2013-DEC-11

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

15972 - Sybase Adaptive Server Enterprise Multiple Vulnerabilities In 15.x

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

Risk Level: High

Description

Multiple vulnerabilities are present in some versions of Sybase Adaptive Server Enterprise.

Observation

Sybase Adaptive Server Enterprise is a popular relational model database server.

Multiple vulnerabilities are present in some versions of Sybase Adaptive Server Enterprise. The flaws are present in multiple components of the software. Successful exploitation could allow malicious users to bypass certain security restrictions, obtain sensitive information, cause a denial of service condition, or execute arbitrary code.

15997 - Avira Secure Backup Multiple Registry Key Value Parsing Local Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2013-6356

Description

A buffer overflow vulnerability is present in some versions of Avira Secure Backup.

Observation

Avira Secure Backup is an online storage solution.

A buffer overflow vulnerability is present in some versions of Avira Secure Backup. The flaw is due to improperly validated lengths of fetched values from registry keys "AutoUpdateDownloadFilename" and "AutoUpdateProgressFilename". Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition. Exploitation requires an attacker to convince a user to import an arbitrary .reg file.

16013 - (MS13-096) Vulnerability In Microsoft Graphics Component Could Allow Remote Code Execution (2908005)

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

Risk Level: High

CVE: CVE-2013-3906

Microsoft ID: MS13-096

Microsoft KB: 2908005

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 a parsing error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to download a malicious file.

Microsoft has provided MS13-096 to address this issue. The host appears to be missing this patch.

16014 - (MS13-096) Microsoft Graphics Component Memory Corruption Remote Code Execution (2908005)

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

Risk Level: High

CVE: CVE-2013-3906

Microsoft ID: MS13-096

Microsoft KB: 2908005

Description

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

Observation

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

The flaw lies in the handling of TIFF images by the Graphics component that is present in versions of Windows, Office, and Lync. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious file or visit a malicious website.

16018 - (MS13-105) Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2915705)

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

Risk Level: High

CVE: CVE-2013-1330, CVE-2013-5072, CVE-2013-5763, CVE-2013-5791

Microsoft ID: MS13-105

Microsoft KB: 2915705

Description

Multiple vulnerabilities are present in some versions of Microsoft Exchange Server.

Observation

Microsoft Exchange is an industry standard server for providing E-Mail, calendar and contacts services.

Multiple vulnerabilities are present in some versions of Microsoft Exchange Server. The flaws are present in the WebReady Document Viewing and Data Loss Prevention features. Successful exploitation could allow an attacker to execute remote code on the effected server.

Microsoft has provided MS13-105 to address these issues. The host appears to be missing this patch.

16019 - (MS13-097) Cumulative Security Update for Internet Explorer (2898785)

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

Risk Level: High

CVE: CVE-2013-5045, CVE-2013-5046, CVE-2013-5047, CVE-2013-5048, CVE-2013-5049, CVE-2013-5051, CVE-2013-5052

Microsoft ID: MS13-097

Microsoft KB: 2898785

Description

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

Observation

Multiple vulnerabilities are present in some versions of Microsoft Internet Explorer. The flaws lie in multiple memory corruption and logic errors. Successful exploitation could allow an attacker to execute remote code or bypass some security restrictions. The exploit requires the user to open a malicious website.

Microsoft has provided MS13-097 to address these issues. The host appears to be missing this patch.

16023 - (MS13-097) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2898785)

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

Risk Level: High

CVE: CVE-2013-5047

Microsoft ID: MS13-097

Microsoft KB: 2898785

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 malicious website.

16024 - (MS13-101) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430)

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

Risk Level: High

CVE: CVE-2013-3899, CVE-2013-3902, CVE-2013-3903, CVE-2013-3907, CVE-2013-5058

Microsoft ID: MS13-101

Microsoft KB: 2880430

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 and other components handle objects in memory. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

Microsoft has provided MS13-101 to address these issues. The host appears to be missing this patch.

16031 - (MS13-107) Microsoft Exchange MAC Disabled Remote Code Execution (2915705)

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

Risk Level: High

CVE: CVE-2013-1330

DISA IAVA: 2013-A-0174

Microsoft ID: MS13-067

Microsoft KB: 2834052

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 handling of unassigned workflows. Successful exploitation could allow an attacker to execute remote code in the context of the W3WP service account.

16042 - (MS13-098) Vulnerability in Windows Could Allow Remote Code Execution (2893294)

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

Risk Level: High

CVE: CVE-2013-3900

Microsoft ID: MS13-098

Microsoft KB: 2893294

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 WinVerifyTrust function which handles Windows Authenticode signature verification for portable executable (PE) files. Successful exploitation could allow an attacker to execute remote code. Exploitation requires an attacker to convince a user to execute a specially crafted malicious portable executable (PE) file.

Microsoft has provided MS13-098 to address this issue. The host appears to be missing this patch.

16043 - (MS13-099) Microsoft Windows Use After Free Remote Code Execution (2909158)

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

Risk Level: High

CVE: CVE-2013-5056

Microsoft ID: MS13-099

Microsoft KB: 2909158

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 Microsoft Scripting Runtime Object Library. Successful exploitation could allow an attacker to execute remote code. Exploitation requires an attacker to convince a user to visit a malicious web page.

16044 - (MS13-099) Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution (2909158)

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

Risk Level: High

CVE: CVE-2013-5056

Microsoft ID: MS13-099

Microsoft KB: 2909158

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 Microsoft Scripting Runtime Object Library. Successful exploitation could allow an attacker to execute remote code. Exploitation requires an attacker to convince a user to visit a malicious web page.

Microsoft has provided MS13-099 to address this issue. The host appears to be missing this patch.

16045 - (MS13-100) Microsoft Sharepoint Page Content Privilege Escalation (2904244)

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

Risk Level: High

CVE: CVE-2013-5059

Microsoft ID: MS13-100

Microsoft KB: 2904244

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 the Page Content component. Successful exploitation could allow an attacker to execute commands with elevated privileges. The exploit requires the user to open a malicious SharePoint share.

16046 - (MS13-100) Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (2904244)

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

Risk Level: High

CVE: CVE-2013-5059

Microsoft ID: MS13-100

Microsoft KB: 2904244

Description

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

Observation

Microsoft SharePoint Server is a popular business collaboration platform.

A privilege escalation vulnerability is present in some versions of Microsoft SharePoint. The flaw lies in the Page Content component. Successful exploitation could allow an attacker to execute commands with elevated privileges. The exploit requires the user to open a malicious SharePoint share.

Microsoft has provided MS13-100 to address this issue. The host appears to be missing this patch.

16047 - (MS13-102) Microsoft Windows LPC Server Buffer Overrun Privilege Escalation (2898715)

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

Risk Level: High

CVE: CVE-2013-3878

Microsoft ID: MS13-102

Microsoft KB: 2898715

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 Local Procedure Call (LPC) component. Successful exploitation could allow an attacker to execute commands with elevated privileges.

16048 - (MS13-102) Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2898715)

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

Risk Level: High

CVE: CVE-2013-3878

Microsoft ID: MS13-102

Microsoft KB: 2898715

Description

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

Observation

Microsoft Windows is an industry standard operating system.

A privilege escalation vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Local Procedure Call (LPC) component. Successful exploitation could allow an attacker to execute commands with elevated privileges.

16060 - (APSB13-29) Vulnerabilities In Adobe Shockwave Player

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

Risk Level: High

CVE: CVE-2013-5333, CVE-2013-5334

Description

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

Observation

Adobe Shockwave Player is software used to view multimedia files created with Adobe Director.

Multiple vulnerabilities are present in some versions of Adobe Shockwave Player. There are multiple memory corruption vulnerabilities in the Shockwave Player. Successful exploitation could allow the attacker to run malicious code on the affected system.

The update provided by Adobe bulletin APSB13-29 resolves these issues. The target system appears to be missing this update.

16061 - (APSB13-28) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2013-5331, CVE-2013-5332

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 APSB13-28 resolves the issues. The target system is missing this update.

15973 - (HPSBMU02933) HP SiteScope "issueSiebelCmd" SOAP Request Arbitrary Code Execution Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-4835

Description

A remote code execution vulnerability is present in some versions of HP SiteScope.

Observation

HP SiteScope is an agentless monitoring software that monitors the availability and performance of IT infrastructures and application components remotely.

A remote code execution vulnerability is present in some versions of HP SiteScope. It could be remotely exploited to allow execution of code.

15991 - Microsoft Enhanced Mitigation Experience Toolkit ASLR Protection Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-6791

Description

An ASLR security protection bypass vulnerability is present in some versions of Microsoft Enhanced Mitigation Experience Toolkit.

Observation

Microsoft Enhanced Mitigation Experience Toolkit is an application that prevents software vulnerabilities from being exploited.

An ASLR security protection bypass vulnerability is present in some versions of Microsoft Enhanced Mitigation Experience Toolkit. The flaw lies in the mechanism in place to defeat ROP, particularly in the way it uses an inline hook in a memory block with a fixed address. Successful exploitation could allow an attacker to bypass the ASLR protection and execute arbitrary code.

15992 - Cisco IOS Software MLDP Processing Chunk Corruption Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-6693

Description

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

Observation

Cisco IOS is an operating system used in Cisco device.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw lies in the MLDP processing. Successful exploitation by a remote attacker could result in a denial of service condition.

15993 - Cisco IOS Software IPSec MTU Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-6694

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco device.

A vulnerability is present in some versions of Cisco IOS. The flaw lies in the IPSec MTU. Successful exploitation by a remote attacker could cause IPSec tunnels to drop.

15994 - Wordpress dhtmlxSpreadsheet Plugin Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-6281

Description

A cross-site scripting (XSS) vulnerability is present in some versions of cdhtmlxSpreadsheet plugin of WordPress.

Observation

WordPress is a popular open source blog web application.

A cross-site scripting (XSS) vulnerability is present in some versions of dhtmlxSpreadsheet plugin of WordPress. Successful exploitation could allow an attacker to inject arbitrary web script or HTML via the page parameter.

15995 - WordPress Tweet Blender Plugin "tb tab index" Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-6342

Description

A cross-site scripting vulnerability is present in some versions of the WordPress Tweet Blender plugin.

Observation

WordPress is a popular blog web application.

A cross-site scripting vulnerability is present in some versions of the WordPress Tweet Blender plugin. The flaw lies in the wp-admin/options-general.php file. Successful exploitation could allow an attacker to execute arbitrary HTML and script code.

15996 - Novell iPrint Client id1.GetPrinterURLList Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-3708

Description

A denial of service vulnerability is present in some versions of Novell iPrint.

Observation

Novell iPrint Client is a software used to submit print job to network printer.

A denial of service vulnerability is present in some versions of Novell iPrint. The flaw is due to an unspecified defect. Successful exploitation by a remote attacker could cause a denial of service.

16016 - (MS13-106) Vulnerability In A Microsoft Office Shared Component Could Allow Security Feature Bypass (2905238)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5057

Microsoft ID: MS13-106

Microsoft KB: 2905238

Description

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

Observation

A security bypass vulnerability is present in some versions of Microsoft Office. The flaw lies in the ASLR component. Successful exploitation could allow an attacker to bypass security measures.

Microsoft has provided MS13-106 to address this issue. The host appears to be missing this patch.

16017 - (MS13-106) Microsoft Office HDXS ASLR Security Bypass (2905238)

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

Risk Level: Medium

CVE: CVE-2013-5057

Microsoft ID: MS13-106

Microsoft KB: 2905238

Description

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

Observation

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

The flaw lies in the ASLR component. Successful exploitation could allow an attacker to bypass security measures.

16020 - (MS13-097) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2898785)

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

Risk Level: Medium

CVE: CVE-2013-5052

Microsoft ID: MS13-097

Microsoft KB: 2898785

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 malicious website.

16021 - (MS13-097) Microsoft Internet Explorer Memory Corruption I Privilege Escalation (2898785)

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

Risk Level: Medium

CVE: CVE-2013-5045

Microsoft ID: MS13-097

Microsoft KB: 2898785

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 a memory corruption error. Successful exploitation could allow a remote attacker to gain elevated privileges. The exploit requires the user to open a malicious website.

16022 - (MS13-097) Microsoft Internet Explorer Memory Corruption II Privilege Escalation (2898785)

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

Risk Level: Medium

CVE: CVE-2013-5046

Microsoft ID: MS13-097

Microsoft KB: 2898785

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 a memory corruption error. Successful exploitation could allow an attacker to bypass security measures. The exploit requires the user to open a malicious website.

16025 - (MS13-104) Vulnerability in Microsoft Office Could Allow Information Disclosure (2909976)

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

Risk Level: Medium

CVE: CVE-2013-5054

Microsoft ID: MS13-104

Microsoft KB: 2909976

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 flaw lies in the way Microsoft Office components parse and validate data when opening files on a malicious web site. Successful exploitation could allow an attacker to disclose private information.

Microsoft has provided MS13-104 to address these issues. The host appears to be missing this patch.

16026 - (MS13-097) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2898785)

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

Risk Level: Medium

CVE: CVE-2013-5051

Microsoft ID: MS13-097

Microsoft KB: 2898785

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 malicious website.

16027 - (MS13-097) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2898785)

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

Risk Level: Medium

CVE: CVE-2013-5049

Microsoft ID: MS13-097

Microsoft KB: 2898785

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 malicious website.

16028 - (MS13-097) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2898785)

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

Risk Level: Medium

CVE: CVE-2013-5048

Microsoft ID: MS13-097

Microsoft KB: 2898785

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 malicious website.

16030 - (MS13-103) Vulnerability in ASP.NET SignalR could allow Elevation of Privilege (2905244)

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

Risk Level: Medium

CVE: CVE-2013-5042, CVE-2013-5059

Microsoft ID: MS13-103

Microsoft KB: 2905244

Description

A privilege escalation vulnerability is 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 flaw lies in the ASP.NET SignalR component. Successful exploitation could allow an attacker to escalate privileges.

Microsoft has provided MS13-103 to address these issues. The host appears to be missing this patch.

16032 - (MS13-107) Microsoft Exchange Oracle Outside In Technologies Remote Code Execution (2915705)

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

Risk Level: Medium

CVE: CVE-2013-5763

Microsoft ID: MS13-105

Microsoft KB: 2915705

Description

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

Observation

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

The flaw lies in the Oracle Outside In Technology component. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open or view a malicious email.

16033 - (MS13-101) Microsoft Windows Integer Overflow I Privilege Escalation (2880430)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3899

Microsoft ID: MS13-101

Microsoft KB: 2880430

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 an integer overflow error. Successful exploitation could allow an attacker to execute commands with elevated privileges.

16034 - (MS13-101) Microsoft Windows Use-After-Free Privilege Escalation (2880430)

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

Risk Level: Medium

CVE: CVE-2013-3902

Microsoft ID: MS13-101

Microsoft KB: 2880430

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 an Use-After-Free error. Successful exploitation could allow an attacker to execute commands with elevated privileges.

16035 - (MS13-101) Microsoft Windows TrueType Font Parsing Privilege Escalation (2880430)

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

Risk Level: Medium

CVE: CVE-2013-3903

Microsoft ID: MS13-101

Microsoft KB: 2880430

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 parsing of TrueType fonts. Successful exploitation could allow an attacker to execute commands with elevated privileges.

16036 - (MS13-101) Microsoft Windows Point-Class Driver Double Fetch Privilege Escalation (2880430)

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

Risk Level: Medium

CVE: CVE-2013-3907

Microsoft ID: MS13-101

Microsoft KB: 2880430

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 a Point-Class driver. Successful exploitation could allow an attacker to execute commands with elevated privileges.

16037 - (MS13-101) Microsoft Windows Integer Overflow II Privilege Escalation (2880430)

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

Risk Level: Medium

CVE: CVE-2013-5058

Microsoft ID: MS13-101

Microsoft KB: 2880430

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 an integer overflow error. Successful exploitation could allow an attacker to execute commands with elevated privileges.

16038 - (MS13-104) Microsoft Office Token Hijacking Information Disclosure (2909976)

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

Risk Level: Medium

CVE: CVE-2013-5054

Microsoft ID: MS13-104

Microsoft KB: 2909976

Description

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

Observation

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

The flaw lies in the manipulation of tokens when Office is opening a document directly from a website. Successful exploitation could allow an attacker to obtain sensitive information. The exploit requires the user to open a file from a malicious website.

16039 - (MS13-102) Microsoft ASP. NET SignalR XSS Privilege Escalation (2905244)

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

Risk Level: Medium

CVE: CVE-2013-5042

Microsoft ID: MS13-102

Microsoft KB: 2905244

Description

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

Observation

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

The flaw lies in a cross site scripting error in the SignalR component. Successful exploitation could allow an attacker to execute commands with elevated privileges.

16041 - (MS13-098) Microsoft Windows WinVerifyTrust Signature Validation Remote Code Execution (2893294)

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

Risk Level: Medium

CVE: CVE-2013-3900

Microsoft ID: MS13-098

Microsoft KB: 2893294

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 WinVerifyTrust function which handles Windows Authenticode signature verification for portable executable (PE) files. Successful exploitation could allow an attacker to execute remote code. Exploitation requires an attacker to convince a user to execute a specially crafted malicious portable executable (PE) file.

16050 - Microsoft Windows Certificate Spoofing (2916652)

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

Risk Level: Medium

Microsoft KB: 2916652

Description

A new spoofing vulnerability is present in some versions of Microsoft Windows.

Observation

A new spoofing vulnerability is present in some versions of Microsoft Windows.

the flaw lies in the handling of some certificates signed by Microsoft. Successful exploitation could allow an attacker to impersonate another entity on the vulnerable system. The exploit requires the user to visit a malicious website, open a mail of file.

16058 - (MS13-105) Microsoft Exchange OWA XSS Remote Code Execution (2915705)

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

Risk Level: Medium

CVE: CVE-2013-5072

Microsoft ID: MS13-105

Microsoft KB: 2915705

Description

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

Observation

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

The flaw lies in an cross site scripting error in the OWA component. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open or view a malicious email.

16059 - (MS13-105) Microsoft Exchange Oracle Outside In Technologies II Remote Code Execution (2915705)

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

Risk Level: Medium

CVE: CVE-2013-5791

Microsoft ID: MS13-105

Microsoft KB: 2915705

Description

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

Observation

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

The flaw lies in the Oracle Outside In Technology component. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open or view a malicious email.

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.

2298 - WU-FTPD /bin SITE EXEC Misconfiguration

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

CVE: CVE-1999-0080, CVE-1999-0955, CVE-2000-0573, CVE-2000-0574

DISA IAVA: 2000-B-0004.0.0

Update Details

Observation is updated.
Recommendation is updated.

13855 - (MS12-043) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)

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

Risk Level: High

CVE: CVE-2012-1889

Microsoft ID: MS12-043

Update Details

Recommendation is updated.

14579 - (MS13-002) Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)

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

Risk Level: High

CVE: CVE-2013-0006, CVE-2013-0007

Microsoft ID: MS13-002

Microsoft KB: 2756145

Update Details

Recommendation is updated.

15317 - Apache Struts DefaultActionMapper Redirection and OGNL Security Bypass Vulnerabilities

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

Risk Level: High

CVE: CVE-2013-2248, CVE-2013-2251

DISA IAVA: 2013-A-0154

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.

15845 - NETGEAR WNDR3700v4 ping6 Diagnostic Page Command Injection Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: High

Update Details

Recommendation is updated.

15863 - Microsoft Graphics Component Remote Code execution

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

Risk Level: High

CVE: CVE-2013-3906, CVE-2013-3906

Microsoft ID: MS13-096

Microsoft KB: 2896666

Update Details

Observation is updated.
CVE is updated.

15980 - Mozilla Seamonkey Multiple Vulnerabilities Prior To 2.22.1

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-2566, CVE-2013-5605, CVE-2013-5606, CVE-2013-5607

Update Details

Risk is updated.

15981 - Mozilla Seamonkey Multiple Vulnerabilities Prior To 2.22.1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-2566, CVE-2013-5605, CVE-2013-5606, CVE-2013-5607

Update Details

Risk is updated.

37348 - IBM AIX IV47427 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-5419

Update Details

Recommendation is updated.

37349 - IBM AIX IV47428 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-5419

Update Details

Recommendation is updated.

37350 - IBM AIX IV47429 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-5419

Update Details

Recommendation is updated.

85642 - CentOS 5, 6 CESA-2013-1778 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: High

CVE: CVE-2012-5576, CVE-2013-1913, CVE-2013-1978

Update Details

Risk is updated.

91407 - Oracle Enterprise Linux ELSA-2013-1553 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2012-6075, CVE-2013-2007, CVE-2013-2231, CVE-2013-4344

Update Details

Risk is updated.

95366 - SuSE SLES 10 SP4, SLED 10 SP4 inst-source-utils-8376 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-0427

Update Details

Risk is updated.

95371 - SuSE SLES 11, 11 SP2, SLED 11, 11 SP2 inst-source-utils-6817 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-0427

Update Details

Risk is updated.

95878 - SuSE Linux 12.3 openSUSE-SU-2013:1776-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2925, CVE-2013-2926, CVE-2013-2927, CVE-2013-2928, CVE-2013-2931, CVE-2013-6621, CVE-2013-6622, CVE-2013-6623, CVE-2013-6624, CVE-2013-6625, CVE-2013-6626, CVE-2013-6627, CVE-2013-6628, CVE-2013-6629, CVE-2013-6630, CVE-2013-6631, CVE-2013-6632

Update Details

Risk is updated.

95879 - SuSE Linux 12.2 openSUSE-SU-2013:1777-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2931, CVE-2013-6621, CVE-2013-6622, CVE-2013-6623, CVE-2013-6624, CVE-2013-6625, CVE-2013-6626, CVE-2013-6627, CVE-2013-6628, CVE-2013-6629, CVE-2013-6630, CVE-2013-6631, CVE-2013-6632

Update Details

Risk is updated.

140363 - Red Hat Enterprise Linux RHSA-2013-1778 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2012-5576, CVE-2013-1913, CVE-2013-1978

Update Details

Risk is updated.

177765 - Gentoo Linux GLSA-201310-19 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: High

CVE: CVE-2013-4376

Update Details

Risk is updated.

187278 - Fedora Linux 20 FEDORA-2013-20869 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4400

Update Details

Risk is updated.

15369 - (MS13-066) Vulnerability In Active Directory Federation Services Could Allow Information Disclosure (2873872)

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

Risk Level: Medium

CVE: CVE-2013-3185

Microsoft ID: MS13-066

Microsoft KB: 2873872

Update Details

FASLScript 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.

58731 - Debian Linux 7.0 DSA-2804-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6385, CVE-2013-6386, CVE-2013-6387, CVE-2013-6388, CVE-2013-6389

Update Details

Risk is updated.

58734 - Debian Linux 6.0, 7.0 DSA-2805-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4478, CVE-2013-4479

Update Details

Risk is updated.

58737 - Debian Linux 6.0, 7.0 DSA-2807-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6050

Update Details

Risk is updated.

87889 - Fedora Linux 19 FEDORA-2013-11904 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1953

Update Details

Risk is updated.

87896 - Fedora Linux 18 FEDORA-2013-12032 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1953

Update Details

Risk is updated.

91397 - Oracle Enterprise Linux ELSA-2013-2585 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2012-6545, CVE-2013-0343, CVE-2013-1928, CVE-2013-2164, CVE-2013-2234, CVE-2013-2888, CVE-2013-2889, CVE-2013-2892, CVE-2013-3231, CVE-2013-4345, CVE-2013-4591

Update Details

Risk is updated.

91398 - Oracle Enterprise Linux ELSA-2013-1620 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-1940, CVE-2013-4396

Update Details

Risk is updated.

91399 - Oracle Enterprise Linux ELSA-2013-1764 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-4164

Update Details

Risk is updated.

91400 - Oracle Enterprise Linux ELSA-2013-1591 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2010-5107

Update Details

Risk is updated.

91401 - Oracle Enterprise Linux ELSA-2013-1536 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-2124, CVE-2013-4419

Update Details

Risk is updated.

91405 - Oracle Enterprise Linux ELSA-2013-2584 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2012-6545, CVE-2013-0343, CVE-2013-1928, CVE-2013-2888, CVE-2013-2889, CVE-2013-2892, CVE-2013-3231, CVE-2013-4345, CVE-2013-4387, CVE-2013-4592

Update Details

Risk is updated.

91406 - Oracle Enterprise Linux ELSA-2013-2583 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-0343, CVE-2013-2888, CVE-2013-2889, CVE-2013-2892, CVE-2013-4345, CVE-2013-4387, CVE-2013-4592

Update Details

Risk is updated.

93150 - Mandriva Linux MBS1 MDVSA-2013-190 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1953

Update Details

Risk is updated.

95199 - SuSE SLES 11, 11 SP1, SLED 11, 11 SP1 zypper-6527 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-0420

Update Details

Risk is updated.

95213 - SuSE SLES 11, 11 SP2, SLED 11, 11 SP2 zypper-6528 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-0420

Update Details

Risk is updated.

174390 - Scientific Linux Security ERRATA Low: openssh on SL6.x i386/x86_64 (1312-571)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2010-5107

Update Details

Risk is updated.

174391 - Scientific Linux Security ERRATA Critical: ruby on SL6.x i386/x86_64 (1312-936)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2013-4164

Update Details

Risk is updated.

174393 - Scientific Linux Security ERRATA Important: 389-ds-base on SL6.x i386/x86_64 (1312-318)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2013-4485

Update Details

Risk is updated.

174394 - Scientific Linux Security ERRATA Low: pacemaker on SL6.x i386/x86_64 (1312-691)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2013-0281

Update Details

Risk is updated.

187287 - Fedora Linux 20 FEDORA-2013-20942 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4445, CVE-2013-4446

Update Details

Risk is updated.

187339 - Fedora Linux 19 FEDORA-2013-20965 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4445, CVE-2013-4446

Update Details

Risk is updated.

187349 - Fedora Linux 18 FEDORA-2013-20976 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4445, CVE-2013-4446

Update Details

Risk is updated.

187361 - Fedora Linux 19 FEDORA-2013-21844 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6385, CVE-2013-6386, CVE-2013-6387, CVE-2013-6388, CVE-2013-6389

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

2684 - OpenSSH buffer_init Buffer Management Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1156

CVE: CVE-2003-0693, CVE-2003-0695

DISA IAVA: 2003-T-0020,2001-T-0017,2001-A-0013

7693 - OpenSSH Remote Root Authentication Timing Side Channel Weakness Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

CVE: CVE-2003-1562

7692 - OpenSSH Portable PAM Support User Identification Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2003-0190

15098 - Microsoft Windows Kernel win32k.sys Privilege Escalation Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-3660, CVE-2013-3661

ADDITIONAL NOTES

2684 - ,7692,7693 and 15098 were deleted. New scripts will be covering the vulnerabilities.

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.