831, CVE-2013-5832, CVE-2013-5838, CVE-2013-5840, CVE-2013-5842, CVE-2013-5843, CVE-2013-5844, CVE-2013-5846, CVE-2013-5848, CVE-2013-5849, CVE-2013-5850, CVE-2013-5851, CVE-2013-5852, CVE-2013-5854

Description

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

Observation

Oracle Java SE is used to running 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 execute arbitrary code.

15754 - Cogent DataHub Denial of Service Vulnerability Prior To 7.3.3

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

Risk Level: Medium

Description

A denial of service vulnerability present in some versions of Cogent DataHub.

Observation

Cogent DataHub is a popular real-time data integration SCADA solution.

A denial of service vulnerability present in some versions of Cogent DataHub. The flaw is due to when processing HTTP requests. Successful exploitation by a remote attacker could result in a denial of service condition on the affected device.

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.

15325 - Juniper Junos SRX Flow Daemon HTTP Messages Buffer Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-4685

DISA IAVA: 2013-A-0139

Update Details

Observation is updated.
Recommendation is updated.

15343 - Juniper Junos OSPF Protocol Routes Injection Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-0149

Update Details

Observation is updated.
Recommendation is updated.

15555 - (MS13-067) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)

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

Risk Level: High

CVE: CVE-2013-0081, CVE-2013-1315, CVE-2013-1330, CVE-2013-3179, CVE-2013-3180, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3857, CVE-2013-3858

Microsoft ID: MS13-067

Microsoft KB: 2834052

Update Details

FASLScript is updated.

15689 - Mitsubishi MC-WorkX IcoLaunch ActiveX Control Remote Code Execution Vulnerability

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

Risk Level: High

Update Details

Recommendation is updated.

11039 - IBM WebSphere Application Server Snoop Servlet Information Disclosure Vulnerability

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

Risk Level: Medium

Update Details

Recommendation is updated.
Risk is updated.

14895 - Oracle MySQL yaSSL TLS CBC Ciphersuite Plaintext Recovery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-1623

Update Details

Observation is updated.

15309 - Juniper Junos OpenSSL Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-0166, CVE-2013-0169

DISA IAVA: 2013-A-0139,2013-A-0077

Update Details

Observation is updated.
Recommendation is updated.

15310 - Juniper Junos J-Web SSL/TLS Renegotiation Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2011-1473

DISA IAVA: 2013-A-0139

Update Details

Observation is updated.
Recommendation is updated.

15541 - (MS13-067) Microsoft SharePoint Denial of Service (2834052)

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

Risk Level: Medium

CVE: CVE-2013-0081

DISA IAVA: 2013-A-0174

Microsoft ID: MS13-067

Microsoft KB: 2834052

Update Details

FASLScript is updated.

15543 - (MS13-067) Microsoft SharePoint Cross-Site Scripting Privilege Escalation (2834052)

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

Risk Level: Medium

CVE: CVE-2013-3179

DISA IAVA: 2013-A-0174

Microsoft ID: MS13-067

Microsoft KB: 2834052

Update Details

FASLScript is updated.

15544 - (MS13-067) Microsoft SharePoint POST Cross-Site Scripting Privilege Escalation (2834052)

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

Risk Level: Medium

CVE: CVE-2013-3180

DISA IAVA: 2013-A-0174

Microsoft ID: MS13-067

Microsoft KB: 2834052

Update Details

FASLScript is updated.

15600 - TP-LINK TD-W8951ND Router Cross-Site Scripting and Request Forgery Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

Update Details

Recommendation 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.