McAfee Exploit Prevention Content 8773

Release Notes | 2018-11-16

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8773

McAfee Endpoint Security Exploit Prevention: 10.6.0.8773

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 6124: *Fileless Threat: Spoof Parent Process* *(BZ #1250838)* *Description:* - *This event indicates a fileless attack where a powershell script attempt to spoof the parent of a process. This is a malicious activity and signifies infection.* - *This signature is set to level Low by default* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*
Signature 6125: *Java Remote Shellcode Injection* *(BZ #1250797)* *Description:* - *This event indicates a java program attempt to inject and execute malicious shellcode into another process. This is a malicious activity and signifies infection.* - *This signature is set to level Low by default.* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*

Note: Refer to the KB for the default Reaction-type associated with Signature severity level for all supported Product versions: https://kc.mcafee.com/corporate/index?page=content&id=KB90369

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 413: *Suspicious Double File Extension Execution* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 2812: *Disttrack malware infection* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 2837: *Microsoft Antimalware Client Privilege Escalation Vulnerability* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 2842: *Exploitation using Library load from UNC Path* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 2844: *Microsoft Word WordPerfect5 Converter Module Buffer Overflow Vulnerability* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 6076: *Microsoft Windows media centre MCL Vulnerability* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 6077: *Microsoft Visio DLL Hijacking Vulnerability* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 6088: *Microsoft Office DLL planting vulnerability* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 6089: *Microsoft Office DLL side load vulnerability* *(BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*

Signature 6093: *Microsoft Office OneNote DLL side load vulnerability (BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 6094: *Adobe Acrobat Reader DLL side load vulnerability (BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 6107: *MS Word trying to execute unwanted programs (BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
Signature 6112: *MS Outlook trying to execute unwanted programs (BZ #1247674)* *Description:* - *The Signature has been modified to reduce false positives*	*NA*	*10.5.3*
BugFix: *Host Intrusion Prevention and Endpoint Security Exploit Prevention content signatures have been updated to display the correct vulnerability coverage information in the Signature Description section.* *(BZ #1257528)*	*8.0.0*	*10.2.0*

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-2018-8544* - *CVE-2018-8552* - *CVE-2018-8563*	*8.0.0*	*10.2.0*
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-8522* - *CVE-2018-8524* - *CVE-2018-8539* - *CVE-2018-8570* - *CVE-2018-8573* - *CVE-2018-8574* - *CVE-2018-8577* - *CVE-2018-8576* - *CVE-2018-8582*	*8.0.0*	*10.2.0*

Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-8553* - *CVE-2018-8562* - *CVE-2018-8565* - *CVE-2018-8589*	*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'