2014-OCT-15

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

17278 - Oracle Java SE Critical Patch Update October 2014

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

Risk Level: High

CVE: CVE-2014-4288, CVE-2014-6456, CVE-2014-6457, CVE-2014-6458, CVE-2014-6466, CVE-2014-6468, CVE-2014-6476, CVE-2014-6485, CVE-2014-6492, CVE-2014-6493, CVE-2014-6502, CVE-2014-6503, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6513, CVE-2014-6515, CVE-2014-6517, CVE-2014-6519, CVE-2014-6527, CVE-2014-6531, CVE-2014-6532, CVE-2014-6558, CVE-2014-6562

Description

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

Observation

Oracle Java SE is used to run Java application.

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.

17277 - Microsoft Windows EAP TLS Man-In-The-Middle Attack (2977292)

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

Risk Level: Medium

Microsoft KB: 2977292

Description

A vulnerability in some versions of Microsoft Windows could lead to a man-in-the-middle attack.

Observation

A vulnerability in some versions of Microsoft Windows could lead to a man-in-the-middle attack.

The flaw lies in the Microsoft Extensible Authentication Protocol implementation that enables the use of Transport Layer Security 1.1 or 1.2. Successful exploitation could allow a remote attacker to gain access to sensitive information from encrypted sessions.

17281 - SSLv3 Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3566

Description

A vulnerability is present in some versions of the SSL Protocol.

Observation

TLS/SSL is a network communication protocol used for secure connections.

A vulnerability is present in some versions of the SSL Protocol. The flaw lies in a weakness in the CBC encryption algorithm within the SSL 3.0 protocol. Successful exploitation by a remote attacker could allow access to potentially sensitive information.

17279 - Availability of SHA-2 Hashing Algorithm for Windows 7 and Windows Server 2008 R2 (2949927)

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

Risk Level: Low

Microsoft KB: 2949927

Description

A weakness is present in some versions of Microsoft Windows.

Observation

The Secure Hash Algorithm (SHA) was used to generate a 160-bit hash value.

A weakness is present in in some versions of Microsoft Windows. The SHA-2 signing and verification functionality isn't included in system. Successful exploitation could allow an attacker to generate additional spoofed certificates that have the same digital signature as an original.

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.

16961 - (MS14-044) Vulnerabilities in SQL Server Could Allow Elevation of Privilege (2984340)

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

Risk Level: Medium

CVE: CVE-2014-1820, CVE-2014-4061

DISA IAVA: 2014-A-0126

Microsoft ID: MS14-044

Microsoft KB: 2984340

Update Details

FASLScript is updated.

16963 - (MS14-044) Microsoft SQL Server Stack Overrun Privilege Escalation (2984340)

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

Risk Level: Medium

CVE: CVE-2014-4061

DISA IAVA: 2014-A-0126

Microsoft ID: MS14-044

Microsoft KB: 2984340

Update Details

FASLScript is updated.

93381 - Mandriva Linux MBS1 MDVSA-2014-185 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4488

Update Details

Risk is updated.

181267 - FreeBSD Bugzilla Multiple Security Issues (b6587341-4d88-11e4-aef9-20cf30e32f6d)

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

Risk Level: Medium

CVE: CVE-2014-1571, CVE-2014-1572, CVE-2014-1573

Update Details

Risk is updated.

187485 - Fedora Linux 19 FEDORA-2013-23517 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4488

Update Details

Risk is updated.

187489 - Fedora Linux 20 FEDORA-2013-23260 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4488

Update Details

Risk is updated.

58948 - Debian Linux 7.0 DSA-3024-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-5270

Update Details

Risk is updated.

93387 - Mandriva Linux MBS1 MDVSA-2014-176 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-5270

Update Details

Risk is updated.

142382 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 libgcrypt-devel-9646 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-5270

Update Details

Risk is updated.

177967 - Gentoo Linux GLSA-201408-10 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Low

CVE: CVE-2014-5270

Update Details

Risk is updated.

184541 - Ubuntu Linux 10.04, 12.04, 14.04 USN-2339-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-5270

Update Details

Risk is updated.

184546 - Ubuntu Linux 10.04, 12.04 USN-2339-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-5270

Update Details

Risk is updated.

2327 - DNS Dynamic Updates

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Informational

CVE: CVE-1999-0184

DISA IAVA: 2003-B-0001,2002-T-0010,2002-A-0006(v1),2002-A-0006,2001-A-0001

Update Details

FASLScript is updated.

DELETED CHECKS

14444 - Oracle Fusion Middleware HTTP Server Apache HTTPD Denial Of Service

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

Risk Level: High

CVE: CVE-2011-3192

DISA IAVA: 2011-A-0141,2011-A-0130

ADDITIONAL NOTES

14444 - is deleted due to FP in certain situations.

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.