McAfee Exploit Prevention Content 11535

Release Notes | 2021-06-15

Content package version for –

McAfee Endpoint Security Exploit Prevention: 10.6.0.11535[1]

McAfee Host Intrusion Prevention: 8.0.0.11535[2]

[1] - Applicable on all versions of McAfee Endpoint Security Exploit Prevention including version 10.7.x

[2] - Applicable on all versions of McAfee Host Intrusion Prevention content including Host IPS 8.0 Patch 16.

IMPORTANT: McAfee V3 Virus Definition Updates (DATs) version 3786 or above is a mandatory prerequisite for this Exploit prevention content update on McAfee Endpoint Security versions 10.5.x and 10.6.x only.
Refer to the below KB for more information:
https://kc.mcafee.com/corporate/index?page=content&id=KB91867

IMPORTANT: Either of the below McAfee Host IPS 8.0 Extension packages is a mandatory prerequisite for receiving the new security or policy updates for this content

1. Host IPS 8.0 Patch 15 Extension (build 8.0.0.1334) – Applicable for Host IPS 8.0 Patch 15 and below
2. Host IPS 8.0 Patch 14 Extension Hotfix 114831 (build 8.0.0.1326) – Applicable for Host IPS 8.0 Patch 14 and below

Refer to the below KB for more information:
https://kc.mcafee.com/corporate/index?page=content&id=KB92596

New Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 6204: *HTTP Protocol Stack Remote Code Execution Vulnerability* *Description:* - *HTTP.sys is a web server for ASP.NET Core that only runs on Windows independently or in conjunction with IIS. This event indicates a suspicious attempt made to exploit a vulnerability in HTTP.SYS by sending malformed query packets. Successful exploitation of this vulnerability can lead to Remote code execution as kernel. This signature can slow down HTTP request processing so customers are advised to enable the signature only as a temporary stop-gap measure on vulnerable OS platforms.* - *The signature is disabled by default.*	*8.0.0 (Patch 13)*	*10.6.0*

Note: Customer can change the level/reaction-type of this signature based on their requirement.		
Signature 6205: *T1055 - Malware Behavior: Process Hollowing attempt on Explorer.EXE* *Description:* - *Process hollowing is a technique used by some malware in which a legitimate process is loaded on the system solely to act as a container for hostile code. At launch, the legitimate code is deallocated and replaced with malicious code. The advantage is that this helps the process hide amongst normal processes better. This event indicates a malware attempt to hollow explorer.exe process. This technique was seen to be used by malwares like IcedID and Hancitor.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*Not Applicable*	*10.6.0*
Signature 6206: *T1105 - ASR : File Download attempt using Bitsadmin* *Description:* - *This event indicates that BitsAdmin attempted to download a file. This is an access protection rule that can be used by customers who want to restrict the usage of bitsadmin for file download.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*Not Applicable*	*10.6.0*
Signature 6207: *ASR : File Download attempt by Scripts* *Description:* - *This event indicates that vbscript/cscript attempted to download a file. This is an access protection rule that can be used by customers who want to restrict the usage of vbscript/cscript for file download.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*Not Applicable*	*10.6.0*

NOTE: Refer to the KB for the default Reaction-type associated with Signature severity level for all supported Product versions:
https://kc.mcafee.com/corporate/index?page=content&id=KB90369

Updated Windows Signatures			Minimum Supported Product version	
			Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature Description Modification: *The default signature description has been modified for the below signature .*				
Signature 6189: *Malicious Behavior: Possible Encryption attempt on a directory detected*			*Not Applicable*	*10.6.0*
Signature Severity Level Modification: *The default signature severity level has been modified for the below signatures as specified with an intent to be deprecated from content in future releases. The below listed signatures are for protection against very old vulnerabilities and are obsolete on Windows 7, Windows Server 2008 R2 or higher platforms.*				
	Previous Setting	Current Setting		
Signature 2201*: Vulnerabilities in Windows Search Could Allow Remote Code Execution (CVE-2008-4269)*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 2212*: Vulnerabilities in Windows Win32k Kernel Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 2213*: Vulnerability in Microsoft Exchange EMSMDB32 Could Allow Denial of Service*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 2251*: Vulnerability in Windows Shell Handler Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3727*: IE drag and drop file installation*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3728*: MSRPC LLSSRV Buffer Overflow*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3730*: Windows Explorer MSHTA Script Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3731*: URL Decoding Zone Spoofing Vulnerability*	*High*	*Disabled*	*8.0.0*	*10.6.0*
Signature 3733*: Windows Messenger Service Buffer Overflow*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3734*: Print Spooler Service Buffer Overflow*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3735*: Plug and Play Buffer Overflow (Zotob)*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3736*: Telephony Service Buffer Overflow*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3738*: MSDTC RPC Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3739*: Windows Plug-and-Play Buffer Overflow Vulnerability 2*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3740*: Client Services For Netware Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3741*: Windows Metafile Heap Overflow Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3742*: Windows Enhanced Metafile Heap Overflow Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
Signature 3744*: Graphics Rendering Engine Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*

***Signature 3749**: Internet Explorer HTA Execution Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3750**: Remote COM Activation by Desktop.ini Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3752**: MSDTC RPC DoS Vulnerability*	*High*	*Disabled*	*8.0.0*	*10.6.0*
***Signature 3757**: MSHTA Directory Traversal Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3758**: Management Console Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3759**: MHTML Parsing Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3760**: Internet Explorer FTP Command Injection Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3761**: Winsock Hostname Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3767**: Windows Server Service Buffer Overflow Vulnerability (2)*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3768**: Windows Server Service Buffer Overflow Vulnerability (Tighter Security)*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3769**: Windows Metafile Denial of Service Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3771**: Vulnerability in Indexing Service Could Allow Cross-Site Scripting*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3772**: Client Services for Netware BO Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3775**: Windows Shell Vulnerability in WebViewFolderIcon*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3777**: Windows ASN.1 Heap Overflow Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3778**: Internet Explorer 7 Address Bar Spoofing Vulnerability*	*Medium*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3780**: IPNATHLP.DLL Malformed DNS Denial of Service*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3781**: Netware Driver Denial of Service Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3782**: Vulnerability in Workstation Service Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3792**: Vulnerability in Windows Media Player Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3797**: Microsoft Windows Message Queuing Buffer Overflow Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3799**: Vulnerability in Windows Media Player ASX PlayList File*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3805**: Adobe Download Manager Stack Overflow Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3812**: Adobe Reader Plug-in Cross-Site Scripting Vulnerability (2)*	*Medium*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3815**: Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3824**: Google Desktop JavaScript Injection Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*

***Signature 3825**: CAPICOM.DLL Improper Arguments Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3832**: EMF Elevation of Privilege Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3836**: GDI Incorrect Parameter Elevation of Privilege Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3839**: Microsoft Agent URL Parsing Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3840**: Vulnerability in RPC on Windows DNS Server Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3847**: Vulnerability in Win32 API Could Allow Remote Code Execution*	*Medium*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3849**: URL Redirect Vulnerability in MHTML Protocol Handler via Internet Explorer*	*Medium*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3850**: IE and OE Cross Domain Security Bypass Vulnerability*	*Medium*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3853**: Command Injection flaw in IE/Firefox*	*Medium*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3855**: Firefox Illegal URL Quotes Vulnerability*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3858**: Vulnerability in OLE Automation Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3864**: MS Agent Buffer Overflow Vulnerability*	*Medium*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3865**: Vulnerability in Windows UNIX Services could allow elevation of privilege*	*Medium*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3866**: Vulnerability in Apple QuickTime 'qtnext' attribute could allow remote code execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3868**: Vulnerability in ShellExecute Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3917**: Windows File Share Creation*	*Low*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3945**: Adobe Flash Clipboard Poisoning Vulnerability*	*Low*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3918**: Outlook mailto URI Handling Vulnerability*	*High*	*Disabled*	*8.0.0*	*10.6.0*
***Signature 3924**: Vulnerability in Windows GDI32 Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3926**: IBM Lotus Expeditor cai: URI handling Vulnerability*	*High*	*Disabled*	*8.0.0*	*10.6.0*
***Signature 3939**: Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution*	*High*	*Disabled*	*8.0.0*	*Not Applicable*
***Signature 3947**: OneNote URI Validation Error Vulnerability*	*High*	*Disabled*	*8.0.0*	*10.6.0*

Existing Coverage for New Vulnerability	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Coverage by GPOP: *GBOP signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerability:* - *CVE-2021-28554*	*8.0.0*	*10.6.0*
Coverage by GPOP: *GBOP signatures 428, 1146, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerability:* - *CVE-2021-31959*	*8.0.0*	*10.6.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2021-31951* - *CVE-2021-31952* - *CVE-2021-31954* - *CVE-2021-31956*	*8.0.0*	*10.6.0*

How to Update

Please find below the KB article reference on how to update the content for following products:

1. McAfee Endpoint Security Exploit Prevention:
https://kc.mcafee.com/corporate/index?page=content&id=KB92136
2. McAfee Host Intrusion Prevention:
https://kc.mcafee.com/corporate/index?page=content&id=KB53092