2014-NOV-11
FSL version 7.5.645

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

17357 - (MS14-066) Vulnerability in Schannel Could Allow Remote Code Execution (2992611)

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

Risk Level: High

CVE: CVE-2014-6321

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 way Secure Channel process specially crafted packets. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS14-066 to address this issue. The host appears to be missing this patch.

17412 - (APSB14-24) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2014-0573, CVE-2014-0574, CVE-2014-0576, CVE-2014-0577, CVE-2014-0581, CVE-2014-0582, CVE-2014-0583, CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, CVE-2014-0588, CVE-2014-0589, CVE-2014-0590, CVE-2014-8437, CVE-2014-8438, CVE-2014-8440, CVE-2014-8441, CVE-2014-8442

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 APSB14-24 resolves these issues. The target system is missing this update.

17413 - (APSB14-24) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0573, CVE-2014-0574, CVE-2014-0576, CVE-2014-0577, CVE-2014-0581, CVE-2014-0582, CVE-2014-0583, CVE-

2014-0584, CVE-2014-0585, CVE-2014-0586, CVE-2014-0588, CVE-2014-0589, CVE-2014-0590, CVE-2014-8437, CVE-2014-8438, CVE-2014-8440, CVE-2014-8441, CVE-2014-8442

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 APSB14-24 resolves these issues. The target system is missing this update.

17362 - (MS14-064) Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)

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

Risk Level: High

CVE: CVE-2014-6332, CVE-2014-6352

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 lie 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 MS14-064 to address these issues. The host appears to be missing this patch.

17366 - (MS14-067) Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958)

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

Risk Level: High

CVE: CVE-2014-4118

Description

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

Observation

Windows is Microsoft operating system.

A remote code execution vulnerability is present in some versions of Microsoft MSXML. The flaw lies in the parsing of XML content. Successful exploitation could allow an attacker to disclose information. The exploit requires the user to visit a malicious website.

Microsoft has released MS14-067 to address this issue. The host is missing this patch.

17372 - (MS14-065) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-4143

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17373 - (MS14-065) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6337

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17374 - (MS14-065) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6341

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17375 - (MS14-065) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6342

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17376 - (MS14-065) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6343

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17377 - (MS14-065) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6344

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17378 - (MS14-065) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6347

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could

result in the execution of arbitrary code.

17379 - (MS14-065) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6348

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17380 - (MS14-065) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6351

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17381 - (MS14-065) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6353

Description

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Internet Explorer could lead to remote code execution.

The flaw occurs when Internet Explorer improperly accesses an object in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17384 - (MS14-065) Cumulative Security Update for Internet Explorer (3003057)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4143, CVE-2014-6323, CVE-2014-6337, CVE-2014-6339, CVE-2014-6340, CVE-2014-6341, CVE-2014-6342, CVE-2014-6343, CVE-2014-6344, CVE-2014-6345, CVE-2014-6346, CVE-2014-6347, CVE-2014-6348, CVE-2014-6349, CVE-2014-6350, CVE-2014-6351, CVE-2014-6353

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 MS14-065 to address these issues. The host appears to be missing this patch.

17385 - (MS14-069) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3009710)

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

Risk Level: High

CVE: CVE-2014-6333 , CVE-2014-6334 , CVE-2014-6335

Description

Multiple vulnerabilities are present in some versions of Microsoft Word.

Observation

Microsoft Office is a popular office suite.

Multiple vulnerabilities are present in some versions of Microsoft Word. The flaws exist 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 MS14-069 to address these issues. The host appears to be missing this patch.

17399 - (MS14-073) Vulnerability in Microsoft SharePoint Foundation Could Allow Elevation of Privilege (3000431)

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

Risk Level: High

CVE: CVE-2014-4116

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 SharePoint lists. Successful exploitation could allow an attacker to gain elevated privileges or execute remote code.

Microsoft has provided MS14-073 to address this issue. The host appears to be missing this patch.

17408 - (MS14-079) Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (3002885)

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

Risk Level: High

CVE: CVE-2014-6317

Description

A denial of service vulnerability is 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.

A denial of service vulnerability is present in the kernel-mode device drivers in some versions of Microsoft Windows. The flaw is due to improper handling of TrueType font files by the Windows kernel-mode drivers. Successful exploitation could allow a denial of service condition.

Microsoft has provided MS14-079 to address this issue. The host appears to be missing this patch.

17356 - (MS14-076) Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass (2982998)

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

Risk Level: Medium

CVE: CVE-2014-4078

Description

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

Observation

Microsoft Internet Information Services (IIS) is a popular web server for Windows operating system.

A security bypass vulnerability is present in some versions of Microsoft Internet Information Services. The flaw is due to the incoming web requests are not properly verified against the IP and domain restriction filtering list. Successful exploitation could allow an attacker to bypass security restrictions.

Microsoft has provided MS14-076 to address this issue. The host appears to be missing this patch.

17359 - (MS14-076) Microsoft Internet Information Services IP And Domain Filtering List Security Bypass (2982998)

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

Risk Level: Medium

CVE: CVE-2014-4078

Description

A vulnerability in some versions of Microsoft Internet Information Services could lead to a security bypass.

Observation

A vulnerability in some versions of Microsoft Internet Information Services could lead to a security bypass.

The flaw lies in the IP And Domain Filtering List components. Successful exploitation could allow an attacker to bypass security measures. The exploit requires the user to open a vulnerable website, email or document.

17360 - (MS14-066) Microsoft Windows Schannel Remote Code Execution (2992611)

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

Risk Level: Medium

CVE: CVE-2014-6321

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 lies in the Schannel component. Successful exploitation could allow an attacker to execute remote code.

17363 - (MS14-064) Microsoft Windows OLE Automation Array Remote Code Execution (3011443)

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

Risk Level: Medium

CVE: CVE-2014-6332

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 lies in the OLE component. Successful exploitation could allow an attacker to execute remote code.

17364 - (MS14-064) Microsoft Windows OLE Remote Code Execution (3011443)

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

Risk Level: Medium

CVE: CVE-2014-6352

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 lies in the OLE component. Successful exploitation could allow an attacker to execute remote code.

17365 - (MS14-065) Microsoft Internet Explorer ASLR Security Bypass (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6339

Description

A vulnerability in some versions of Internet Explorer could lead to a security bypass.

Observation

A vulnerability in some versions of Internet Explorer could lead to a security bypass.

The flaw occurs when Internet Explorer does not use the Address Space Layout Randomization (ASLR) security feature, allowing an attacker to more reliably predict the memory offsets of specific instructions in a given call stack. Successful exploitation could allow a remote attacker to bypass intended access restrictions.

17367 - (MS14-065) Microsoft Internet Explorer Clipboard Information Disclosure (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6323

Description

A vulnerability in some versions of Internet Explorer could lead to an information disclosure.

Observation

A vulnerability in some versions of Internet Explorer could lead to an information disclosure.

The flaw occurs when Internet Explorer does not properly restrict access to the clipboard of a user who visits the attackers site. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

17368 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure I (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6340

Description

A vulnerability in some versions of Internet Explorer could lead to an information disclosure.

Observation

A vulnerability in some versions of Internet Explorer could lead to an information disclosure.

The flaw is caused when Internet Explorer does not properly enforce cross-domain policies. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

17369 - (MS14-067) Microsoft Windows MSXML Core Services Remote Code Execution (2993958)

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

Risk Level: Medium

CVE: CVE-2014-4118

Description

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

Observation

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

The flaw lies in the Core Services component. Successful exploitation could allow an attacker to execute remote code.

17370 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure II (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6345

Description

A vulnerability in some versions of Internet Explorer could lead to an information disclosure.

Observation

A vulnerability in some versions of Internet Explorer could lead to an information disclosure.

The flaw occurs when Internet Explorer does not properly enforce cross-domain policies. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

17371 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure III (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6346

Description

A vulnerability in some versions of Internet Explorer could lead to an information disclosure.

Observation

A vulnerability in some versions of Internet Explorer could lead to an information disclosure.

The flaw occurs when Internet Explorer does not properly enforce cross-domain policies. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

17382 - (MS14-065) Microsoft Internet Explorer Permission Validation I Privilege Escalation (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6349

Description

A vulnerability in some versions of Internet Explorer could lead to a privilege escalation.

Observation

A vulnerability in some versions of Internet Explorer could lead to a privilege escalation.

The flaw occurs when Internet Explorer does not properly validate permissions under specific conditions. Successful exploitation could allow a local user to gain elevated privileges.

17383 - (MS14-065) Microsoft Internet Explorer Permission Validation II Privilege Escalation (3003057)

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

Risk Level: Medium

CVE: CVE-2014-6350

Description

A vulnerability in some versions of Internet Explorer could lead to a privilege escalation.

Observation

A vulnerability in some versions of Internet Explorer could lead to a privilege escalation.

The flaw occurs when Internet Explorer does not properly validate permissions under specific conditions. Successful exploitation could allow a local user to gain elevated privileges.

17386 - (MS14-069) Microsoft Word Invalid Pointer Remote Code Execution (3009710)

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

Risk Level: Medium

CVE: CVE-2014-6335

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 lies in the parsing of specially crafted Word files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17387 - (MS14-069) Microsoft Word Bad Index Remote Code Execution (3009710)

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

Risk Level: Medium

CVE: CVE-2014-6334

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 lies in the parsing of specially crafted Word files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17388 - (MS14-069) Microsoft Word Double Delete Remote Code Execution (3009710)

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

Risk Level: Medium

CVE: CVE-2014-6333

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 lies in the parsing of specially crafted Word files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17389 - (MS14-071) Vulnerability in Windows Audio Service Could Allow Elevation of Privilege (3005607)

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

Risk Level: Medium

CVE: CVE-2014-6322

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 Windows audio service. Successful exploitation could allow an attacker to escalate privileges.

Microsoft has provided MS14-071 to address this issue. The host appears to be missing this patch.

17390 - (MS14-071) Microsoft Windows Audio Services Privilege Escalation (3005607)

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

Risk Level: Medium

CVE: CVE-2014-6322

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 lies in the Audio Services component. 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.

17391 - (MS14-070) Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935)

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

Risk Level: Medium

CVE: CVE-2014-4076

Description

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

Observation

Microsoft Windows is an industry standard operating system. Windows includes support for TCP/IP networking.

A privilege escalation vulnerability is present in some versions of Microsoft Windows. The flaw lies in the TCP/IP component. 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.

Microsoft has provided MS14-070 to address these issues. The host appears to be missing this patch.

17392 - (MS14-070) Microsoft Windows TCP/IP IOCTL Privilege Escalation (2989935)

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

Risk Level: Medium

CVE: CVE-2014-4076

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 lies in the TCP/IP component. 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.

17393 - (MS14-074) Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass (3003743)

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

Risk Level: Medium

CVE: CVE-2014-6318

Description

A security bypass vulnerability exists in some versions of Microsoft Windows.

Observation

Microsoft Windows is an industry standard operating system.

A security bypass vulnerability exists in some versions of Microsoft Windows. The flaw lies within the Remote Desktop Protocol. Successful exploitation could allow an attacker to bypass security restrictions.

Microsoft has provided MS14-074 to address this issue. The host appears to be missing this patch.

17394 - (MS14-074) Microsoft Windows Remote Desktop Protocol Audit Log Security Bypass (3003743)

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

Risk Level: Medium

CVE: CVE-2014-6318

Description

A vulnerability in some versions of Microsoft Remote Desktop Protocol could lead to a security bypass.

Observation

A vulnerability in some versions of Microsoft Remote Desktop Protocol could lead to a security bypass.

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

17395 - (MS14-072) Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)

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

Risk Level: Medium

CVE: CVE-2014-4149

Description

An elevation of privilege vulnerability exists in some versions of Microsoft Windows .NET Framework.

Observation

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

An elevation of privilege vulnerability exists in some versions of Microsoft Windows .NET Framework. The flaw lies in the TypeFilterLevel component. Successful exploitation could allow a remote attacker to escalate privileges.

Microsoft has provided MS14-072 to address this issue. The host appears to be missing this patch.

17396 - (MS14-072) Microsoft .NET Framework Remoting TypeFilterLevel Privilege Escalation (3005210)

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

Risk Level: Medium

CVE: CVE-2014-4149

Description

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

Observation

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

The flaw lies in the TypeFilterLevel component. 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.

17397 - (MS14-078) Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)

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

Risk Level: Medium

CVE: CVE-2014-4077

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 Microsoft IME. Successful exploitation could allow an attacker to escape the application's security sandbox and escalate privileges.

Microsoft has provided MS14-078 to address this issue. The host appears to be missing this patch.

17398 - (MS14-078) Microsoft Windows IME (Japanese) Privilege Escalation (2992719)

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

Risk Level: Medium

CVE: CVE-2014-4077

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 lies in the IME (Japanese) component. 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.

17400 - (MS14-073) Microsoft SharePoint Lists Privilege Escalation (3000431)

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

Risk Level: Medium

CVE: CVE-2014-4116

Description

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

Observation

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

The flaw lies in the Lists component. Successful exploitation could allow an attacker to execute commands with elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

17406 - (MS14-077) Vulnerability in Active Directory Federation Services could allow Information Disclosure (3003381)

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

Risk Level: Medium

CVE: CVE-2014-6331

Description

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

Observation

Active Directory (AD) is a directory service implemented by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Active Directory. The flaw lies in the Federation

Services component. Successful exploitation could allow an attacker to obtain sensitive information.

The vendor has released MS14-077 to address this issue. The host appears to be missing this patch.

17407 - (MS14-077) Microsoft Active Directory Federation Services Information Disclosure (3003381)

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

Risk Level: Medium

CVE: CVE-2014-6331

Description

A vulnerability in some versions of Microsoft Active Directory could lead to an information disclosure.

Observation

A vulnerability in some versions of Microsoft Active Directory could lead to an information disclosure.

The flaw lies in the Federation Services component. Successful exploitation could allow an attacker to obtain sensitive information. The exploit requires the user to open a vulnerable website, email or document.

17409 - (MS14-079) Microsoft Windows Kernel Denial of Service (3002885)

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

Risk Level: Medium

CVE: CVE-2014-6317

Description

A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

The flaw lies in the Kernel component. Successful exploitation could allow an attacker to cause a denial of service. The exploit requires the user to open a vulnerable website, email or document.

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.

33277 - Oracle Solaris 150512-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Update Details

Risk is updated

33278 - Oracle Solaris 150513-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Update Details

Risk is updated

58949 - Debian Linux 7.0 DSA-3025-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0487, CVE-2014-0488, CVE-2014-0489, CVE-2014-0490

Update Details

Risk is updated

58963 - Debian Linux 7.0 DSA-3040-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634

Update Details

Risk is updated

58967 - Debian Linux 7.0 DSA-3045-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0142, CVE-2014-0143, CVE-2014-0144, CVE-2014-0145, CVE-2014-0146, CVE-2014-0147, CVE-2014-0222, CVE-2014-0223, CVE-2014-3615, CVE-2014-3640

Update Details

Risk is updated

58969 - Debian Linux 7.0 DSA-3044-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0142, CVE-2014-0143, CVE-2014-0144, CVE-2014-0145, CVE-2014-0146, CVE-2014-0147, CVE-2014-0222, CVE-2014-0223, CVE-2014-3615, CVE-2014-3640

Update Details

Risk is updated

58986 - Debian Linux 7.0 DSA-3060-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3610, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-3647, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-3690, CVE-2014-7207

Update Details

Risk is updated

85774 - CentOS 6 CESA-2014-1075 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0222, CVE-2014-0223

Update Details

Risk is updated

85814 - CentOS 5 CESA-2014-1671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634

Update Details

Risk is updated

91554 - Oracle Enterprise Linux ELSA-2014-0927 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4148, CVE-2013-4149, CVE-2013-4150, CVE-2013-4151, CVE-2013-4527, CVE-2013-4529, CVE-2013-4535, CVE-2013-4536, CVE-2013-4541, CVE-2013-4542, CVE-2013-6399, CVE-2014-0182, CVE-2014-0222, CVE-2014-0223, CVE-2014-3461

Update Details

Risk is updated

91582 - Oracle Enterprise Linux ELSA-2014-1075 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0222, CVE-2014-0223

Update Details

Risk is updated

91623 - Oracle Enterprise Linux ELSA-2014-1671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634

Update Details

Risk is updated

93292 - Mandriva Linux MBS1, MES5 MDVSA-2014-058 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2015

Update Details

Risk is updated

93402 - Mandriva Linux MBS1 MDVSA-2014-196 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634, CVE-2014-3683

Update Details

Risk is updated

140507 - Red Hat Enterprise Linux RHSA-2014-1075 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0222, CVE-2014-0223

Update Details

Risk is updated

140527 - Red Hat Enterprise Linux RHSA-2014-0927 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4148, CVE-2013-4149, CVE-2013-4150, CVE-2013-4151, CVE-2013-4527, CVE-2013-4529, CVE-2013-4535, CVE-2013-4536, CVE-2013-4541, CVE-2013-4542, CVE-2013-6399, CVE-2014-0182, CVE-2014-0222, CVE-2014-0223, CVE-2014-3461

Update Details

Risk is updated

140593 - Red Hat Enterprise Linux RHSA-2014-1671 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634

Update Details

Risk is updated

142052 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:0343-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2015

Update Details

Risk is updated

142127 - SuSE SLES 11, 11 SP3 freeradius-server-8968 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-2015

Update Details
Risk is updated

142462 - SuSE SLES 11, 11 SP3 rsyslog-9840 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-3634, CVE-2014-3683

Update Details
Risk is updated

142463 - SuSE Linux 13.1 openSUSE-SU-2014:1297-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-3634, CVE-2014-3683

Update Details
Risk is updated

142464 - SuSE Linux 12.3 openSUSE-SU-2014:1298-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-3634, CVE-2014-3683

Update Details
Risk is updated

174536 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL6.x i386/x86_64 (1408-1194)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: High
CVE: CVE-2014-0222, CVE-2014-0223

Update Details
Risk is updated

174570 - Scientific Linux Security ERRATA Moderate: rsyslog5 and rsyslog on SL5.x, SL6.x i386/x86_64 (1410-2253)

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

CVE: CVE-2014-3634

Update Details

Risk is updated

177923 - Gentoo Linux GLSA-201406-12 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2015

Update Details

Risk is updated

181266 - FreeBSD rsyslog Remote Syslog PRI Vulnerability (8e0e86ff-48b5-11e4-ab80-000c29f6ae42)

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

Risk Level: High

CVE: CVE-2014-3634

Update Details

Risk is updated

184540 - Ubuntu Linux 10.04, 12.04, 14.04 USN-2342-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4148, CVE-2013-4149, CVE-2013-4150, CVE-2013-4151, CVE-2013-4526, CVE-2013-4527, CVE-2013-4529, CVE-2013-4530, CVE-2013-4531, CVE-2013-4532, CVE-2013-4533, CVE-2013-4534, CVE-2013-4535, CVE-2013-4536, CVE-2013-4537, CVE-2013-4538, CVE-2013-4539, CVE-2013-4540, CVE-2013-4541, CVE-2013-4542, CVE-2013-6399, CVE-2014-0142, CVE-2014-0143, CVE-2014-0144, CVE-2014-0145, CVE-2014-0146, CVE-2014-0147, CVE-2014-0182, CVE-2014-0222, CVE-2014-0223, CVE-2014-3461, CVE-2014-3471

Update Details

Risk is updated

184551 - Ubuntu Linux 10.04, 12.04, 14.04 USN-2348-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0487, CVE-2014-0488, CVE-2014-0489, CVE-2014-0490

Update Details

Risk is updated

184579 - Ubuntu Linux 10.04, 12.04, 14.04 USN-2381-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634, CVE-2014-3683

Update Details

Risk is updated

187701 - Fedora Linux 20 FEDORA-2014-3184 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2015

Update Details

Risk is updated

187705 - Fedora Linux 19 FEDORA-2014-3192 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2015

Update Details

Risk is updated

187919 - Fedora Linux 20 FEDORA-2014-6288 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4148, CVE-2013-4149, CVE-2013-4150, CVE-2013-4151, CVE-2013-4526, CVE-2013-4527, CVE-2013-4529, CVE-2013-4530, CVE-2013-4531, CVE-2013-4533, CVE-2013-4534, CVE-2013-4535, CVE-2013-4536, CVE-2013-4537, CVE-2013-4538, CVE-2013-4539, CVE-2013-4540, CVE-2013-4541, CVE-2013-4542, CVE-2013-6399, CVE-2014-0182

Update Details

Risk is updated

187974 - Fedora Linux 20 FEDORA-2014-6970 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0222, CVE-2014-0223, CVE-2014-3461

Update Details

Risk is updated

188369 - Fedora Linux 21 FEDORA-2014-12563 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3634

Update Details

Risk is updated

188388 - Fedora Linux 20 FEDORA-2014-12503 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-3634

Update Details
Risk is updated

188403 - Fedora Linux 19 FEDORA-2014-12878 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-3634

Update Details
Risk is updated

188418 - Fedora Linux 20 FEDORA-2014-12910 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-3634

Update Details
Risk is updated

58982 - Debian Linux 7.0 DSA-3058-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-3684

Update Details
Risk is updated

5524 - Apache Tomcat cal2.jsp CSRF

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server
Risk Level: Medium
CVE: CVE-2006-7196, CVE-2007-4724

Update Details
CVE is updated

17039 - BlackBerry OS OpenSSL Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Blackberry
Risk Level: Medium
CVE: CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

Update Details
Recommendation is updated

17281 - SSLv3 Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous
Risk Level: Medium
CVE: CVE-2014-3566

Update Details
Recommendation is updated

58972 - Debian Linux 7.0 DSA-3047-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-3683

Update Details
Risk is updated

58979 - Debian Linux 7.0 DSA-3057-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-3660

Update Details
Risk is updated

58985 - Debian Linux 7.0 DSA-3063-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-8483

Update Details
Risk is updated

93409 - Mandriva Linux MBS1 MDVSA-2014-204 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Mandriva Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-3660

Update Details
Risk is updated

142477 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1330-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-3660

Update Details

Risk is updated

181275 - FreeBSD libxml2 Denial Of Service (0642b064-56c4-11e4-8b87-bcaec565249c)

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

Risk Level: Medium

CVE: CVE-2014-3660

Update Details

Risk is updated

184595 - Ubuntu Linux 10.04, 12.04, 14.04 USN-2389-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3660

Update Details

Risk is updated

188343 - Fedora Linux 21 FEDORA-2014-11677 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0334

Update Details

Risk is updated

188344 - Fedora Linux 20 FEDORA-2014-11630 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0334

Update Details

Risk is updated

188357 - Fedora Linux 19 FEDORA-2014-11649 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0334

Update Details

Risk is updated

188363 - Fedora Linux 20 FEDORA-2014-12995 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-3660

Update Details
Risk is updated

15322 - McAfee Data Loss Prevention Manager Multiple Vulnerabilities Prior To 9.2.2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: Medium
CVE: CVE-2014-8519, CVE-2014-8534, CVE-2014-8535, CVE-2014-8536, CVE-2014-8537

Update Details
Risk is updated

181254 - FreeBSD phpMyAdmin XSRF/CSRF Due To DOM Based XSS In The Micro History Feature (cc627e6c-3b89-11e4-b629-6805ca0b3d42)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-6300

Update Details
Risk is updated

188267 - Fedora Linux 21 FEDORA-2014-10885 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-6300

Update Details
Risk is updated

188290 - Fedora Linux 19 FEDORA-2014-10989 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-6300

Update Details
Risk is updated

188291 - Fedora Linux 20 FEDORA-2014-10981 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-6300

Update Details

Risk is updated

188400 - Fedora Linux 20 FEDORA-2014-13773 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-3610, CVE-2014-3611, CVE-2014-3646, CVE-2014-8369

Update Details
Risk is updated

85807 - CentOS 7 CESA-2014-1669 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Low
CVE: CVE-2014-3615

Update Details
Risk is updated

91636 - Oracle Enterprise Linux ELSA-2014-1669 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Low
CVE: CVE-2014-3615

Update Details
Risk is updated

140590 - Red Hat Enterprise Linux RHSA-2014-1669 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Low
CVE: CVE-2014-3615

Update Details
Risk is updated

174560 - Scientific Linux Security ERRATA Low: qemu-kvm on SL7.x x86_64 (1410-1189)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Low
CVE: CVE-2014-3615

Update Details
Risk is updated

188244 - Fedora Linux 20 FEDORA-2014-10445 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low

CVE: CVE-2014-3615

Update Details

Risk is updated

188268 - Fedora Linux 21 FEDORA-2014-10761 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3615, CVE-2014-5388

Update Details

Risk is updated

188318 - Fedora Linux 21 FEDORA-2014-11588 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3640

Update Details

Risk is updated

188382 - Fedora Linux 20 FEDORA-2014-11641 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3640

Update Details

Risk is updated

DELETED CHECKS

17312 - Vulnerability in Microsoft OLE Could Allow Remote Code Execution (3010060)

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

Risk Level: High

CVE: CVE-2014-6352

ADDITIONAL NOTES

- **17312** - has been replaced by FID17362, FID17363 and FID17364.

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.