2013-OCT-08

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

15693 - Cisco IOS Software Zone-Based Firewall and Content Filtering Denial of Service

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-5476

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

A denial of service vulnerability is present in some versions of Cisco IOS.

The flaw lies in the Zone-Based Firewall component. Successful exploitation by a remote attacker could result in a denial of service condition.

15694 - Cisco IOS Software Internet Key Exchange Memory Leak Denial of Service

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-5473

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

A denial of service vulnerability is present in some versions of Cisco IOS.

The flaw lies in the Internet Key Exchange (IKE) protocol. Successful exploitation by a remote attacker could result in a denial of service condition.

15695 - Cisco IOS Software DHCP Denial of Service

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-5475

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

A denial of service vulnerability is present in some versions of Cisco IOS.

The flaw lies in the DHCP implementation. Successful exploitation by a remote attacker could result in a denial of service condition.

15696 - Cisco IOS Software Multicast Network Time Protocol Denial of Service

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-5472

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

A denial of service vulnerability is present in some versions of Cisco IOS.

The flaw lies in the Network Time Protocol (NTP) feature. Successful exploitation by a remote attacker could result in a denial of service condition.

15697 - Cisco IOS Software Resource Reservation Protocol Interface Queue Wedge Denial of Service

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-5478

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

A denial of service vulnerability is present in some versions of Cisco IOS.

The flaw lies in the Resource Reservation Protocol (RSVP) feature. Successful exploitation by a remote attacker could result in a denial of service condition.

15698 - Cisco IOS Software IPv6 Virtual Fragmentation Reassembly Denial of Service

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-5474

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

A denial of service vulnerability is present in some versions of Cisco IOS.

The flaw lies in the virtual fragmentation reassembly (VFR) feature for IP version 6 (IPv6). Successful exploitation by a remote attacker could result in a denial of service condition.

15699 - Cisco IOS Software Queue Wedge Denial of Service

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-5477

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

A denial of service vulnerability is present in some versions of Cisco IOS.

The flaw lies in the T1/E1 driver queue implementation. Successful exploitation by a remote attacker could result in a denial of service condition.

15700 - (APSB13-25) Vulnerabilities In Adobe Acrobat And Reader

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

Risk Level: High

CVE: CVE-2013-5325

Description

A Javascript related vulnerability is present in some versions of Adobe Reader and Acrobat.

Observation

Adobe Reader and Acrobat are two popular software packages used to handle PDF files.

A Javascript related vulnerability is present in some versions of Adobe Reader and Acrobat. The flaw is due to a regression that occurred in the last update that allows the execution of Javascript scheme URIs when viewing PDF files within a browser. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB13-25 resolves this issue. The target system appears to be missing this update.

15702 - (MS13-085) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2885080)

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

Risk Level: High

CVE: CVE-2013-3889, CVE-2013-3890

Microsoft ID: MS13-085

Microsoft KB: 2870699

Description

Multiple vulnerabilities are present in some versions of Microsoft Excel.

Observation

Microsoft Excel is a popular spreadsheet application.

Multiple vulnerabilities are present in some versions of Microsoft Excel. The flaws lie in the way Excel parses and validate data when opening files. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS13-085 to address these issues. The host appears to be missing this patch.

15711 - (MS13-087) Vulnerability in Silverlight Could Allow Information Disclosure (2890788)

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

Risk Level: High

CVE: CVE-2013-3896

Microsoft ID: MS13-087

Microsoft KB: 2890788

Description

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

Observation

Microsoft Silverlight is a Microsoft framework for rich Internet applications.

An information disclosure vulnerability is present in some versions of Microsoft Silverlight. The flaw is due to how Silverlight handles objects in memory. Successful exploitation by a remote attacker could result in the exposure of private information.

Microsoft has provided MS13-087 to address this issue. The host appears to be missing this patch.

15717 - (MS13-087) Vulnerability in Silverlight Could Allow Information Disclosure (2890788)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-3896

Microsoft ID: MS13-087

Microsoft KB: 2890788

Description

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

Observation

Microsoft Silverlight is a Microsoft framework for rich Internet applications.

An information disclosure vulnerability is present in some versions of Microsoft Silverlight. The flaw is due to how Silverlight handles objects in memory. Successful exploitation by a remote attacker could result in the exposure of private information.

Microsoft has provided MS13-087 to address this issue. The host appears to be missing this patch.

15720 - (MS13-080) Cumulative Security Update for Internet Explorer (2879017)

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

Risk Level: High

CVE: CVE-2013-3871, CVE-2013-3872, CVE-2013-3873, CVE-2013-3874, CVE-2013-3875, CVE-2013-3882, CVE-2013-3885, CVE-2013-3886, CVE-2013-3893, CVE-2013-3897

Microsoft ID: MS13-080

Microsoft KB: 2879017

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 multiple memory errors. Successful exploitation could allow an attacker to execute arbitrary code.

Microsoft has provided MS13-080 to address these issues. The host appears to be missing this patch.

15721 - (MS13-084) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2885089)

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

Risk Level: High

CVE: CVE-2013-3889, CVE-2013-3895

Microsoft ID: MS13-084

Microsoft KB: 2885089

Description

Multiple vulnerabilities are present in some versions of Microsoft SharePoint.

Observation

Microsoft SharePoint Server is a popular business collaboration platform.

Multiple vulnerabilities are present in some versions of Microsoft SharePoint. The flaws are due to improper handling of objects in memory, user supplied input, and unassigned workflows, Successful exploitation could allow an attacker to gain elevated privileges or execute remote code.

Microsoft has provided MS13-084 to address these issues. The host appears to be missing this patch.

15724 - (MS13-083) Microsoft Windows Comctl32 Integer Overflow Remote Code Execution (2864058)

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

Risk Level: High

CVE: CVE-2013-3195

Microsoft ID: MS13-083

Microsoft KB: 2864058

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 Windows common control library. Successful exploitation by a remote attacker could result in the execution of arbitrary code if an affected system received a specially crafted web request to an ASP.NET web application.

15725 - (MS13-083) Vulnerability In Windows Common Control Library Could Allow Remote Code Execution (2864058)

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

Risk Level: High

CVE: CVE-2013-3195

Microsoft ID: MS13-083

Microsoft KB: 2864058

Description

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

Observation

Microsoft Windows is an industry standard operating system.

A remote code execution vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Windows common control library. Successful exploitation by a remote attacker could result in the execution of arbitrary code if an affected system received a specially crafted web request to an ASP.NET web application.

Microsoft has release MS13-083 to address this issue. The host appears to be missing this patch.

15726 - (MS13-086) Microsoft Word Memory Corruption I Remote Code Execution (2885084)

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

Risk Level: High

CVE: CVE-2013-3891

Microsoft ID: MS13-086

Microsoft KB: 2885084

Description

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

Observation

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

The flaw lies in the parsing of crafted files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious Word document.

15727 - (MS13-086) Microsoft Word Memory Corruption II Remote Code Execution (2885084)

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

Risk Level: High

CVE: CVE-2013-3892

Microsoft ID: MS13-086

Microsoft KB: 2885084

Description

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

Observation

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

The flaw lies in the parsing of crafted files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious Word document.

15728 - (MS13-082) Vulnerabilities In .NET Framework Could Allow Remote Code Execution (2878890)

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

Risk Level: High

CVE: CVE-2013-3128, CVE-2013-3860, CVE-2013-3861

Microsoft ID: MS13-082

Microsoft KB: 2878890

Description

Multiple vulnerabilities are present in some versions of Microsoft .NET Framework.

Observation

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

Multiple vulnerabilities are present in some versions of Microsoft .NET Framework. The flaws lie in how .NET framework handles OpenType fonts, XML digital signatures, and document type definitions in JSON data encodings. Successful exploitation could allow an attacker to cause a denial of services or execute remote code. The flaw requires the user to visit a malicious website.

Microsoft has provided MS13-082 to address these issues. The host appears to be missing this patch.

15729 - (MS13-086) Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2885084)

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

Risk Level: High

CVE: CVE-2013-3891, CVE-2013-3892

Microsoft ID: MS13-086

Microsoft KB: 2885084

Description

Multiple vulnerabilities are present in some versions of Microsoft Word.

Observation

Microsoft Office Word is a popular word processor.

Multiple vulnerabilities are present in some versions of Microsoft Word. The flaws are due to the parsing of crafted files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious Word document.

Microsoft has released MS13-086 to address this issue. The host appears to be missing this patch.

15734 - (MS13-081) Microsoft Windows TrueType Font CMAP Remote Code Execution (2870008)

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

Risk Level: High

CVE: CVE-2013-3894

Microsoft ID: MS13-081

Microsoft KB: 2870008

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 parsing for TrueType fonts. Successful exploitation could allow an attacker to execute remote code. The exploit requries the user to open a malicious file.

15740 - (MS13-081) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)

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

Risk Level: High

CVE: CVE-2013-3128, CVE-2013-3200, CVE-2013-3879, CVE-2013-3880, CVE-2013-3881, CVE-2013-3888, CVE-2013-3894

Microsoft ID: MS13-081

Microsoft KB: 2870008

Description

Multiple vulnerabilities are present in some versions of Microsoft Windows.

Observation

Microsoft Windows is an industry standard operating system.

Multiple vulnerabilities are present in some versions of Microsoft Windows. The flaws are due to the way Win32K handles OpenType Font and TrueType Font files and how it manage objects in memory. Successful exploitation could allow an attacker to execute arbitrary code.

Microsoft has provided MS13-081 to address these issues. The host appears to be missing this patch.

15751 - (MS13-081) Microsoft Windows Kernel-Mode Driver OpenType Font Parsing Remote Code Execution (2870008)

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

Risk Level: High

CVE: CVE-2013- 3128

Microsoft ID: MS13-081

Microsoft KB: 2870008

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 exists in the way that Windows parses specially crafted OpenType fonts (OTF). Successful exploitation by a remote attacker could result in the execution of arbitrary code.

15703 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution I (2885080)

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

Risk Level: Medium

CVE: CVE-2013-3889

Microsoft ID: MS13-085

Microsoft KB: 2885080

Description

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

Observation

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

The flaw is due to the way that Microsoft Excel parses content in Excel files. The attacker who successfully exploited this vulnerability could take complete control of an affected system and could result in the execution of arbitrary code.

15704 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution II (2885080)

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

Risk Level: Medium

CVE: CVE-2013-3890

Microsoft ID: MS13-085

Microsoft KB: 2885080

Description

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

Observation

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

The flaw is due to the way that Microsoft Excel parses content in Excel files. The attacker who successfully exploited this vulnerability could take complete control of an affected system and could result in the execution of arbitrary code.

15705 - (MS13-080) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3871

Microsoft ID: MS13-080

Microsoft KB: 2879017

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.

15706 - (MS13-080) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3872

Microsoft ID: MS13-080

Microsoft KB: 2879017

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.

15707 - (MS13-080) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3873

Microsoft ID: MS13-080

Microsoft KB: 2879017

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.

15708 - (MS13-080) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3874

Microsoft ID: MS13-080

Microsoft KB: 2879017

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.

15709 - (MS13-080) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3875

Microsoft ID: MS13-080

Microsoft KB: 2879017

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 the way Internet Explorer accesses objects that no longer exist. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15710 - (MS13-080) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3882

Microsoft ID: MS13-080

Microsoft KB: 2879017

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 the way Internet Explorer accesses objects that no longer exist. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15712 - (MS13-080) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3885

Microsoft ID: MS13-080

Microsoft KB: 2879017

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 the way Internet Explorer accesses objects that no longer exist. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15713 - (MS13-080) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3886

Microsoft ID: MS13-080

Microsoft KB: 2879017

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 the way Internet Explorer accesses objects that no longer exist. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious website.

15714 - (MS13-087) Microsoft Silverlight Information Disclosure (2890788)

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

Risk Level: Medium

CVE: CVE-2013-3896

Microsoft ID: MS13-087

Microsoft KB: 2890788

Description

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

Observation

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

The flaw exists in how Silverlight handles certain objects in memory. The attacker would have to convince users to visit a website, typically by getting them to click a link in email or IM message that would take them to the attacker's website. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

15715 - (MS13-080) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3897

Microsoft ID: MS13-080

Microsoft KB: 2879017

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.

15716 - (MS13-080) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2879017)

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

Risk Level: Medium

CVE: CVE-2013-3893

Microsoft ID: MS13-080

Microsoft KB: 2879017

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.

15719 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution I (2885080)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-3889

Microsoft ID: MS13-085

Microsoft KB: 2885080

Description

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

Observation

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

The flaw is due to the way that Microsoft Excel parses content in Excel files. The attacker who successfully exploited this vulnerability could take complete control of an affected system and could result in the execution of arbitrary code.

15722 - (MS13-084) Microsoft SharePoint Excel Remote Code Execution (2885089)

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

Risk Level: Medium

CVE: CVE-2013-3889

Microsoft ID: MS13-084

Microsoft KB: 2885089

Description

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

Observation

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

The flaw lies in the parsing of Excel content by Office Services and Webapps. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to access a malicious Excel file in a sharepoint location.

15723 - (MS13-084) Microsoft SharePoint Parameter Injection Privilege escalation (2885089)

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

Risk Level: Medium

CVE: CVE-2013-3895

Microsoft ID: MS13-084

Microsoft KB: 2885089

Description

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

Observation

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

The flaw lies in an error that allows an attacker to inject parameters. Successful exploitation could allow an attacker to execute commands with elevated privileges. The exploit requires the user to click on a malicious Sharepoint link.

15730 - (MS13-082) Microsoft .NET Framework JSON Parsing Denial of Service (2878890)

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

Risk Level: Medium

CVE: CVE-2013-3861

Microsoft ID: MS13-082

Microsoft KB: 2878890

Description

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

Observation

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

The flaw lies in the parsing of JSON data. Successful exploitation could allow an attacker to cause a denial of services.

15731 - (MS13-082) Microsoft .NET Framework Entity Expansion Denial of Service (2878890)

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

Risk Level: Medium

CVE: CVE-2013-3860

Microsoft ID: MS13-082

Microsoft KB: 2878890

Description

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

Observation

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

The flaw lies in the parsing of document type definition when a XML signature is validated. Successful exploitation could allow an attacker to cause a denial of service.

15732 - (MS13-082) Microsoft .NET Framework OpenType Font Remote Code Execution (2878890)

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

Risk Level: Medium

CVE: CVE-2013-3128

Microsoft ID: MS13-082

Microsoft KB: 2878890

Description

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

Observation

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

The flaw lies in the handling of OpenType Fonts residing in an XAML Browser application. Successful epxloitation could allow an attacker to execute remote code. The flaw requires the user to visit a malicious website.

15735 - (MS13-081) Microsoft Windows DirectX Graphics Kernel Subsystem Double Fetch Privilege Escalation (2870008)

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

Risk Level: Medium

CVE: CVE-2013-3888

Microsoft ID: MS13-081

Microsoft KB: 2870008

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 exists when the Microsoft DirectX graphics kernel subsystem (dxgkrnl.sys) improperly handles objects in memory. The local attacker could then run arbitrary code in kernel mode and gain elevated privileges.

15736 - (MS13-081) Microsoft Windows Win32k NULL Page Privilege Escalation (2870008)

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

Risk Level: Medium

CVE: CVE-2013-3881

Microsoft ID: MS13-081

Microsoft KB: 2870008

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 exists when the Windows kernel-mode driver improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges and allow them to install programs; view, change, or delete data; or create new accounts with full administrative rights.

15737 - (MS13-081) Microsoft Windows App Container Privilege Escalation (2870008)

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

Risk Level: Medium

CVE: CVE-2013-3880

Microsoft ID: MS13-081

Microsoft KB: 2870008

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 exists in the Windows App Container. The attacker must have valid logon credentials and run a malicious application to exploit this vulnerability. Successful exploitation could allow a local user to gain elevated privileges.

15738 - (MS13-081) Microsoft Windows Win32k Use After Free Privilege Escalation (2870008)

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

Risk Level: Medium

CVE: CVE 2013-3879

Microsoft ID: MS13-081

Microsoft KB: 2870008

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

15739 - (MS13-081) Microsoft Windows USB Descriptor Privilege Escalation (2870008)

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

Risk Level: Medium

CVE: CVE-2013-3200

Microsoft ID: MS13-081

Microsoft KB: 2870008

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 occurs when Windows USB drivers improperly handle objects in memory. 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.

15622 - IBM DB2 Security Bypass Vulnerability Prior To 10.5 Fix Pack 1

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2013-4033

Update Details

Recommendation is updated.

70046 - macosx.fasl3.inc

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

Risk Level: Informational

Check Version: 1.4378

Update Details

FASLScript is updated.

DELETED CHECKS

15632 - Microsoft Internet Explorer Memory Corruption Remote Code Execution (2887505)

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

Risk Level: High

CVE: CVE-2013-3893

Microsoft KB: 2887505

ADDITIONAL NOTES

15632 - was deleted and replaced by FID15716 (MS13-080)

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.