McAfee Exploit Prevention Content 7850

Release Notes | 2017-07-11

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7850

McAfee Endpoint Security Exploit Prevention: 10.5.0.7850

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 6097: *Windows Search Service Remote Code Execution Vulnerability (CVE-2017-8543)* *Description:* - *This event indicates an attempt to exploit Windows Search Service remotely.* - *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 Patch 9*	*Not Applicable*

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 the false positives*	*8.0.0*	*10.1*
Signature 6048: *Suspicious Function Invocation - Different Stack* *Description:* - *The severity level of the Signature has been modified to level High by default*	*8.0.0*	*10.1*

Signature 6087: *Powershell Command Restriction - EncodedCommand* *Description:* - *The Signature has been modified to reduce the false positives*	*8.0.0*	*10.5.0*
Signature 6095: *Windows SMB Remote Code Execution Vulnerability* *Description:* - *The severity level of the Signature has been modified to level High by default*	*8.0.0* *Patch 9*	*Not Applicable*

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, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2017-8594* - *CVE-2017-8618*	*8.0.0*	*10.1*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2017-0243*	*8.0.0*	*10.1*

Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2017-3099* - *CVE-2017-3100*	*8.0.0*	*10.1*
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014, 6015, 6047, 6048 and 6049 are expected to cover the below vulnerabilities:* - *CVE-2017-8601* - *CVE-2017-8605* - *CVE-2017-8617* - *CVE-2017-8619* - *CVE-2017-8598*	*Not Applicable*	*10.5.1*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2017-8577* - *CVE-2017-8578* - *CVE-2017-8580*	*8.0.0*	*10.1*

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'