2014-OCT-22

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

17284 - Cisco Nexus Multiple Products GNU Bash Environment Variable Command Injection Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6271, CVE-2014-7169

Description

Multiple vulnerabilities are present in some versions of Cisco NX-OS.

Observation

Cisco NX-OS is Cisco Nexus switches Operating System.

Multiple vulnerabilities are present in some versions of Cisco NX-OS. The flaws lie in the embedded version of Bash. Successful exploitation could allow an attacker to execute remote code or cause a denial of service condition.

17300 - Drupal Database Abstraction API SQL Injection Vulnerability

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

Risk Level: High

CVE: CVE-2014-3704

Description

A SQL injection vulnerability is present in some versions of Drupal.

Observation

Drupal is a popular open source content management system.

A SQL injection vulnerability is present in some versions of Drupal. The flaw lies in a database abstraction API in Drupal 7.x. Successful exploitation by a remote attacker could lead to privilege escalation, arbitrary code execution or other attacks.

17312 - Vulnerability in Microsoft OLE Could Allow Remote Code Execution (3010060)

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

Risk Level: High

CVE: CVE-2014-6352

Description

A vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is an industrial standard operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in OLE object handling. Successful exploitation could allow an attacker to execute arbitrary code.

17178 - Schneider Electric SCADA Expert ClearSCADA Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-5411, CVE-2014-5412, CVE-2014-5413

Description

Multiple vulnerabilities are present in some versions of Schneider Electric ClearScada.

Observation

Schneider Electric ClearScada.is a supervisory control and data acquisition software used for managing critical infrastructure.

Multiple vulnerabilities are present in some versions of Schneider Electric ClearScada. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code or cause a denial of service condition.

17213 - WordPress Multiple Vulnerabilities Prior To 3.9.2

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

Risk Level: Medium

CVE: CVE-2014-2053, CVE-2014-5203, CVE-2014-5204, CVE-2014-5205, CVE-2014-5240

Description

Multiple vulnerabilities are present in some versions of WordPress.

Observation

WordPress is a popular blogging tool.

Multiple vulnerabilities are present in some versions of WordPress. Successful exploitation could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.

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.

17180 - Mozilla Firefox 32 NSS RSA Signature Security Bypass (BERserk)

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

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17181 - Mozilla Firefox ESR 24.8 NSS RSA Signature Security Bypass (BERserk)

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

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17182 - Mozilla Firefox ESR 31.1 NSS RSA Signature Security Bypass (BERserk)

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

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17183 - Mozilla Firefox 32 NSS RSA Signature Security Bypass (BERserk)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17184 - Mozilla Firefox ESR 24.8 NSS RSA Signature Security Bypass (BERserk)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17185 - Mozilla Firefox ESR 31.1 NSS RSA Signature Security Bypass (BERserk)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17188 - Mozilla Thunderbird 31 NSS RSA Signature Security Bypass (BERserk)

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

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17189 - Mozilla Thunderbird 31 NSS RSA Signature Security Bypass (BERserk)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17190 - Mozilla Thunderbird 24 NSS RSA Signature Security Bypass (BERserk)

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

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17191 - Mozilla Thunderbird 24 NSS RSA Signature Security Bypass (BERserk)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17192 - Mozilla SeaMonkey 2.29 NSS RSA Signature Security Bypass (BERserk)

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

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

17193 - Mozilla SeaMonkey 2.29 NSS RSA Signature Security Bypass (BERserk)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-1568

DISA IAVA: 2014-A-0145

Update Details

Recommendation is updated.

16680 - OpenSSL Multiple MITM and DTLS Invalid Fragment Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-0195, CVE-2014-0224

DISA IAVA: 2014-B-0080,2014-A-0083

Update Details

FASLScript is updated.

17210 - GNU Bash read_token_word parse.y Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-7187

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.