2015-DEC-17
FSL version 7.5.775

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.

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.

19334 - (MS15-128) Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)

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

Risk Level: High

CVE: CVE-2015-6106, CVE-2015-6107, CVE-2015-6108

Update Details

Name is updated Recommendation is updated

19338 - (MS15-128) Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-6106, CVE-2015-6107, CVE-2015-6108

Update Details

Name is updated Recommendation is updated

7134 - Microsoft Windows Allow LocalSystem Null Session Fallback Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7135 - Microsoft Windows Allow PKU2U Authentication Requests to This Computer to Use Online Identities Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7136 - Microsoft Windows Allow The Use Of Biometrics Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7143 - Microsoft Windows Allow Users To Logon Using Biometrics Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7144 - Microsoft Windows Allow Domain Users To Logon Using Biometrics Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7145 - Microsoft Windows Prevent Redirection Of USB Devices Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7146 - Microsoft Windows Audit Incoming NTLM Traffic Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7147 - Microsoft Windows Turn Off Data Execution Prevention For HTML Help Executables Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7148 - Microsoft Windows Turn Off System Restore Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7149 - Microsoft Windows Restrict Incoming NTLM Traffic

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7150 - Microsoft Windows Restrict Outgoing NTLM Traffic to Remote Servers Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7151 - Microsoft Windows Server SPN Target Name Validation Level Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7153 - Microsoft Windows Allow LocalSystem to Use Computer Identity for NTLM Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7154 - Microsoft Windows Turn Off Problem Steps Recorder Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7155 - Microsoft Windows Turn Off Application Telemetry Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7156 - Microsoft Windows Turn Off Autoplay for Non-Volume Devices Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7157 - Microsoft Windows Turn Off Program Inventory Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7158 - Microsoft Windows Turn Off SwitchBack Compatibility Engine Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7159 - Microsoft Windows Restrict NTLM Authentication In This Domain Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

7160 - Microsoft Windows Audit NTLM Authentication In This Domain Policy

Category: Windows Host Assessment -> Security Policy/Options
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70001 - windowspolicy.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.