2014-DEC-05
FSL version 7.5.652

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

17511 - Microsoft Internet Explorer display:run-in Use After Free Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2014-8967

Description

A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer.

Observation

Microsoft Internet Explorer is a popular Internet web browser.

A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer. The vulnerability is due to improper management of HTML object references in memory. Successful exploitation could allow an attacker to execute remote code.

17470 - Google Chrome Flash Player Vulnerability Prior To 39.0.2171.71

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

Risk Level: High

CVE: CVE-2014-8439

Description

A remote code execution vulnerability is present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser for Microsoft Windows, Apple Mac OS X and Linux.

A remote code execution vulnerability is present in some versions of Google Chrome. The flaw lies in the Adobe Flash Player component of Google Chrome. Successful exploitation could allow an attacker to execute arbitrary code.

17472 - (SOL15547) F5 BIG-IP MIT Kerberos 5 Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-4342

Description

A denial of service vulnerability is present in some versions of F5's BIG-IP.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A denial of service vulnerability is present in some versions of F5's BIG-IP. The flaw lies in MIT Kerberos 5 when processing invalid tokens in GSSAPI application session. Successful exploitation could allow an attacker to cause a denial of service condition.

17475 - (SOL15552) F5 BIG-IP MIT Kerberos 5 Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-4341

Description

A denial of service vulnerability is present in some versions of F5's BIG-IP.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A denial of service vulnerability is present in some versions of F5's BIG-IP. The flaw lies in MIT Kerberos 5 when processing invalid tokens in GSSAPI application session. Successful exploitation could allow an attacker to cause a denial of service condition.

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.

2131 - W32/Mydoom@MM Server Detected

Category: General Vulnerability Assessment -> NonIntrusive -> Trojan, Backdoors, Viruses, and Malware

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Documentation is updated

181255 - FreeBSD security/ossec-hids-* Root Escalation Via Temp Files (36858e78-3963-11e4-ad84-000c29f6ae42)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-5284

Update Details

Risk is updated

181293 - FreeBSD flac Multiple Vulnerabilities (a33addf6-74e6-11e4-a615-f8b156b6dcc8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

Update Details

Risk is updated

184612 - Ubuntu Linux 14.10 USN-2411-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-1421

Update Details

Risk is updated

17476 - WordPress Multiple Vulnerabilities III

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

Risk Level: Medium

CVE: CVE-2014-9031, CVE-2014-9032, CVE-2014-9033, CVE-2014-9034, CVE-2014-9035, CVE-2014-9036, CVE-2014-9037, CVE-2014-9038, CVE-2014-9039

Update Details

Risk is updated

130003 - Debian Linux 7.0 DSA-3084-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-8104

Update Details

Risk is updated

181291 - FreeBSD phpMyAdmin XSS And Information Disclosure Vulnerabilities (a5d4a82a-7153-11e4-88c7-6805ca0b3d42)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-8958, CVE-2014-8959, CVE-2014-8960, CVE-2014-8961

Update Details

Risk is updated

181295 - FreeBSD OpenVPN Denial Of Service Security Vulnerability (23ab5c3e-79c3-11e4-8b1e-d050992ecde8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-8104

Update Details

Risk is updated

184613 - Ubuntu Linux 14.04, 14.10 USN-2422-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-7141, CVE-2014-7142

Update Details

Risk is updated

184625 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2430-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-8104

Update Details

Risk is updated

188532 - Fedora Linux 21 FEDORA-2014-15601 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-7850

Update Details

Risk is updated

93426 - Mandriva Linux MBS1 MDVSA-2014-217 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes

Risk Level: Low

CVE: CVE-2013-6497

Update Details

Risk is updated

188446 - Fedora Linux 21 FEDORA-2014-14347 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2013-6494

Update Details

Risk is updated

188488 - Fedora Linux 20 FEDORA-2014-14027 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2013-6494

Update Details

Risk is updated

188492 - Fedora Linux 19 FEDORA-2014-14252 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2013-6494

Update Details

Risk is updated

188530 - Fedora Linux 20 FEDORA-2014-15473 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2013-6497

Update Details

Risk 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.