McAfee Exploit Prevention Content 7767

Release Notes | 2017-05-19

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7767

Note: This content update is not applicable for Endpoint Security Exploit Prevention

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 6093**: Microsoft Office OneNote DLL side load vulnerability (CVE-2017-0197)* *Description:* - *This event indicates an attempt to exploit a vulnerability that exist in Microsoft Office OneNote 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 6094**: Adobe Acrobat Reader DLL side load vulnerability (CVE-2017-3013)* *Description:* - *This event indicates an attempt to exploit a vulnerability that exist in Adobe Acrobat Reader 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 6095**: Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144, CVE-2017-0145)* *(BZ #1191755)* *Description:* - *This event indicates an attempt to exploit SMB remotely* - *This signature is set to level Low by default* *Note: Customer can change the level of this signature based on their requirement.*	*8.0.0 Patch 9*	*Not Applicable*

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Signature 825**: BackOrifice 2000 Trojan* *Description :* - *A new Signature instance has been added to protect renaming of registry key by BackOrifice 2000 Trojan horse*	*8.0.0*	*Not Applicable*
***Signature 3907**: Access Protection - Prevent programs registering as a service* *(BZ #1190654)* *Description:* - *This signature has been modified to reduce the false positives*	*8.0.0*	*Not Applicable*
***Signature 6048**: Suspicious Function Invocation - Different Stack* *Description:* - *This signature has been modified to support all 32-bit processes* - *Signature Description has been modified to remove the specific processes coverage information as it provides generic protection*	*8.0.0*	*Not Applicable*

Other Changes

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-2017-0222* - *CVE-2017-0224* - *CVE-2017-0226* - *CVE-2017-0228* - *CVE-2017-0229* - *CVE-2017-0230* - *CVE-2017-0238*	*8.0.0*	*10.1*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-0254* - *CVE-2017-0261* - *CVE-2017-0262* - *CVE-2017-0264* - *CVE-2017-0265* - *CVE-2017-0281*	*8.0.0*	*10.1*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2017-0077* - *CVE-2017-0213* - *CVE-2017-0244* - *CVE-2017-0246* - *CVE-2017-0263*	*8.0.0*	*10.1*
Coverage by Other Signatures: *IIS Cross-Site Scripting Signature (Signature 940) is expected to cover the below vulnerability:* - *CVE-2017-0255*	*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'