McAfee Exploit Prevention Content 8591

Release Notes | 2018-08-14

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8591

McAfee Endpoint Security Exploit Prevention: 10.6.0.8591

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 2837: *Microsoft Antimalware Client Privilege Escalation Vulnerability (CVE-2013-0078)* *Description:* - *This event indicates an attempt to exploit a vulnerability in Microsoft Antimalware Client Mstscax that could allow attackers to escalate their privileges on the machine.* - *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 (Content: 8.0.0.4865)*	*10.5.3*
Signature 2842: *Exploitation using Library load from UNC Path* *Description:* - *This event indicates library load from UNC path which allows attacker to exploit remote code execution vulnerability.* - *This signature is Disabled by default.* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*8.0.0 (Content: 8.0.0.5221)*	*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 413: *Suspicious Double File Extension Execution (BZ #1244696)* *Description:* - *The Signature has been modified to reduce false positives*	*8.0.0*	*10.5.3*
Signature 6118: *Fileless Threat: Malicious Code Execution using DotNetToJScript Technique* *Description:* - *The Signature has been modified to extend coverage for Microsoft Outlook process* - *The default level of the signature is changed to High*	*8.0.0*	*10.2.0*
Signature 8001: *Suspicious Exploit Behavior* *Description:* - *The Signature has been modified to enhance the protection*	*8.0.0*	*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-2018-8371* - *CVE-2018-8376* - *CVE-2018-8344* - *CVE-2018-8389* - *CVE-2018-8353*	*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-2018-8345* - *CVE-2018-12808*	*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-2018-8379*	*8.0.0*	*10.2.0*

Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-8401* - *CVE-2018-8404* - *CVE-2018-8405* - *CVE-2018-8406*	*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'