McAfee Exploit Prevention Content 8623

Release Notes | 2018-09-11

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8623

McAfee Endpoint Security Exploit Prevention: 10.6.0.8623

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 960: *Msgina.dll File Modified* *Description:* - *This event indicates an attempt to modify or delete the MSGINA.DLL file used for authentication. An attacker would replace this DLL with a Trojan horse version in order to capture user names and passwords from the network. A Trojan horse file is a malicious application, usually intended to allow a remote attacker access to the target system. A Trojan horse file masquerades as a legitimate application or file.* - *This signature is set to level Medium by default* *Note: Customer can change the level / reaction-type of this signature based on their requirement.* *This signature is already available on Host Intrusion Prevention and has been newly added to Endpoint Security Exploit Prevention.*	*8.0.0*	*10.5.3*
Signature 2844: *Microsoft Word WordPerfect5 Converter Module Buffer Overflow Vulnerability* *Description:* - *This event indicates an attempt to exploit a vulnerability exists in Microsoft Word that loads WordPerfect5 converter module which contains multiple buffer overflow vulnerabilities* - *This signature is Disabled by default.* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*8.0.0 (Content: 8.0.0.5221)*	*10.5.3*

This signature is already available on Host Intrusion Prevention and has been newly added to Endpoint Security Exploit Prevention.		
Signature 6120: *Fileless Threat: Process Hollowing* *Description:* - *This event indicates a fileless attack where a powershell script tried to start a process in suspended mode and then execute it after replacing its memory with malicious code.* - *This signature is Low by default.* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.0*
Signature 6121: *Fileless Threat: Shellcode Self Injection* *Description:* - *This event indicates a fileless attack where a powershell script attempt to inject and execute malicious shellcode into the powershell process itself. This is a malicious activity and signifies infection.* - *This signature is Low by default.* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.0*
Signature 6122: *Fileless Threat: Reflective Loading of mimikatz using DotNetToJScript Technique* *Description:* - *This event indicates an attempt to load mimikatz.exe using DotNetToJScript Technique.* - *This signature is Low by default.* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.0*
Signature 6123: *Windows Shell Remote Code Execution Vulnerability (CVE-2018-8414)* *(BZ #1252172)* *Description:* - *A remote code execution vulnerability exists in Windows Shell where the shell does not validate file paths. This signature is applicable on Windows 10 and Windows Server 2016* - *This signature is 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 3809: *Microsoft Outlook VEVENT Vulnerability* *(BZ #1251710)* *Description:* - *The description of this Signature has been modified to include vulnerable product versions.*	*8.0.0*	*10.5.3*

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-2018-8420* - *CVE-2018-8461* - *CVE-2018-8447* - *CVE-2018-8475*	*8.0.0*	*10.2.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-8410*	*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'