2013-NOV-12

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

15845 - NETGEAR WNDR3700v4 ping6 Diagnostic Page Command Injection Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: High

Description

A command injection vulnerability is present in some versions of NETGEAR WNDR3700v4 router's firmware.

Observation

NETGEAR WNDR3700v4 is a wireless router.

A command injection vulnerability is present in some versions of NETGEAR WNDR3700v4 router's firmware. The flaw lies in ping6_traceroute6_hidden_info.htm. Successful exploitation could allow an attacker to execute arbitrary command.

15852 - BlackBerry PlayBook OS libexif Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Blackberry

Risk Level: High

CVE: CVE-2012-2812, CVE-2012-2813, CVE-2012-2814, CVE-2012-2836, CVE-2012-2837, CVE-2012-2840, CVE-2012-2841, CVE-2012-2845

Description

Multiple vulnerabilities are present in some versions of BlackBerry PlayBook OS.

Observation

BlackBerry PlayBook OS is a popular mobile device's operating system.

Multiple vulnerabilities are present in some versions of BlackBerry PlayBook OS. The flaws lie in the bundled libexif library. Successful exploitation of the vulnerabilities could allow an attacker to execute remote code, access private information or cause a denial of service on the affected device.

15853 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 17.0.10

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

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-5590, CVE-2013-5595, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5604

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition or execute arbitrary code.

15854 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 17.0.10

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-5590, CVE-2013-5595, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5604

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition or execute arbitrary code.

15855 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 24.1

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

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-5590, CVE-2013-5591, CVE-2013-5593, CVE-2013-5595, CVE-2013-5596, CVE-2013-5597, CVE-2013-5598, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5603, CVE-2013-5604

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct clickjacking attacks, cause a denial of service condition or execute arbitrary code.

15856 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 24.1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-5590, CVE-2013-5591, CVE-2013-5593, CVE-2013-5595, CVE-2013-5596, CVE-2013-5597, CVE-2013-5598, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5603, CVE-2013-5604

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct clickjacking attacks, cause a denial of service condition or execute arbitrary code.

15860 - Nullsoft Winamp 'gen_ff.dll' Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2009-1831

Description

A vulnerability in Nullsoft Winamp may allow remote code execution.

Observation

A vulnerability in Nullsoft Winamp may allow remote code execution.

The Nullsoft Modern Skins Support module (gen_ff.dll) in Nullsoft Winamp before 5.552 allows remote attackers to execute arbitrary code via a crafted MAKI file, which triggers an incorrect sign extension, and integer overflow, and a stack-based buffer overflow.

15861 - Mozilla Seamonkey Multiple Vulnerabilities Prior To 2.22

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

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-5590, CVE-2013-5591, CVE-2013-5592, CVE-2013-5593, CVE-2013-5595, CVE-2013-5596, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5603, CVE-2013-5604

Description

Multiple vulnerabilities are present in some versions of Mozilla SeaMonkey.

Observation

Mozilla SeaMonkey is an Internet application suite.

Multiple vulnerabilities are present in some versions of Mozilla SeaMonkey. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition or execute arbitrary code.

15862 - Mozilla Seamonkey Multiple Vulnerabilities Prior To 2.22

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-1739, CVE-2013-5590, CVE-2013-5591, CVE-2013-5592, CVE-2013-5593, CVE-2013-5595, CVE-2013-5596, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5603, CVE-2013-5604

Description

Multiple vulnerabilities are present in some versions of Mozilla SeaMonkey.

Observation

Mozilla SeaMonkey is an Internet application suite.

Multiple vulnerabilities are present in some versions of Mozilla SeaMonkey. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition or execute arbitrary code.

15910 - (MS13-090) Cumulative Security Update of ActiveX Kill Bits (2900986)

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

Risk Level: High

CVE: CVE-2013-3918

Microsoft ID: MS13-090

Microsoft KB: 2900986

Description

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

Observation

Microsoft Windows is a popular operating system.

A remote code execution vulnerability is present in some versions of Microsoft Windows. The flaw lies in the InformationCardSigninHelper Class ActiveX control. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to visit a malicious website.

Microsoft has provided MS13-090 to address this issue. The host appears to be missing this patch.

15912 - (MS13-089) Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (2876331)

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

Risk Level: High

CVE: CVE-2013-3940

Microsoft ID: MS13-089

Microsoft KB: 2876331

Description

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

Observation

Microsoft Windows is a popular operating system.

A remote code execution vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Windows Graphics Device Interface (GDI). Successful exploitation by a remote attacker could result in the execution of arbitrary code.

Microsoft has provided MS13-089 to address these issues. The host appears to be missing this patch.

15928 - (MS13-088) Cumulative Security Update for Internet Explorer (2888505)

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

Risk Level: High

CVE: CVE-2013-3871, CVE-2013-3908, CVE-2013-3909, CVE-2013-3910, CVE-2013-3911, CVE-2013-3912, CVE-2013-3914, CVE-2013-3915, CVE-2013-3916, CVE-2013-3917

Description

Multiple vulnerabilities are present in some versions of Microsoft Internet Explorer.

Observation

Microsoft Internet Explorer is a popular Internet web browser.

Multiple vulnerabilities are present in some versions of Microsoft Internet Explorer. The majority of the flaws are due to multiple memory errors. Successful exploitation could allow an attacker to execute arbitrary code.

Microsoft has provided MS13-088 to address these issues. The host appears to be missing this patch.

15932 - (MS13-091) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2885093)

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

Risk Level: High

CVE: CVE-2013-0082, CVE-2013-1324, CVE-2013-1325

Microsoft ID: MS13-091

Microsoft KB: 2885093

Description

Multiple vulnerabilities are present in some versions of Microsoft Office.

Observation

Microsoft Office is a popular office suite.

Multiple vulnerabilities are present in some versions of Microsoft Office. The flaws lies in the parsing of WordPerfect documents. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious file.

Microsoft has provided MS13-091 to address these issues. The host appears to be missing this patch.

15933 - (MS13-093) Microsoft Windows Ancillary Function Driver Information Disclosure (2875783)

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

Risk Level: High

CVE: CVE-2013-3887

Microsoft ID: MS13-093

Microsoft KB: 2875783

Description

An information disclosure vulnerability is present in some versions of Microsoft Windows.

Observation

An information disclosure vulnerability is present in some versions of Microsoft Windows.

The flaw lies in the handling of data when it is being copied between the kernel and user memory. Successful exploitation could allow an attacker to obtain sensitive information. The exploit requires the attacker to have valid credentials for the vulnerable system.

15934 - (MS13-093) Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3887

Microsoft ID: MS13-093

Microsoft KB: 2875783

Description

An information disclosure vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operating system.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in the handling of data when it is being copied between the kernel and user memory. Successful exploitation could allow an attacker to obtain sensitive information. The exploit requires the attacker to have valid credentials for the vulnerable system.

Microsoft has provided MS13-093 to address these issues. The host appears to be missing this patch.

15938 - (APSB13-26) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2013-5329, CVE-2013-5330

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in multiple core components. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service condition.

The update provided by Adobe bulletin APSB13-26 resolves the issues. The target system is missing this update.

15883 - Cogent DataHub HTTP Server POST Denial of Service Vulnerability

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

Risk Level: Medium

Description

A denial of service vulnerability is present in some versions of Cogent DataHub.

Observation

Cogent DataHub is a popular real-time data solution.

A denial of service vulnerability is present in some versions of Cogent DataHub. The flaw is due to an error when handling specially crafted HTTP POST requests. Successful exploitation by a remote attacker could result in a denial of service.

15901 - Wireshark Multiple Vulnerabilities Prior To 1.8.11

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

Risk Level: Medium

CVE: CVE-2013-6336, CVE-2013-6337, CVE-2013-6338, CVE-2013-6339, CVE-2013-6340

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is an industry standard network protocol analyzer.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple components of Wireshark such as the TCP, NBAP, OpenWire and IEEE 802.15.4 dissectors. Successful exploitation could allow execution of arbitrary code.

15902 - Wireshark Multiple Vulnerabilities Prior To 1.10.3

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

Risk Level: Medium

CVE: CVE-2013-6336, CVE-2013-6337, CVE-2013-6338, CVE-2013-6339, CVE-2013-6340

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is an industry standard network protocol analyzer.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple components of Wireshark such as the TCP, NBAP, OpenWire and IEEE 802.15.4 dissectors. Successful exploitation could allow execution of arbitrary code.

15907 - (MS13-095) Microsoft Windows XML Digital Signatures Denial of Service (2868626)

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

Risk Level: Medium

CVE: CVE-2013-3869

Microsoft ID: MS13-095

Microsoft KB: 2868626

Description

A denial of service vulnerability is present in some versions of Microsoft Windows.

Observation

A denial of service vulnerability is present in some versions of Microsoft Windows.

The flaw is related to the .NET implementation of XML Digital Signatures and is due to how X.509 certificates are parsed. Successful exploitation by a remote attacker could result in a denial of service condition.

15908 - (MS13-095) Vulnerability in XML Digital Signatures Could Allow Denial of Service (2868626)

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

Risk Level: Medium

CVE: CVE-2013-3869

Microsoft ID: MS13-095

Microsoft KB: 2868626

Description

A denial of service vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operating system.

A denial of service vulnerability is present in some versions of Microsoft Windows. The flaw lies in the implementation of X.509 certificate parsing component. Successful exploitation could allow an attacker to cause a denial of service condition.

Microsoft has provided MS13-095 to address these issues. The host appears to be missing this patch.

15909 - (MS13-089) Microsoft Windows Graphics Device Interface Remote Code Execution (2876331)

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

Risk Level: Medium

CVE: CVE-2013-3940

Microsoft ID: MS13-089

Microsoft KB: 2876331

Description

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

Observation

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

The flaw lies in the handling of Write files in Wordpad by the Graphics Device Interface. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious file.

15911 - (MS13-090) Microsoft ActiveX KillBits InformationCardSigninHelper Remote Code Execution (2900986)

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

Risk Level: Medium

CVE: CVE-2013-3918

Microsoft ID: MS13-090

Microsoft KB: 2900986

Description

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

Observation

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

The flaw lies in the InformationCardSigninHelper Class ActiveX control. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to visit a malicious website. Recent informations have reported that exploits for this vulnerability have been seen. The exploits include the following hashes:

660ebfb2c3148a0467f658e340849721
acbc249061a6a2fb09271a68d53567d9
104130d666ab3f640255140007f0b12d
90a37e54c53ffb78969644b1a7038e8c
20854f54b0d03118681410245be39bd8

15913 - (MS13-094) Microsoft Outlook S/MIME AIA Information Disclosure (2894514)

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

Risk Level: Medium

CVE: CVE-2013-3905

Microsoft ID: MS13-094

Microsoft KB: 2894514

Description

A information disclosure vulnerability is present in some versions of Microsoft Outlook.

Observation

A information disclosure vulnerability is present in some versions of Microsoft Outlook.

The flaw lies in the handling of S/MIME certificate data. Successful exploitation could allow an attacker to obtain sensitive information. The exploit requires the user to open an email with a malicious certificate attached.

15914 - (MS13-094) Vulnerability In Microsoft Outlook Could Allow Information Disclosure (2894514)

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

Risk Level: Medium

CVE: CVE-2013-3905

Microsoft ID: MS13-094

Microsoft KB: 2894514

Description

An information disclosure vulnerability is present in some versions of Microsoft Outlook.

Observation

Microsoft Office is a very popular office suite for Microsoft Windows and Mac OS X operating systems.

An information disclosure vulnerability is present in some versions of Microsoft Outlook. The flaw lies in the parsing of special email messages. Successful exploitation could allow an attacker to disclose information. The exploit requires the user to open a malicious email.

Microsoft has provided MS13-094 to address this issue. The host appears to be missing this patch.

15915 - (MS13-092) Vulnerability In Hyper-V Could Allow Elevation of Privilege (2893986)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3898

Microsoft ID: MS13-092

Microsoft KB: 2893986

Description

An elevation of privilege vulnerability exists in Hyper-V on Windows Server 8 and Windows Server 2012.

Observation

Microsoft Windows is a popular operating system.

An elevation of privilege vulnerability exists in Hyper-V on Windows Server 8 and Windows Server 2012. Hyper-V is a hypervisor-based technology that is a key feature of Windows Server. The flaw is caused by the insufficient validation of specific sequences of machine instructions by Hyper-V. Successful exploitation could allow an attacker to elevate its privilege.

Microsoft has provided MS13-092 to address this issue. The host appears to be missing this patch.

15916 - (MS13-092) Microsoft Windows Hyper-V Address Corruption Privilege Escalation (2893986)

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

Risk Level: Medium

CVE: CVE-2013-3898

Microsoft ID: MS13-092

Microsoft KB: 2893986

Description

A privilege escalation vulnerability is present in some versions of Microsoft Windows.

Observation

A privilege escalation vulnerability is present in some versions of Microsoft Windows.

The flaw lies in the improper verification of data structures. Successful exploitation could allow an attacker to execute commands with elevated privileges. The exploit requires the attacker to have valid credentials and administrator privileges for the vulnerable virtual machine.

15917 - (MS13-088) Microsoft Internet Explorer CSS Characters Information Disclosure (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3909

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

A information disclosure vulnerability is present in some versions of Microsoft Internet Explorer.

Observation

A information disclosure vulnerability is present in some versions of Microsoft Internet Explorer.

The flaw lies in the handling of CSS special characters. Successful exploitation could allow an attacker to obtain sensitive information. The exploit requires the user to visit a malicious website.

15918 - (MS13-088) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3910

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

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

Observation

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

The flaw is due to Internet Explorer improperly accessing an object in memory. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15919 - (MS13-088) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3911

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

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

Observation

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

The flaw is due to Internet Explorer improperly accessing an object in memory. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15920 - (MS13-088) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3912

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

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

Observation

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

The flaw is due to Internet Explorer improperly accessing an object in memory. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15921 - (MS13-088) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3914

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

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

Observation

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

The flaw is due to Internet Explorer improperly accessing an object in memory. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15922 - (MS13-088) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3915

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

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

Observation

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

The flaw is due to Internet Explorer improperly accessing an object in memory. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15923 - (MS13-088) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3916

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

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

Observation

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

The flaw is due to Internet Explorer improperly accessing an object in memory. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15924 - (MS13-088) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3917

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

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

Observation

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

The flaw is due to Internet Explorer improperly accessing an object in memory. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15925 - (MS13-088) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3871

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

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

Observation

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

The flaw is due to Internet Explorer improperly accessing an object in memory. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15926 - (MS13-088) Microsoft Internet Explorer Print Preview Information Disclosure (2888505)

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

Risk Level: Medium

CVE: CVE-2013-3908

Microsoft ID: MS13-088

Microsoft KB: 2888505

Description

A information disclosure vulnerability is present in some versions of Microsoft Internet Explorer.

Observation

A information disclosure vulnerability is present in some versions of Microsoft Internet Explorer.

The flaw lies in the handling of print previews. Successful exploitation could allow an attacker to obtain sensitive information. The exploit requires the user to create a print preview of a malicious website.

15929 - (MS13-091) Microsoft Office Word Buffer Overflow Remote Code Execution (2885093)

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

Risk Level: Medium

CVE: CVE-2013-1324

Microsoft ID: MS13-091

Microsoft KB: 2885093

Description

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

Observation

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

The flaw lies in the parsing of WordPerfect documents. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious file.

15930 - (MS13-091) Microsoft Office Word Heap Overwrite Remote Code Execution (2885093)

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

Risk Level: Medium

CVE: CVE-2013-1325

Microsoft ID: MS13-091

Microsoft KB: 2885093

Description

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

Observation

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

The flaw lies in the parsing of WordPerfect documents. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious file.

15931 - (MS13-091) Microsoft Office WPD File Format Remote Code Execution (2885093)

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

Risk Level: Medium

CVE: CVE-2013-0082

Microsoft ID: MS13-091

Microsoft KB: 2885093

Description

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

Observation

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

The flaw lies in the parsing of WordPerfect documents. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious file.

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.

13294 - (MS12-009) Vulnerabilities In Ancillary Function Driver Could Allow Elevation Of Privilege (2645640)

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

Risk Level: High

CVE: CVE-2012-0148, CVE-2012-0149

Microsoft ID: MS12-009

Update Details

Observation is updated.

15312 - Dell iDRAC Web Interface testurls BackDoor Page

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

Risk Level: High

CVE: CVE-2013-4785

Update Details

FASLScript is updated.

15689 - Mitsubishi MC-WorkX IcoLaunch ActiveX Control Remote Code Execution Vulnerability

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

Risk Level: High

Update Details

Recommendation is updated.

15759 - Cogent DataHub Two Vulnerabilities

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

Risk Level: High

Update Details

Recommendation is updated.

31514 - Sun Solaris 124997-01 Update Is Not Installed

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

Risk Level: High

Check Version: 1.3006

CVE: CVE-2007-0470

Update Details

Description is updated.
Observation is updated.
Recommendation is updated.
Risk is updated.

31517 - Sun Solaris 123368-01 Update Is Not Installed

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

Risk Level: High

Check Version: 1.3006

CVE: CVE-2007-0470

Update Details

Risk is updated.

31529 - Sun Solaris 124998-01 Update Is Not Installed

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

Risk Level: High

Check Version: 1.3006

CVE: CVE-2007-0470

Update Details

Risk is updated.

31533 - Sun Solaris 123369-01 Update Is Not Installed

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

Risk Level: High

Check Version: 1.3006

CVE: CVE-2007-0470

Update Details

Risk is updated.

31536 - Sun Solaris 124833-02 Update Is Not Installed

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

Risk Level: High

Check Version: 1.3240

CVE: CVE-2007-1003, CVE-2007-1351, CVE-2007-1352

DISA IAVA: 2009-A-0015

Update Details

Risk is updated.

8080 - Bugzilla Directory Access Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-3989

Update Details

Recommendation is updated.

8081 - Bugzilla Group Selection Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-3387

Update Details

Name is updated.

10440 - Bugzilla Directory Access Information Disclosure Vulnerability I

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

Risk Level: Medium

CVE: CVE-2009-3989

Update Details

Recommendation is updated.

10607 - Bugzilla Time Tracking Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2010-1204

Update Details

Recommendation is updated.

15423 - DotNetNuke DNNArticle Module "categoryid" SQL Injection Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-5117

Update Details

Recommendation is updated.

15600 - TP-LINK TD-W8951ND Router Cross-Site Scripting and Request Forgery Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

Update Details

Recommendation is updated.

15619 - Cisco Prime Network Control System (NCS) Health Monitor Login Page Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2012-5990

Update Details

Recommendation is updated.

12087 - Bugzilla localconfig Information Disclosure Vulnerability

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

Risk Level: Low

CVE: CVE-2010-0180

Update Details

Recommendation is updated.

31518 - Sun Solaris 123372-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
Check Version: 1.3006
CVE: CVE-2007-0895

Update Details
Risk is updated.

31519 - Sun Solaris 124830-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
Check Version: 1.3006
CVE: CVE-2006-5214, CVE-2006-5215

Update Details
Risk is updated.

31522 - Sun Solaris 124969-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
Check Version: 1.3006
CVE: CVE-2007-0895

Update Details
Risk is updated.

31534 - Sun Solaris 123373-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
Check Version: 1.3006
CVE: CVE-2007-0895

Update Details
Risk is updated.

31535 - Sun Solaris 124831-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
Check Version: 1.3006
CVE: CVE-2006-5214, CVE-2006-5215

Update Details

Risk is updated.

31538 - Sun Solaris 124970-01 Update Is Not Installed

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

Risk Level: Low

Check Version: 1.3006

CVE: CVE-2007-0895

Update Details

Risk is updated.

70014 - netbios-helpers.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

Update Details

FASLScript is updated.

DELETED CHECKS

8081 - Bugzilla Group Selection Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2009-3387

ADDITIONAL NOTES

8081 - was deleted due to False Positive issues. A future FSL script will be released to cover CVE-2009-3387

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.