McAfee Exploit Prevention Content 9096

Release Notes | 2019-03-12

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.9096

McAfee Endpoint Security Exploit Prevention: 10.6.0.9096

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 1149: *CMD Tool Access by a Windows Mail Client or IE* *Description:* - *This event indicates an attempt by a mail client or Internet Explorer to access, modify or execute a system program that may be used to modify the configuration of your system* - *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 2798: *Windows Lync Insecure DLL loading Vulnerability* *Description:* - *This event indicates an attempt to exploit a vulnerability exists in Microsoft Lync that loads malicious DLLs* - *This signature is Disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*
Signature 3829: *Sticky Keys File Replacement Backdoor* *Description:* - *This event could indicate an attempt to exploit a vulnerability in the Microsoft Windows that could allow successful attackers to maintain access to confidential information. A successful exploit would allow a user with administrative permissions to no longer need a username or password to access the computer in the future.* - *This signature is set to level Low by default.*	*8.0.0*	*10.5.3*

Note: Customer can change the level/reaction-type of this signature based on their requirement.		

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=KB67561

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 6013: *Suspicious Function Invocation - CALL Not Found* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*

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-2019-0665* - *CVE-2019-0666* - *CVE-2019-0667* - *CVE-2019-0680* - *CVE-2019-0763* - *CVE-2019-0765* - *CVE-2019-0772* - *CVE-2019-0780* - *CVE-2019-0783* - *CVE-2019-0784*	*8.0.0*	*10.2.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2019-0614* - *CVE-2019-0696* - *CVE-2019-0702* - *CVE-2019-0755* - *CVE-2019-0759* - *CVE-2019-0767* - *CVE-2019-0774* - *CVE-2019-0775*	*8.0.0*	*10.2.0*

- *CVE-2019-0776* - *CVE-2019-0782* - *CVE-2019-0797* - *CVE-2019-0808*		

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'