McAfee Exploit Prevention Content 8330

Release Notes | 2018-04-10

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8330

McAfee Endpoint Security Exploit Prevention: 10.5.0.8330

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 8000**: Behavior Based Exploit Protection* *Description:* *- This event indicates detection of exploit behavior* *- This signature is set to level Low 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*	*8.0.0 (Content: 8.0.0.7616)*	*10.5.3*
***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*	*8.0.0 (Content: 8.0.0.7616)*	*10.5.3*

***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*	*8.0.0 (Content: 8.0.0.7616)*	*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**
***Signature 6108**: Powershell - Suspicious downloadstring script execution* *Description:* - *The default Severity level of the Signature has been modified to Medium*	*8.0.0*	*10.2.0*
***Signature 6109:** Powershell - Suspicious wmi script execution* *Description:* - *The default Severity level of the Signature has been modified to Medium*	*8.0.0*	*10.2.0*
***Signature 6110**: Fileless Threat: Startup Program Creation* *Description:* - *The default Severity level of the Signature has been modified to High*	*8.0.0*	*Not Applicable*
***Signature 6111**: Fileless Threat: Click fraud operation* *Description:* - *The default Severity level of the Signature has been modified to High*	*8.0.0*	*Not Applicable*

	Minimum Supported Product version

Existing coverage for New Vulnerabilities	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-2018-0870* - *CVE-2018-0988* - *CVE-2018-0991* - *CVE-2018-0996* - *CVE-2018-0997* - *CVE-2018-1001* - *CVE-2018-1004* - *CVE-2018-1018* - *CVE-2018-1023*	*8.0.0*	*10.2.0*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-0920* - *CVE-2018-1003* - *CVE-2018-1011* - *CVE-2018-1026* - *CVE-2018-1027* - *CVE-2018-1028* - *CVE-2018-1029* - *CVE-2018-1030*	*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-2018-4932* - *CVE-2018-4935* - *CVE-2018-4936* - *CVE-2018-4937*	*8.0.0*	*10.2.0*

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'