McAfee Exploit Prevention Content 7927

Release Notes | 2017-08-14

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7927

McAfee Endpoint Security Exploit Prevention: 10.5.0.7927

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 6098**: Windows LNK File Remote Code Execution (CVE-2017-8464)* *Description:* - *This event indicates an attempt to execute remote code using windows LNK file.* - *This signature is Low by default* *Note: Customer can change the level of this signature based on their requirement.*	*8.0.0*	*10.5.1*
***Signature 6099**: Firefox Installer Privilege escalation (CVE-2017-7755)* *Description:* - *This event indicates an attempt to do a privilege escalation using firefox installer.* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement.*	*8.0.0*	*Not Applicable*

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
BugFix: *Exploit Prevention Content's Application Protection List has been modified to include the below processes:* - *ApplicationFrameHost.exe* - *browser_broker.exe*	*Not Applicable*	*10.5.1*
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-2017-8625* - *CVE-2017-8634* - *CVE-2017-8635* - *CVE-2017-8636* - *CVE-2017-8638* - *CVE-2017-8639* - *CVE-2017-8640* - *CVE-2017-8641* - *CVE-2017-8645* - *CVE-2017-8646* - *CVE-2017-8651* - *CVE-2017-8653* - *CVE-2017-8655* - *CVE-2017-8656*	*8.0.0*	*10.1*

- *CVE-2017-8657* - *CVE-2017-8669* - *CVE-2017-8671* - *CVE-2017-8672* - *CVE-2017-8674*		
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014, 6015, 6047, 6048 and 6049 are expected to cover the below vulnerabilities:* - *CVE-2017-0293* - *CVE-2017-8661* - *CVE-2017-8658*	*Not Applicable*	*10.5.1*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2017-8593* - *CVE-2017-8624*	*8.0.0*	*10.1*
Coverage by Other Signatures: *IIS Cross-Site Scripting Signature (Signature 940) is expected to cover the below vulnerability:* - *CVE-2017-8654*	*8.0.0*	*Not Applicable*

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'