2015-NOV-27
FSL version 7.5.767

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

19310 - TECO JN5 DriveLink LF5 File Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some versions of TECO JN5 DriveLink could lead to remote code execution.

Observation

A vulnerability in some versions of TECO JN5 DriveLink could lead to remote code execution.

The flaw lies in the handling of a LF5 file. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

19319 - IBM WebSphere Portal Cross-Site Scripting Vulnerability (CVE-2015-4993)

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

Risk Level: Medium

CVE: CVE-2015-4993

Description

A vulnerability is present in some versions of IBM WebSphere Portal.

Observation

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

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw is due to improper verification of user-supplied input. Successful exploitation could allow a remote attacker to inject arbitrary HTML or web script.

19320 - IBM WebSphere Portal Cross-Site Scripting Vulnerability (CVE-2015-4998)

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

Risk Level: Medium

CVE: CVE-2015-4998

Description

A vulnerability is present in some versions of IBM WebSphere Portal.

Observation

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

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw is due to improper verification of user-supplied input. Successful exploitation could allow a remote attacker to inject arbitrary HTML or web script.

19321 - IBM WebSphere Portal Denial of Service Vulnerability (CVE-2015-5001)

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

Risk Level: Medium

CVE: CVE-2015-5001

Description

A vulnerability is present in some versions of IBM WebSphere Portal.

Observation

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

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw is due to improper verification of user-supplied input. Successful exploitation could allow a remote attacker to cause a denial of service.

19322 - IBM WebSphere Portal Cross-Site Scripting Vulnerability (CVE-2015-7413)

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

Risk Level: Medium

CVE: CVE-2015-7413

Description

A vulnerability is present in some versions of IBM WebSphere Portal.

Observation

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

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw is due to improper verification of user-supplied input. Successful exploitation could allow a remote attacker to inject arbitrary HTML or web script.

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.

17458 - (SOL15723) F5 BIG-IP OpenSSL Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-3567

Update Details

FASLScript is updated

7279 - Windows Policy Baselining

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

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.