McAfee Exploit Prevention Content 9684

Release Notes | 2019-11-12

Content package version for –

McAfee Host Intrusion Prevention: 8.0.0.9684

McAfee Endpoint Security Exploit Prevention: 10.6.0.9684

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

Below is the updated signature information for the McAfee Exploit Prevention content.

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 3829: *Sticky Keys File Replacement Backdoor* *Description:* - *The signature has been modified to reduce the false positives*	*8.0.0*	*10.5.0*
Signature 6013: *Suspicious Function Invocation – CALL Not Found* *Description:* - *The signature has been modified to reduce the false positives*	*8.0.0*	*10.5.3*
Signature 6113: *Fileless Threat: Reflective Self Injection* *Description:* - *The severity level of the signature has been changed to High by default*	*8.0.0*	*10.5.3*
Signature 6118: *Fileless Threat: Malicious Code Execution using DotNetToJScript Technique* *Description:* - *Signature has been modified to enhance the protection*	*8.0.0*	*10.5.0*
Signature 6121: *Fileless Threat: Shellcode Self Injection* *Description:* - *Signature has been modified to enhance the protection*	*8.0.0*	*10.5.3*
Signature 6135: *Unmanaged Powershell Detected* *Description:* - *The signature has been modified to reduce the false positives*	*8.0.0*	*10.5.0*

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
BugFix: *Application Protection List has been modified to include the below process* - *wmic.exe*	*8.0.0*	*10.5.0*

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-2019-1406* - *CVE-2019-16445* - *CVE-2019-16446* - *CVE-2019-16448* - *CVE-2019-16449* - *CVE-2019-16450* - *CVE-2019-16451* - *CVE-2019-16452* - *CVE-2019-16454* - *CVE-2019-16455* - *CVE-2019-16456* - *CVE-2019-16457* - *CVE-2019-16458* - *CVE-2019-16459* - *CVE-2019-16460* - *CVE-2019-16461* - *CVE-2019-16462* - *CVE-2019-16463* - *CVE-2019-16464* - *CVE-2019-16465*	*8.0.0*	*10.5.0*
Coverage by GBOP: *GBOP Signatures 428, 1146, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2019-1390* - *CVE-2019-1429* - *CVE-2019-1400*	*8.0.0*	*10.5.0*

- *CVE-2019-1461* - *CVE-2019-1462* - *CVE-2019-1463* - *CVE-2019-1485*		
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2019-1446* - *CVE-2019-1448* - *CVE-2019-1464*	*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-2019-1392* - *CVE-2019-1393* - *CVE-2019-1394* - *CVE-2019-1395* - *CVE-2019-1396* - *CVE-2019-1403* - *CVE-2019-1404* - *CVE-2019-1407* - *CVE-2019-1408* - *CVE-2019-1433* - *CVE-2019-1434* - *CVE-2019-1435* - *CVE-2019-1436* - *CVE-2019-1437* - *CVE-2019-1438* - *CVE-2019-1439* - *CVE-2019-1440* - *CVE-2019-1458* - *CVE-2019-1465* - *CVE-2019-1466* - *CVE-2019-1467* - *CVE-2019-1469* - *CVE-2019-1472* - *CVE-2019-1474*	*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'