McAfee Exploit Prevention Content 9792

Release Notes | 2019-12-19

Content package version for –

McAfee Host Intrusion Prevention: 8.0.0.9792

McAfee Endpoint Security Exploit Prevention: 10.6.0.9792

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 6145: *Attempt to exploit Windows Device Guard* *Description:* - *This event indicates an attempt to exploit vulnerability in windows device guard which can affect the endpoint security on the system.* - *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*
Signature 6147: *Adobe Installer DLL planting vulnerability (CVE-2019-16444)* *Description:* - *This event indicates an attempt to exploit vulnerability in adobe installer by which an attacker can load a dll to execute malicious code.* - *This signature is set to level Low 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 6070: *Hidden Powershell Detected* *Description:* - *The Signature has been modified to reduce false positives.*	*Not Applicable*	*10.5.3*
Signature 6073: *Execution Policy Bypass in Powershell* *Description:* - *The Signature has been modified to reduce false positives.*	*Not Applicable*	*10.5.3*
Signature 6113: *Fileless Threat: Reflective Self Injection* *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, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2020-0609* - *CVE-2020-0610* - *CVE-2020-0612*	*Not Applicable*	*10.5.0*
Coverage by GBOP: *GBOP Signatures 428, 1146, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2020-0611* - *CVE-2020-6040*	*8.0.0*	*10.5.0*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2020-0650* - *CVE-2020-0651* - *CVE-2020-0652* - *CVE-2020-0653*	*8.0.0*	*10.5.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-0742* - *CVE-2020-0607*	*8.0.0*	*10.5.0*

- *CVE-2020-0608* - *CVE-2020-0622* - *CVE-2020-0624* - *CVE-2020-0642* - *CVE-2020-0643*		
Coverage by Access Protection: *File Signature 6147 is expected to cover the below vulnerabilities:* - *CVE-2019-16444*	*8.0.0*	*10.5.3*

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'