McAfee Exploit Prevention Content 9845

Release Notes | 2020-01-18

Content package version for –

McAfee Host Intrusion Prevention: 8.0.0.9845

McAfee Endpoint Security Exploit Prevention: 10.6.0.9845

Note: 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.

Refer to the below KB for more information:

https://kc.mcafee.com/corporate/index?page=content&id=KB91867

New Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 6146: *Remote Desktop Services Remote Code Execution Vulnerability* *Description:* - *This event indicates an attempt to exploit a Remote Code Execution Vulnerability in Remote Desktop Services popularly known as Bluekeep. Note: for this signature to work properly, the 'Automatically block intruders' option should be enabled and the value should be set to greater than or equal to 60 seconds.* - *This signature is Disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.* *For this signature to work properly, The signature should be enabled to "Block" mode in ePO and the 'Automatically block intruders' option should be enabled and the value should be set to greater than or equal to 60 seconds.*	*8.0.0 Patch 12*	*10.5.3*
Signature 6148: *Malware Behavior: Windows EFS abuse* *Description:* - *EFS or Encrypt file system is a Microsoft feature of NTFS that provides file-level encryption. This event indicates a malware attempt to encrypt files and folders using EFS.* - *This signature is set to level High by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*Not Applicable*	*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 6114: *Fileless Threat: Reflective EXE Self Injection* *Description:* - *The Signature has been modified to reduce false positives.*	*Not Applicable*	*10.5.3*
Signature 6115: *Fileless Threat: Reflective DLL Remote Injection* *Description:* - *The Signature has been modified to reduce false positives.*	*Not Applicable*	*10.5.3*
Signature 6121: *Fileless Threat: Shellcode Self Injection* *Description:* - *The Signature has been modified to reduce false positives.*	*Not Applicable*	*10.5.3*
Signature 6145: *Attempt to exploit Device Guard* *Description:* - *The Signature has been modified to reduce false positives.*	*Not Applicable*	*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-2020-0674*	*8.0.0*	*10.5.0*

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'