McAfee
Together is power.

McAfee Exploit Prevention Content 9184

Release Notes | 2019-04-09

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.9184

McAfee Endpoint Security Exploit Prevention: 10.6.0.9184

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 2600: *IE Envelope - Mail Files Access* *Description:* - This event indicates an attempt to read an email file type by Internet Explorer. In most configurations the browser should not access files of this type directly, and such an operation might suggest that the browser is compromised and that an attacker is attempting to use the browser to read private information from the machine running the browser. The event will trigger each time the browser attempts to open a file whose type is known to be used by Microsoft Outlook. These types include single email files, address book files and personal folder files. This event will not be triggered if the email file accessed by the browser is located in a directory used for browser operations, such as the windows system directory or the temporary directories used by the browser. - This signature is set to level Low by default Note: Customer can change the level / reaction-type of this signature based on their requirement. This signature is only applicable on Endpoint Security Exploit Prevention Product.	8.0.0	10.5.3
Signature 2664: *IE Envelope - Windows Help Execution* *Description:* - This event indicates an attempt by Internet Explorer to execute the Microsoft Windows Help (winhlp32.exe). It is possible to invoke Windows Help from Internet Explorer 8,7,6 using VBScript. Passing malicious .HLP file to Windows Help could allow remote attacker to run arbitrary command. This event will trigger each time the browser attempts to execute the Windows Help run time process.	8.0.0	10.5.3

- This signature is set to level Medium by default Note: Customer can change the level / reaction-type of this signature based on their requirement. This signature is only applicable on Endpoint Security Exploit Prevention Product.		
Signature 6131*: Weaponized OLE object infection via WMI* *Description:* - This event indicates an attempt to access WMI through WORD, EXCEL or POWERPOINT using macros. Using WMI the attacker can execute some other executable like powershell or wscript from WMIPRVSE which is a malicious activity and signifies infection. - This signature is set to level Low by default Note: Customer can change the level / reaction-type of this signature based on their requirement.	8.0.0	10.5.3
Signature 6132*: WINRAR Filename Directory Traversal Vulnerability* *Description:* - This event indicates an attempt to exploit a Directory Traversal Vulnerability in WINRAR by creating malicious file in Start Up Directory. Such attempts can be made by adversary to maintain persistence through system reboot. - *This signature is set to level Low by default* Note: Customer can change the level / reaction-type of this signature based on their requirement.	8.0.0	10.5.3

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**
BugFix: *NIPS driver for Endpoint Security Exploit Prevention has been modified to handle policy mismatch of NIPS signatures.*	NA	10.5.3

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, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2019-0752* - *CVE-2019-0753* - *CVE-2019-0842* - *CVE-2019-0862*	8.0.0	10.2.0
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerability:* - *CVE-2019-0827*	8.0.0	10.2.0
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2019-0801* - *CVE-2019-7061* - *CVE-2019-7088* - *CVE-2019-7109* - *CVE-2019-7110* - *CVE-2019-7111* - *CVE-2019-7112* - *CVE-2019-7114* - *CVE-2019-7115* - *CVE-2019-7116* - *CVE-2019-7117* - *CVE-2019-7118* - *CVE-2019-7119* - *CVE-2019-7120* - *CVE-2019-7121* - *CVE-2019-7122* - *CVE-2019-7123* - *CVE-2019-7124* - *CVE-2019-7125* - *CVE-2019-7127* - *CVE-2019-7128* - *CVE-2019-7096* - *CVE-2019-7108*	8.0.0	10.2.0
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2019-0685* - *CVE-2019-0730* - *CVE-2019-0731* - *CVE-2019-0735* - *CVE-2019-0796*	8.0.0	10.2.0

- *CVE-2019-0802* - *CVE-2019-0803* - *CVE-2019-0805* - *CVE-2019-0814* - *CVE-2019-0822* - *CVE-2019-0836* - *CVE-2019-0837* - *CVE-2019-0840* - *CVE-2019-0841* - *CVE-2019-0844* - *CVE-2019-0848* - *CVE-2019-0849* - *CVE-2019-0859*		

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’