McAfee Exploit Prevention Content 8170

Release Notes | 2017-12-12

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8170

McAfee Endpoint Security Exploit Prevention: 10.5.0.8170

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 6107**: MS Word trying to execute unwanted programs* *Description:* - *This event indicates an attempt to execute cmd.exe, powershell.exe, mshta.exe by MS Word.* - *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*

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Inclusion of Host IPS 8.0 Hotfix 1153407 *This content update also applies a Host IPS hotfix 1153407 on the client systems running Host IPS 8.0 Patch 5, Patch 6 or Patch 7 only. Successful installation of hotfix displays a different client version depending on which patch version is installed as indicated below:* *- Patch 7: 8.0.0.3800* *- Patch 6: 8.0.0.3500* *- Patch 5: 8.0.0.3250* *Refer below KB for more details on this hotfix.* *https://kc.mcafee.com/corporate/index?page=content&id=KB87658*	*8.0.0*	*Not Applicable*

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 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-11886* - *CVE-2017-11890* - *CVE-2017-11901* - *CVE-2017-11903* - *CVE-2017-11907* - *CVE-2017-11913*	*8.0.0*	*10.2*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-11935*	*8.0.0*	*10.2*

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'