McAfee Exploit Prevention Content 8274

Release Notes | 2018-03-13

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8274

McAfee Endpoint Security Exploit Prevention: 10.5.0.8274

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

Host IPS 8.0 Hotfix Change	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Removal of Host IPS 8.0 Hotfix 1153407 from content - *The Hotfix 1153407 is removed from the content update package.* - *Host IPS 8.0 Patch 5, 6, 7 will not apply content updates (starting from March content 8.0.0.8274) if Hotfix 1153407 is not installed* *Note: This change does not apply to Host IPS 8.0 Patch 8 or later, nor to Patch 4 and earlier.* *Refer to the KB for further details:* *https://kc.mcafee.com/corporate/index?page=content&id=KB90361*	*8.0.0*	*Not Applicable*

New Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 6112*: MS Outlook trying to execute unwanted programs* *Description:* - *This event indicates an attempt to execute cmd.exe, powershell.exe, mshta.exe by MS Outlook* - *This signature is set to level Low by default.* *Note: Customer can change the level of this signature based on their requirement.*	*8.0.0*	*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 3821**: Vulnerability in Microsoft Word Macro Security* *Description:* - *The Signature has been modified to reduce the false positives*	*Not Applicable*	*10.5.3*
***Signature 6077:** Microsoft Visio DLL Hijacking Vulnerability* *Description:* - *The Signature has been modified to reduce the 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-2018-0889* - *CVE-2018-0935*	*8.0.0*	*10.2.0*
***Coverage by GBOP:** GBOP Signatures 428, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2018-0903* - *CVE-2018-0922*	*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-2018-4919* - *CVE-2018-4920*	*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'