

MCAFFEE 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

20944 - Novell iManager Multiple Vulnerabilities Prior To 2.7 Support Pack 7 Patch 8

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

Risk Level: High

CVE: CVE-2013-1088, CVE-2013-3268, CVE-2015-4000

Description

Multiple vulnerabilities are present in some versions of Novell (NetIQ) iManager.

Observation

Novell iManager is a web-based administration console.

Multiple vulnerabilities are present in some versions of Novell (NetIQ) iManager. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct cipher-downgrade attacks, or hijack the authentication of a logged-in user to perform certain actions.

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.

4188 - Microsoft W3Who ISAPI Connection Headers Cross Site Scripting

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

Risk Level: High

CVE: CVE-2004-1133, CVE-2004-1134

Update Details

Recommendation is updated

4899 - Microsoft Visual Studio .CNT Buffer Overflow

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

Risk Level: High

CVE: CVE-2007-0352, CVE-2007-0427

Update Details

Recommendation is updated

4905 - Microsoft Visual Studio .HPJ Buffer Overflow

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

Risk Level: High

CVE: CVE-2007-0352, CVE-2007-0427

Update Details

Recommendation is updated

5431 - Microsoft Internet Explorer FTP Access Information Disclosure

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

Risk Level: High

CVE: CVE-2007-4356

Update Details

Recommendation is updated

5671 - Microsoft Visual InterDev .sln Vulnerability

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

Risk Level: High

CVE: CVE-2008-0250, CVE-2008-1709

Update Details

Recommendation is updated

5867 - Microsoft Internet Explorer Cross-Zone Scripting Vulnerability

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

Risk Level: High

CVE: CVE-2008-2281

Update Details

Recommendation is updated

10786 - Microsoft Outlook File Attachment Denial Of Service Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14352 - Microsoft Office Excel WriteAV Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14540 - Microsoft Internet Explorer Remote Stack Overflow Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17221 - Microsoft Internet Explorer ScriptEngine Use-After-Free Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18532 - Microsoft Internet Explorer Isolated Heap MemoryProtection ASLR Security Bypass

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

5065 - Microsoft Windows HLP File Handling Heap Buffer Overflow

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

Risk Level: High

CVE: CVE-2007-1912

[Update Details](#)

Recommendation is updated

5242 - Microsoft Office MSODataSourceControl ActiveX Control Vulnerability

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

Risk Level: High

CVE: CVE-2007-3282

[Update Details](#)

Recommendation is updated

9340 - Microsoft SQL Server SQLExecutiveCmdExec Weak Password Encryption Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: High

CVE: CVE-1999-1556

[Update Details](#)

Recommendation is updated

14294 - Microsoft Office Picture Manager Memory Corruption Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

4723 - Microsoft Internet Explorer Window Injection Vulnerability

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

Risk Level: High

CVE: CVE-2004-1155

[Update Details](#)

Recommendation is updated

4997 - Microsoft Windows Explorer DOC File Crash

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

Risk Level: High

CVE: CVE-2007-1347

[Update Details](#)

Recommendation is updated

5182 - Microsoft Internet Information Services Remote DoS

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

Risk Level: High

CVE: CVE-2007-2897

[Update Details](#)

Recommendation is updated

5492 - Microsoft Windows Media Player HTML Backdooring Vulnerability

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

Risk Level: High

CVE: CVE-2007-5095

[Update Details](#)

Recommendation is updated

6007 - Microsoft Internet Explorer Cookie Session Fixation

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

Risk Level: High

CVE: CVE-2008-3173

[Update Details](#)

Recommendation is updated

9270 - Microsoft Visual FoxPro FPOLE.OCX ActiveX Control Remote Command Execution Vulnerability

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

Risk Level: High

CVE: CVE-2007-5322

[Update Details](#)

Recommendation is updated

10610 - Microsoft Internet Explorer 'window.onerror' Information Disclosure

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11008 - Microsoft Windows Ipv6 Router Advertisement Denial Of Service

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

Risk Level: High

CVE: CVE-2010-4669

[Update Details](#)

Recommendation is updated

11890 - Microsoft Reader Integer Overflow

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11898 - Microsoft Reader Heap Overflow Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11899 - Microsoft Reader Integer Overflow Denial of Service II

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11902 - Microsoft Reader NULL Byte Write Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11903 - Microsoft Reader Array Overflow Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13144 - Microsoft Windows Media Player Null Pointer Remote Denial Of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13579 - Microsoft Visual Studio Incremental Linker Integer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18719 - Microsoft Internet Explorer Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

185496 - Ubuntu Linux 14.04 USN-3149-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185498 - Ubuntu Linux 12.04 USN-3149-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185500 - Ubuntu Linux 16.04 USN-3151-4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185502 - Ubuntu Linux 12.04 USN-3150-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185503 - Ubuntu Linux 16.10 USN-3152-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185505 - Ubuntu Linux 16.04 USN-3151-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185509 - Ubuntu Linux 16.10 USN-3152-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185510 - Ubuntu Linux 14.04 USN-3151-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185514 - Ubuntu Linux 12.04 USN-3150-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

185516 - Ubuntu Linux 16.04 USN-3151-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655

[Update Details](#)

Risk is updated

4973 - Microsoft Internet Explorer HTML Tag Information Disclosure

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

Risk Level: Medium

CVE: CVE-2007-3406

[Update Details](#)

Recommendation is updated

5601 - Microsoft Windows Pseudo-Random Number Generator Design Flaw

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

Risk Level: Medium

CVE: CVE-2007-6043

[Update Details](#)

Recommendation is updated

6545 - Microsoft Windows GDI+ EMF Stack Overflow Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-1217

[Update Details](#)

Recommendation is updated

6982 - Microsoft Internet Explorer findText Parsing Denial-of-Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-2655

[Update Details](#)

Recommendation is updated

8213 - Microsoft Virtual PC Hypervisor Memory Protection Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

8299 - Microsoft Internet Explorer Unspecified Heap Overflow Vulnerability (CVE-2010-1117)

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

Risk Level: Medium

CVE: CVE-2010-1117

[Update Details](#)

Recommendation is updated

5457 - Microsoft Internet Explorer Saved Web Page Cross-Site Scripting

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

Risk Level: Medium

CVE: CVE-2007-4478

[Update Details](#)

Recommendation is updated

5488 - Microsoft Visual Studio PDWizard Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2007-4891

[Update Details](#)

Recommendation is updated

5511 - Microsoft Internet Explorer OnKeyDown Focus Information Disclosure

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

Risk Level: Medium

CVE: CVE-2007-5158

[Update Details](#)

Recommendation is updated

8502 - Microsoft Office Communicator (Beta) SIP Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

8688 - Microsoft Windows "SfnLOGONNOTIFY()" And "SfnINSTRING()" Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

8691 - Microsoft Internet Explorer XSS Filter Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2010-1489

Update Details

Recommendation is updated

8937 - Microsoft Internet Explorer UTF-7 Charset Inheritance Cross Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2007-1114

Update Details

Recommendation is updated

9331 - Microsoft SQL Server Login Weak Password Encryption Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: Medium

CVE: CVE-2002-1872

Update Details

Recommendation is updated

9671 - Microsoft Internet Explorer Frame Border Property Denial Of Service Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

10558 - Microsoft Windows Environment Variable Expansion Library Loading Vulnerability (329308)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2007-6753

[Update Details](#)

Recommendation is updated

10918 - Microsoft Remote Access Phonebook Insecure Executable Loading Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

11914 - Microsoft Windows Live Safety Scanner One Care Local Download And Execute Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12531 - Microsoft Internet Explorer 'ledvtool.dll' Malformed HTML Denial Of Service Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

12532 - Microsoft Windows DHCPv6 Packets Remote Denial Of Service

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14323 - Microsoft Windows NTFS.SYS via USB Local Code Execution

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14655 - Microsoft Internet Explorer Proxy Settings TCP Sessions Information Disclosure

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

Risk Level: Medium

CVE: CVE-2013-1450

[Update Details](#)

Recommendation is updated

14656 - Microsoft Internet Explorer Proxy Settings SSL Lock Icon Denial of Service

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

Risk Level: Medium

CVE: CVE-2013-1451

[Update Details](#)

Recommendation is updated

16177 - Microsoft Windows Movie Maker wav File Handling Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-4858

[Update Details](#)

Recommendation is updated

16473 - Microsoft Windows Media Player Crafted WAV File Denial of Service

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

Risk Level: Medium

CVE: CVE-2014-2671

[Update Details](#)

Recommendation is updated

16499 - Microsoft Office XML Parser Nested Entity References Denial of Service

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

Risk Level: Medium

CVE: CVE-2014-2730

[Update Details](#)

Recommendation is updated

16666 - Microsoft Windows DHCP INFORM Configuration Overwrite Security Bypass

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16918 - Microsoft Office SharePoint Server 2007 Source Code Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-3830

[Update Details](#)

Documentation is updated

7139 - Microsoft Internet Explorer URL Spoofing Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-3003

[Update Details](#)

Recommendation is updated

14241 - Microsoft Office Excel ReadAV Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2012-5672

[Update Details](#)

Recommendation is updated

17153 - Microsoft Internet Explorer onreadystatechange Use After Free Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

17515 - Microsoft Windows "xxxMenuWindowProc()" Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

4685 - Microsoft PowerPoint 2003 Zero-Day Vulnerability

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

Risk Level: Low

CVE: CVE-2006-5296

Update Details

Recommendation is updated

6245 - Microsoft Windows LDAP Bind Request Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> BruteForce

Risk Level: Low

CVE: CVE-2008-5112

Update Details

Recommendation is updated

9410 - Microsoft Internet Explorer CSS 'expression' Remote Denial of Service Vulnerability

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

9822 - Microsoft Windows Kerberos "Pass The Ticket" Replay Vulnerability

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12437 - Microsoft Windows CSRSS SrvGetConsoleTitle Type Casting Weakness Information Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12840 - Microsoft Windows Local DNS Poisoning Vulnerabilities

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

13143 - Microsoft Windows Explorer Local Denial Of Service Vulnerability

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14271 - Microsoft Internet Explorer XSS Filter Bypass

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14354 - Microsoft Windows Phone 7 SSL Certificate 'Common Name' Validation Security Bypass Vulnerability

Category: Wireless Assessment -> NonIntrusive -> WinMobile

Risk Level: Low

CVE: CVE-2012-2993

[Update Details](#)

Recommendation is updated

17632 - Microsoft Windows NtPowerInformation Admin Check Security Bypass

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

1022 - Microsoft SQL Server UDP 1434 Database Instance TCP Information Disclosure

Category: General Vulnerability Assessment -> NonIntrusive -> Windows

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

13133 - Microsoft Windows NetBIOS NULL Name Denial Of Service Vulnerability

Category: Windows Host Assessment -> No Credentials Required

Risk Level: Informational

CVE: CVE-2000-0347

[Update Details](#)

Recommendation is updated Risk is updated Documentation is updated

45000 - ShellLogon.fasI3

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.

MCAFFEE 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.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2016 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates