McAfee Exploit Prevention Content 8190

Release Notes | 2018-01-18

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8190

McAfee Endpoint Security Exploit Prevention: 10.5.0.8190

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 2812**: Disttrack malware infection* *Description:* - *This event indicates an attempt by the disttrack malware to infect the system* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 8.0.0.4634)*	*10.5.3*
***Signature 6108**: Powershell - Suspicious downloadstring script execution* *Description:* - *This event indicates that Windows powershell is used for downloading and executing suspicious script.* - *This signature is set to Low by default* *Note: Customer can change the level of this signature based on their requirement*	*8.0.0*	*10.2.0*
***Signature 6109**: Powershell - Suspicious wmi script execution* *Description:* - *This event indicates that Windows powershell is used for executing suspicious script* - *This signature is set to Low by default* *Note: Customer can change the level of this signature based on their requirement*	*8.0.0*	*10.2.0*

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Signature 2787**: W32/Yunsip Infection* *Description:* - *The Signature has been modified to reduce the false positives*	*8.0.0*	*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, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2018-0762* - *CVE-2018-0772*	*8.0.0*	*10.2.0*
***Coverage by GBOP:** GBOP Signatures 428, 3754, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-0792* - *CVE-2018-0794* - *CVE-2018-0797* - *CVE-2018-0804*	*8.0.0*	*10.2.0*

- *CVE-2018-0805* - *CVE-2018-0806* - *CVE-2018-0807* - *CVE-2018-0812*		
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-0791* - *CVE-2018-0793* - *CVE-2018-0795* - *CVE-2018-0796* - *CVE-2018-0798* - *CVE-2018-0801* - *CVE-2018-0802*	*8.0.0*	*10.2.0*
Coverage by Other Signatures: *IIS Cross-Site Scripting Signature (Signature 940) is expected to cover the below vulnerability:* - *CVE-2018-0789* - *CVE-2018-0790*	*8.0.0*	*Not Applicable*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-0744* - *CVE-2018-0748* - *CVE-2018-0751* - *CVE-2018-0752*	*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'