McAfee Host Intrusion Prevention Content 4865 Release Notes | 2013-04-09

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 4865)

New Windows Signatures

Signature 2834: *Java - Creation of suspicious files in Temp folder*

Description:

- *This event indicates an attempt by Java to create suspicious files in temp folder*
- *This signature is set to level Medium by default.*

Signature 2836: *Remote Desktop Client Mstscax Remote Code Execution Vulnerability*

Description:

- *This event indicates an attempt to exploit a vulnerability in Microsoft Remote Desktop Client Mstscax that could allow attackers to execute code remotely (CVE-2013-1296).*
- *This signature is set to level Low by default.*

Signature 2837: *Microsoft Antimalware Client Privilege Escalation Vulnerability*

Description:

- *This event indicates an attempt to exploit a vulnerability in Microsoft Antimalware Client Mstscax that could allow attackers to escalate their privileges on the machine (CVE-2013-0078).*
- *This signature is set to level Low by default.*

Updated Windows Signatures

[BugFix] Signature 2229: *Vulnerabilities in Remote Desktop Client Could Allow Remote Code Execution*

Description:

- *The signature description has been updated with the CVE reference.*

[BugFix] Signature 2802: *Java Envelope - Creation of suspicious files in Temp folder*

Description:

- *The signature has been modified to enhance protection.*

[BugFix] Signature 6013: *Suspicious Function Invocation - CALL Not Found*
Description:

- *The signature has been modified to reduce false positives.*

[BugFix] Signature 6015: *Suspicious Function Invocation - Target Address Mismatch*
Description:

- *The signature has been modified to reduce false positives.*

[BugFix]: *Compatibility issue with ePo5.0 has been fixed.*

[BugFix]: *HIP content has been modified to reduce false positives in Boot time protection.*

[Improvement]: Support for Windows 8 and Windows 2012 Server
Description:

- *Windows 8 and Windows 2012 Server platform support has been added.*
- *This requires Host Intrusion Prevention client Version 8.0 Patch 3 and above.*

[Improvement]: HIP Content project- Compiler migration to a newer version
Description:

- *The compiler has been migrated to a newer version making use of the security features available with the new compiler version.*
- *The following signatures have been affected*
    - ***Signature 2201:*** *Vulnerabilities in Windows Search Could Allow Remote Code Execution (CVE-2008-4269)*
    - ***Signature 2202:*** *Vulnerabilities in GDI Could Allow Remote Code Execution (CVE-2008-2249)*
    - ***Signature 2207:*** *WMP Vulnerability Could Allow an Authentication Reflection Attack by WMS*
    - ***Signature 2212:*** *Vulnerabilities in Windows Win32k Kernel Could Allow Remote Code Execution*
    - ***Signature 2213:*** *Vulnerability in Microsoft Exchange EMSMDB32 Could Allow Denial of Service*
    - ***Signature 2222:*** *Print Spooler Load Library Vulnerability*
    - ***Signature 2228:*** *Vulnerability in Workstation Service Could Allow Elevation of Privilege*
    - ***Signature 2239:*** *Vulnerability in License Logging Server Could Allow Remote Code Execution*
    - ***Signature 2251:*** *Vulnerability in Windows Shell Handler Could Allow Remote Code Execution*
    - ***Signature 2272:*** *Possible Print Spooler Service Impersonation Attempt Detected*
    - ***Signature 2280:*** *Vulnerability in Netlogon RPC Service Could Allow Denial of Service*
    - ***Signature 2285:*** *Active Directory SPN Validation Vulnerability*

- ***Signature 2779:*** *TDSS Rootkit Infection*
- ***Signature 2819:*** *Windows Enumerate File Vulnerability*
- ***Signature 2830:*** *Block User Creation*
    - *This signature is not supported on Windows 2000 Server and 64 bit platforms*
- ***Signature 3727:*** *IE drag and drop file installation*
- ***Signature 3728:*** *MSRPC LLSSRV Buffer Overflow*
- ***Signature 3730:*** *Windows Explorer MSHTA Script Execution*
- ***Signature 3731:*** *URL Decoding Zone Spoofing Vulnerability*
- ***Signature 3733:*** *Windows Messenger Service Buffer Overflow*
- ***Signature 3734:*** *Print Spooler Service Buffer Overflow*
- ***Signature 3735:*** *Plug and Play Buffer Overflow (Zotob)*
- ***Signature 3736:*** *Telephony Service Buffer Overflow*
- ***Signature 3738:*** *MSDTC RPC Vulnerability*
- ***Signature 3739:*** *Windows Plug-and-Play Buffer Overflow Vulnerability 2*
- ***Signature 3740:*** *Client Services For Netware Vulnerability*
- ***Signature 3741:*** *Windows Metafile Heap Overflow Vulnerability*
- ***Signature 3742:*** *Windows Enhanced Metafile Heap Overflow Vulnerability*
- ***Signature 3744:*** *Graphics Rendering Engine Vulnerability*
- ***Signature 3749:*** *Internet Explorer HTA Execution Vulnerability*
- ***Signature 3750:*** *Remote COM Activation by Desktop.ini Vulnerability*
- ***Signature 3752:*** *MSDTC RPC DoS Vulnerability*
- ***Signature 3757:*** *MSHTA Directory Traversal Vulnerability*
- ***Signature 3758:*** *Management Console Vulnerability*
- ***Signature 3759:*** *MHTML Parsing Vulnerability*
- ***Signature 3760:*** *Internet Explorer FTP Command Injection Vulnerability*
- ***Signature 3761:*** *Winsock Hostname Vulnerability*
- ***Signature 3762:*** *IE SourceURL NULL Dereference Vulnerability*
- ***Signature 3763:*** *Windows Kernel Elevation of Privilege Vulnerability*
- ***Signature 3767:*** *Windows Server Service Buffer Overflow Vulnerability (2)*
- ***Signature 3768:*** *Windows Server Service Buffer Overflow Vulnerability (Tighter Security)*
- ***Signature 3769:*** *Windows Metafile Denial of Service Vulnerability*
- ***Signature 3771:*** *Vulnerability in Indexing Service Could Allow Cross-Site Scripting*
- ***Signature 3772:*** *Client Services for Netware BO Vulnerability*
- ***Signature 3775:*** *Windows Shell Vulnerability in WebViewFolderIcon*
- ***Signature 3777:*** *Windows ASN.1 Heap Overflow Vulnerability*
- ***Signature 3778:*** *Internet Explorer 7 Address Bar Spoofing Vulnerability*
- ***Signature 3780:*** *IPNATHLP.DLL Malformed DNS Denial of Service*
- ***Signature 3781:*** *Netware Driver Denial of Service Vulnerability*
- ***Signature 3782:*** *Vulnerability in Workstation Service Could Allow Remote Code Execution*

- ***Signature 3783:*** *Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution*
- ***Signature 3791:*** *Vulnerability in Microsoft Rich Edit and Microsoft MFC*
- ***Signature 3792****: Vulnerability in Windows Media Player Could Allow Remote Code Execution*
- ***Signature 3797:*** *Microsoft Windows Message Queuing Buffer Overflow Vulnerability*
- ***Signature 3799:*** *Vulnerability in Windows Media Player ASX PlayList File*
- ***Signature 3805:*** *Adobe Download Manager Stack Overflow Vulnerability*
- ***Signature 3812:*** *Adobe Reader Plug-in Cross-Site Scripting Vulnerability (2)*
- ***Signature 3815:*** *Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege*
- ***Signature 3822:*** *Vulnerability in Windows Shell Could Allow Elevation of Privilege*
- ***Signature 3825:*** *CAPICOM.DLL Improper Arguments Vulnerability*
- ***Signature 3830:*** *Internet Explorer 7 'navcancl' Address Bar Spoofing Vulnerability*
- ***Signature 3832:*** *EMF Elevation of Privilege Vulnerability*
- ***Signature 3836:*** *GDI Incorrect Parameter Elevation of Privilege Vulnerability*
- ***Signature 3838:*** *Windows Animated Cursor Handling vulnerability*
- ***Signature 3839:*** *Microsoft Agent URL Parsing Vulnerability*
- ***Signature 3840:*** *Vulnerability in RPC on Windows DNS Server Could Allow Remote Code Execution*
- ***Signature 3847:*** *Vulnerability in Win32 API Could Allow Remote Code Execution*
- ***Signature 3849:*** *URL Redirect Vulnerability in MHTML Protocol Handler via Internet Explorer*
- ***Signature 3850:*** *IE and OE Cross Domain Security Bypass Vulnerability*
- ***Signature 3853:*** *Command Injection flaw in IE/Firefox*
- ***Signature 3855:*** *Firefox Illegal URL Quotes Vulnerability*
- ***Signature 3858:*** *Vulnerability in OLE Automation Could Allow Remote Code Execution*
- ***Signature 3864:*** *MS Agent Buffer Overflow Vulnerability*
- ***Signature 3865:*** *Vulnerability in Windows UNIX Services could allow elevation of privilege*
- ***Signature 3866:*** *Vulnerability in Apple QuickTime 'qtnext' attribute could allow remote code execution*
- ***Signature 3868:*** *Vulnerability in ShellExecute Could Allow Remote Code Execution*
- ***Signature 3918:*** *Outlook mailto URI Handling Vulnerability*
- ***Signature 3924:*** *Vulnerability in Windows GDI32 Could Allow Remote Code Execution*
- ***Signature 3926:*** *IBM Lotus Expeditor cai: URI handling Vulnerability*

- ***Signature 3939:*** *Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution*
- ***Signature 3947:*** *OneNote URI Validation Error Vulnerability*
- ***Signature 3948:*** *Windows Metafile Remote Code Execution Vulnerability*
- ***Signature 3958:*** *Vulnerability in Message Queuing Could Allow Remote Code Execution*
- ***Signature 3961:*** *Vulnerability in Server Service Could Allow Remote Code Execution*
- ***Signature 3965:*** *Adobe Acrobat util.printf Buffer Overflow*
- ***Signature 6001:*** *Suspicious Data Sequence in Javascript*
- ***Signature 6026:*** *Vulnerability in Event System could allow Remote Code Execution*
- ***Signature 6027:*** *Vulnerability in GDI could allow Remote Code Execution*
- ***Signature 6028:*** *Vulnerability in Windows Shell Handler URL Validation Could Allow Remote Code Execution*
- ***Signature 6033:*** *Shortcut Icon Loading Vulnerability*
- ***Signature 6034:*** *IE createTextRange Vulnerability*
- ***Signature 6039:*** *Vulnerability in Windows Could Allow Remote Code Execution using maliciously crafted DVR-MS file*

How to Update

You need to check in the update package to the ePO Repository, and then send the updated information to the agents. Please refer to 'Updating' in Chapter 8 of 'Host Intrusion Prevention Product Guide'