McAfee Exploit Prevention Content 7616

Release Notes | 2017-03-14

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7616

Endpoint Security Exploit Prevention: 10.5.0.7616

Below is the updated signature information for the McAfee Exploit Prevention content.

New Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Signature 6089**: Microsoft Office DLL side load vulnerability (CVE-2017-0039)* *Description:* - *This event indicates an attempt to exploit a vulnerability that exists in Microsoft Office which loads a malicious DLL* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement.*	*8.0.0*	*Not Applicable*
***Signature 8000**: Behavior Based Exploit Protection* *Description:* - *This event indicates detection of exploit behavior* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement.* *This signature is applicable only for Windows 7, Windows 8 and Windows 8.1 Operating Systems only* *This signature is applicable only for 32 bit Applications such as Internet Explorer, Adobe Reader and Adobe Collabsync only*	*8.0.0*	*Not Applicable*

***Signature 8001**: Suspicious Exploit Behavior* *Description:* - *This event indicates detection of suspicious exploit behavior. The signature has a pre-condition of sig 8000 being enabled* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement.* *This signature is applicable only for Windows 7, Windows 8 and Windows 8.1 Operating Systems only* *This signature is applicable only for 32 bit Applications such as Internet Explorer, Adobe Reader and Adobe Collabsync only*	*8.0.0*	*Not Applicable*
***Signature 8002**: Possible Exploit Behavior* *Description:* - *This event indicates detection of possible exploit behavior. The signature has a pre-condition of sig 8000 being enabled.* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement.* *This signature is applicable only for Windows 7, Windows 8 and Windows 8.1 Operating Systems only* *This signature is applicable only for 32 bit Applications such as Internet Explorer, Adobe Reader and Adobe Collabsync only*	*8.0.0*	*Not Applicable*

Updated Windows Signatures	**Minimum Supported Product version**	
	Host Intrusion Prevention	**Endpoint Security Exploit Prevention**
***Signature 907**: PWDump Tool Activation* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 913**: Event Log Registry Permissions Modified* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 914**: Event Log File Path Modified* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*

***Signature 993**: System Drive Executable Modification* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 2664**: IE Envelope - Windows Help Execution* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 2786**: IIS 6.0 Denial of Service Vulnerability* *Description:* - *The signature name has been modified to correct a minor spelling error*	*8.0.0*	*Not Applicable*
***Signature 3754**: Illegal Execution in winword.exe* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3789**: Vulnerability in Microsoft Step-by-Step Interactive Training* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3809**: Microsoft Outlook VEVENT Vulnerability* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3814**: Microsoft Word Enveloping - Illegal file creation* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3821**: Vulnerability in Microsoft Word Macro Security* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*

***Signature 3837**: Font Rasterizer Elevation of Privilege Vulnerability* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3854**: Sun Java WebStart JNLP Stack Buffer Overflow Vulnerability* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3861**: Vulnerability in Windows Media Player Could Allow Remote Code Execution* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3921**: MS Word Mail Merge Vulnerability* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3937**: Vulnerability in Microsoft Office WPG Image Converter Filter Could Allow Remote Code Execution* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 3938**: Windows Animated Cursor Handling vulnerability* *(BZ # 1181911)* *Description:* - *This signature has been modified to support Windows 8 and higher platforms*	*8.0.0*	*Not Applicable*
***Signature 6013**: Suspicious Function Invocation - CALL Not Found* *Description:* - *This signature has been modified to reduce the false positives*	*8.0.0*	*10.1*
***Signature 6015**: Suspicious Function Invocation - Target Address Mismatch* *Description:* - *This signature has been modified to reduce the false positives*	*8.0.0*	*10.5*
***Signature 6045**: SMB Brute Force Attack* *(BZ #1178644)* *Description:*	*8.0.0*	*Not Applicable*

- *This signature has been modified to fix a performance issue found with HIPS 8 Patch 6 and above platforms*		
***Signature 6087**: Powershell Command Restriction - EncodedCommand (BZ # 1181795)* *Description:* - *This signature has been modified to enhance the protection*	*8.0.0*	*10.5*

Other Changes

***BugFix:** HIPS Content has been modified to fix a Policy load error which was identified in NIPS for Russian Locale*
(BZ # 1176495)
Note: This change is not applicable for Endpoint Security Exploit Prevention.

Inclusion of Host IPS 8.0 Hotfix 1153407

This content update also applies a Host IPS hotfix 1153407 on the client systems running Host IPS 8.0 Patch 5, Patch 6 or Patch 7 only. Successful installation of hotfix displays a different client version depending on which patch version is installed as indicated below:

- *Patch 7: 8.0.0.3800*
- *Patch 6: 8.0.0.3500*
- *Patch 5: 8.0.0.3250*

Refer below KB for more details on this hotfix.
https://kc.mcafee.com/corporate/index?page=content&id=KB87658

Existing coverage for New Vulnerabilities	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Coverage by GBOP:** GBOP Signatures 428, 1146, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-0009* - *CVE-2017-0014* - *CVE-2017-0018* - *CVE-2017-0023* - *CVE-2017-0037* - *CVE-2017-0040*	*8.0.0*	*10.1*

- *CVE-2017-0049* - *CVE-2017-0059* - *CVE-2017-0130* ***Coverage by GBOP:*** *GBOP Signatures 428, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-0006* - *CVE-2017-0020* - *CVE-2017-0027* - *CVE-2017-0052* ***Coverage by GBOP:*** *GBOP Signatures 428, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-0019* - *CVE-2017-0030* - *CVE-2017-0031* - *CVE-2017-0053* - *CVE-2017-0060* - *CVE-2017-0062* - *CVE-2017-0072* - *CVE-2017-0073* - *CVE-2017-0083* - *CVE-2017-0086* - *CVE-2017-0087* - *CVE-2017-0088* - *CVE-2017-0089* - *CVE-2017-0090* - *CVE-2017-0105* ***Coverage by GPEP:*** *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2017-0001* - *CVE-2017-0005* - *CVE-2017-0024* - *CVE-2017-0025* - *CVE-2017-0026* - *CVE-2017-0047* - *CVE-2017-0050* - *CVE-2017-0056* - *CVE-2017-0078* - *CVE-2017-0079* - *CVE-2017-0080* - *CVE-2017-0082* - *CVE-2017-0103*		

- *CVE-2017-0108* ***Coverage by Other Signatures:*** *IIS Cross-Site Scripting Signature (Signature 940) is expected to cover the below vulnerability:* - *CVE-2017-0055*	*8.0.0*	*Not Applicable*

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'