2014-OCT-14

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

17223 - (MS14-057) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)

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

Risk Level: High

CVE: CVE-2014-4073, CVE-2014-4121, CVE-2014-4122

Microsoft ID: MS14-057

Microsoft KB: 3000414

Description

Multiple vulnerabilities exist in some versions of Microsoft Windows .NET Framework.

Observation

Microsoft .NET framework is a runtime and software framework for the Windows operating system.

Multiple vulnerabilities exist in some versions of Microsoft Windows .NET Framework. The flaw is due to how Microsoft .NET Framework handles specially crafted requests. Successful exploitation could allow a remote attacker to execute remote code, elevate its privileges or bypass security measures.

Microsoft has provided MS14-057 to address these issues. The host appears to be missing this patch.

17225 - (MS14-057) Microsoft .NET Framework Remote Code Execution (3000414)

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

Risk Level: High

CVE: CVE-2014-4121

Microsoft ID: MS14-057

Microsoft KB: 3000414

Description

A vulnerability in some versions of Microsoft .NET could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft .NET could lead to remote code execution.

The flaw occurs when Microsoft .NET framework fails to properly parse specially crafted internationalized resource identifiers resulting in memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17227 - (MS14-058) Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4113, CVE-2014-4148

Microsoft ID: MS14-058

Microsoft KB: 3000061

Description

Multiple vulnerabilities are present in the kernel-mode device drivers in some versions of Microsoft Windows.

Observation

The Windows kernel is the core of the Windows operating system.

Multiple vulnerabilities are present in the kernel-mode device drivers in some versions of Microsoft Windows. The flaws are due to improper handling of objects in memory by the the Windows kernel-mode drivers. Successful exploitation could allow a locally logged-in attacker to execute commands with elevated privileges in kernel mode and disclose memory addresses or other sensitive kernel information.

Microsoft has provided MS14-058 to address these issues. The host appears to be missing this patch.

17235 - (MS14-056) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4126

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17236 - (MS14-056) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4127

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17237 - (MS14-056) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4128

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17238 - (MS14-056) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4132

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17239 - (MS14-056) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4129

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17240 - (MS14-056) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4130

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17241 - (MS14-056) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4133

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17242 - (MS14-056) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4134

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17243 - (MS14-056) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4137

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17244 - (MS14-056) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4138

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17245 - (MS14-056) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4141

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17250 - (MS14-058) Microsoft Windows TrueType Font Parsing Remote Code Execution (3000061)

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

Risk Level: High

CVE: CVE-2014-4148

Microsoft ID: MS14-058

Microsoft KB: 3000061

Description

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw occurs when a Windows kernel-mode driver fails to properly handle TrueType fonts. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17257 - (MS14-061) Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)

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

Risk Level: High

CVE: CVE-2014-4117

Microsoft ID: MS14-061

Microsoft KB: 3000434

Description

A vulnerability is present in some versions of Microsoft Office.

Observation

Microsoft Office is a popular office suite.

A vulnerability is present in some versions of Microsoft Office. The flaw exists in the Microsoft Word component which does not properly handle objects in memory while parsing specially crafted Office files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious Word document.

Microsoft has provided MS14-061 to address these issue. The host appears to be missing this patch.

17259 - (MS14-061) Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-4117

Microsoft ID: MS14-061

Microsoft KB: 3000434

Description

A vulnerability is present in some versions of Microsoft Office.

Observation

Microsoft Office is a popular office suite.

A vulnerability is present in some versions of Microsoft Office. The flaw exists in the Microsoft Word component which does not properly handle objects in memory while parsing specially crafted Office files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious Word document.

Microsoft has provided MS14-061 to address these issue. The host appears to be missing this patch.

17260 - (MS14-062) Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (2993254)

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

Risk Level: High

Microsoft ID: MS14-062

Microsoft KB: 2993254

Description

A vulnerability in some versions of Microsoft Windows could lead to a privilege escalation.

Observation

Microsoft Windows is Microsoft operating system.

A vulnerability in some versions of Microsoft Windows could lead to a privilege escalation. The flaw occurs when the Message Queuing service improperly handles objects in memory by inadvertently allowing overwrite. Successful exploitation could allow a local user to gain elevated privileges.

Microsoft has provided MS14-062 to address this issue. The host appears to be missing this patch.

17262 - (MS14-063) Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege (2998579)

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

Risk Level: High

CVE: CVE-2014-4115

Microsoft ID: MS14-063

Microsoft KB: 2998579

Description

A vulnerability in some versions of Microsoft Windows Disk Partition could lead to a privilege escalation.

Observation

Microsoft Windows is Microsoft operating system.

A vulnerability in some versions of Microsoft Windows Disk Partition could lead to a privilege escalation. The flaw occurs when the FASTFAT driver executes a function that results in a buffer under-allocation issue. Successful exploitation could allow a local user to gain elevated privileges.

Microsoft has provided MS14-063 to address this issue. The host appears to be missing this patch.

17268 - (APSB14-22) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2014-0558, CVE-2014-0564, CVE-2014-0569

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 several components. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-22 resolves these issues. The target system is missing this update.

17269 - (APSB14-22) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0558, CVE-2014-0564, CVE-2014-0569

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 several components. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-22 resolves these issues. The target system is missing this update.

17224 - (MS14-057) Microsoft .NET Framework Address Space Layout Randomization Security Bypass (3000414)

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

Risk Level: Medium

CVE: CVE-2014-4122

Microsoft ID: MS14-057

Microsoft KB: 3000414

Description

A vulnerability in some versions of Microsoft .NET could lead to a security bypass.

Observation

A vulnerability in some versions of Microsoft .NET could lead to a security bypass.

The flaw exists when Microsoft .NET Framework does not use the Address Space Layout Randomization security feature. Successful exploitation could allow a remote attacker to bypass intended access restrictions.

17226 - (MS14-057) Microsoft .NET Framework ClickOnce Privilege Escalation (3000414)

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

Risk Level: Medium

CVE: CVE-2014-4073

Microsoft ID: MS14-057

Microsoft KB: 3000414

Description

A vulnerability in some versions of Microsoft .NET could lead to a privilege escalation.

Observation

A vulnerability in some versions of Microsoft .NET could lead to a privilege escalation.

The flaw occurs when Microsoft .NET Framework inadvertently processes data prior to verification. Successful exploitation could allow a local user to gain elevated privileges.

17228 - (MS14-058) Microsoft Windows Win32k.sys Privilege Escalation (3000061)

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

Risk Level: Medium

CVE: CVE-2014-4113

Microsoft ID: MS14-058

Microsoft KB: 3000061

Description

A vulnerability in some versions of Microsoft Windows could lead to a privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to a privilege escalation.

The flaw occurs when the Windows kernel-mode driver improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

17231 - (MS14-056) Cumulative Security Update for Internet Explorer (2987107)

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

Risk Level: Medium

CVE: CVE-2014-4123, CVE-2014-4124, CVE-2014-4126, CVE-2014-4127, CVE-2014-4128, CVE-2014-4129, CVE-2014-4130, CVE-2014-4132, CVE-2014-4133, CVE-2014-4134, CVE-2014-4137, CVE-2014-4138, CVE-2014-4140, CVE-2014-4141

Microsoft ID: MS14-056

Microsoft KB: 2987107

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 flaws are due to several memory corruption vulnerabilities. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS14-056 to address these issues. The host appears to be missing this patch.

17232 - (MS14-056) Microsoft Internet Explorer I Privilege Escalation (2987107)

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

Risk Level: Medium

CVE: CVE-2014-4123

Microsoft ID: MS14-056

Microsoft KB: 2987107

Description

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

Observation

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

The flaw lies in an error while validating permissions. Successful exploitation could allow an attacker to execute commands with elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

17233 - (MS14-056) Microsoft Internet Explorer II Privilege Escalation (2987107)

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

Risk Level: Medium

CVE: CVE-2014-4124

Microsoft ID: MS14-056

Microsoft KB: 2987107

Description

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

Observation

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

The flaw lies in an error while validating permissions. Successful exploitation could allow an attacker to execute commands with elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

17234 - (MS14-056) Microsoft Internet Explorer ASLR Security Bypass (2987107)

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

Risk Level: Medium

CVE: CVE-2014-4140

Microsoft ID: MS14-056

Microsoft KB: 2987107

Description

A security bypass vulnerability is present in some versions of Microsoft Internet Explorer.

Observation

A security bypass vulnerability is present in some versions of Microsoft Internet Explorer.

The flaw lies in the ASLR component. Successful exploitation could allow an attacker to bypass security measures. The exploit requires the user to open a vulnerable website, email or document.

17246 - (MS14-060) Microsoft Windows OLE Remote Code Execution (3000869)

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

Risk Level: Medium

CVE: CVE-2014-4114

Microsoft ID: MS14-060

Microsoft KB: 3000869

Description

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw occurs when a user downloads, or receives, and then opens a specially crafted Microsoft Office file which contains OLE objects. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17247 - (MS14-059) Microsoft ASP.NET MVC Feature Cross-Site Scripting (2990942)

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

Risk Level: Medium

CVE: CVE-2014-4075

Microsoft ID: MS14-059

Microsoft KB: 2990942

Description

A vulnerability in some versions of Microsoft ASP.NET could lead to cross-site scripting.

Observation

A vulnerability in some versions of Microsoft ASP.NET could lead to cross-site scripting.

The flaw occurs when ASP.NET MVC fails to properly encode input. Successful exploitation could allow a remote attacker to inject arbitrary web script or HTML code.

17249 - (MS14-060) Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869)

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

Risk Level: Medium

CVE: CVE-2014-4114

Microsoft ID: MS14-060

Microsoft KB: 3000869

Description

A vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is an industry standard operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in Windows OLE. Successful exploitation could allow an attacker to execute remote code within the security context of the current logged-on user.

Microsoft has provided MS14-060 to address this issue. The host appears to be missing this patch.

17251 - (MS14-059) Vulnerability in ASP.NET MVC Could Allow Security Feature Bypass (2990942)

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

Risk Level: Medium

CVE: CVE-2014-4075

Microsoft ID: MS14-059

Microsoft KB: 2990942

Description

A cross-site scripting vulnerability is present in some versions of Microsoft ASP.NET MVC.

Observation

Microsoft ASP.NET MVC is a popular framework for creating sophisticated applications that use the latest web standards.

A cross-site scripting vulnerability is present in some versions of Microsoft ASP.NET MVC. The flaw lies in ASP.NET MVC. Successful exploitation could allow an attacker to execute remote code into the user's web browser.

Microsoft has provided MS14-059 to address this issue. The host appears to be missing this patch.

17258 - (MS14-061) Microsoft Word File Format Remote Code Execution (3000434)

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

Risk Level: Medium

CVE: CVE-2014-4117

Microsoft ID: MS14-061

Microsoft KB: 3000434

Description

A vulnerability in some versions of Microsoft Word could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Word could lead to remote code execution.

The flaw occurs when Microsoft Word does not properly handle objects in memory while parsing specially crafted Office files. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17261 - (MS14-062) Microsoft Message Queuing Service Arbitrary Write Privilege Escalation (2993254)

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

Risk Level: Medium

CVE: CVE-2014-4971

Microsoft ID: MS14-062

Microsoft KB: 2993254

Description

A vulnerability in some versions of Microsoft MQAC could lead to a privilege escalation.

Observation

A vulnerability in some versions of Microsoft MQAC could lead to a privilege escalation.

The flaw occurs when the Message Queuing service improperly handles objects in memory by inadvertently allowing overwrite. Successful exploitation could allow a local user to gain elevated privileges.

17263 - (MS14-063) Microsoft Windows Disk Partition Driver Privilege Escalation (2998579)

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

Risk Level: Medium

CVE: CVE-2014-4115

Microsoft ID: MS14-063

Microsoft KB: 2998579

Description

A vulnerability in some versions of Microsoft Windows Disk Partition could lead to a privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows Disk Partition could lead to a privilege escalation.

The flaw occurs when the FASTFAT driver executes a function that results in a buffer under-allocation issue. Successful exploitation could allow a local user to gain elevated privileges.

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.

58833 - Debian Linux 7.0 DSA-2918-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1518, CVE-2014-1523, CVE-2014-1524, CVE-2014-1529, CVE-2014-1530, CVE-2014-1531, CVE-2014-1532

Update Details

Observation is updated.

58866 - Debian Linux 7.0 DSA-2955-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1533, CVE-2014-1538, CVE-2014-1541, CVE-2014-1545

Update Details

Observation is updated.

ADDITIONAL NOTES

1 - NuGet updates are not included as part of our Patch Tuesday coverage (MS14-059).

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.