McAfee Exploit Prevention Content 8231

Release Notes | 2018-02-13

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8231

McAfee Endpoint Security Exploit Prevention: 10.5.0.8231

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 6110**: Fileless Threat: Startup Program Creation* *Description:* - *This event indicates that a new program has been designated to run at startup, or that the startup status of an existing program has been modified by a fileless malware such as Kovter* - *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*	*Not Applicable*
***Signature 6111**: Fileless Threat: Click fraud operation* *Description:* - *This event indicates that a new program has been designated to run at startup, or that the startup status of an existing program has been modified by a fileless malware such as Powelike* - *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*	*Not Applicable*

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*	*8.0.0*	*Not Applicable*

Updated Non-Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Signature 1051**: Linux Agent Shielding - File Mod* *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-2018-0825* - *CVE-2018-4877* - *CVE-2018-4879* - *CVE-2018-4888* - *CVE-2018-4892* - *CVE-2018-4895* - *CVE-2018-4898* - *CVE-2018-4901* - *CVE-2018-4902* - *CVE-2018-4910* - *CVE-2018-4911* - *CVE-2018-4913* - *CVE-2018-4915* - *CVE-2018-4916*	*8.0.0*	*10.2.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-0742* - *CVE-2018-0844* - *CVE-2018-0846*	*8.0.0*	10.2.0
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and Other Signatures like 8001 and 1149 are expected to cover the below vulnerability:* - *CVE-2018-4878*	*8.0.0*	*Not Applicable* (Only GBOP signatures are applicable and are supported from 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'