McAfee Exploit Prevention Content 8381

Release Notes | 2018-05-08

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8381

McAfee Endpoint Security Exploit Prevention: 10.5.0.8381

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 6113: *Fileless Threat: Reflective Self Injection* *Description:* - *Reflective loading refers to loading a PE from memory rather than from disk. A crafted function/script can reflectively load portable executable without getting registered as a loaded module in the process and hence can perform actions without leaving foot prints. Powershell is one of the most widely used application to execute these crafted scripts. This event indicates a fileless attack where a powershell script tried to inject a portable executable into the powershell process itself.* - *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*	*10.5.0*
Signature 6114: *Fileless Threat: Reflective EXE Self Injection* *Description:* - *Reflective loading refers to loading a PE from memory rather than from disk. A crafted function/script can reflectively load an EXE without getting registered as a loaded module in the process and hence can perform actions without leaving foot prints. Powershell is one of the most widely used application to execute these crafted scripts. This event indicates a fileless attack where a powershell script tried to inject an EXE into the powershell process itself.* - *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*	*10.5.0*

***Signature 6115**: Fileless Threat: Reflective DLL Remote Injection* *Description :* - *Reflective loading refers to loading a PE from memory rather than from disk. A crafted function/script can reflectively load a DLL without getting registered as a loaded module in the process and hence can perform actions without leaving foot prints. Powershell is one of the most widely used application to execute these crafted scripts. This event indicates a fileless attack where a powershell script tried to inject a DLL into a remote process.* - *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*	*10.5.0*
***Signature 6116**: Mimikatz LSASS Suspicious Memory Read* *Description :* - *This event indicates that a powershell script has invoked mimikatz and tried to read LSASS memory to steal password. Some of the Ransomware worms use similar techniques for infection and attack.* - *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*	*10.5.0*
***Signature 6117**: Mimikatz LSASS Suspicious Memory DMP Read* *Description :* - *This event indicates that a powershell script has invoked mimikatz and tried to read LSASS memory dump to steal password. Some of the Ransomware worms use similar techniques for infection and attack.* - *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*	*10.5.0*
***Signature 413**: Suspicious Double File Extension Execution* *Description :* - *This event indicates that a file with two extensions (such as readme.txt. exe) was run. This poses a security risk, because such files are often viruses or Trojan horses. <P>For example, a file might be named "Readme.txt. exe," with the second extension not visible in Windows Explorer because of spaces separating the first and second extension. In this example, a user might think that such a document was a text file and double-click it, thus unintentionally launching the Trojan horse application. <P>In some cases, this event may indicate the execution of the Nimda worm (also called " Concept Virus"). If the string "mem" is in the name of the file with the double extension, then this suggests that the computer is infected by the Nimda worm.* - *This signature is set to level High by default*	*8.0.0 (Content: 2616)*	*10.5.3*

Note: Customer can change the level / reaction-type of this signature based on their requirement.		

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 6079: *Suspicious LSASS Access Detected* *Description:* - *The signature has been deprecated from the content as it is more generic and false prone.* *Note: This signature functionality has been replaced by the below Signatures released along with this content. Customers are requested to change the level / reaction-type of below Signatures based on their requirement.* • *Signature 6116: Mimikatz LSASS Suspicious Memory Read* • *Signature 6117: Mimikatz LSASS Suspicious Memory DMP Read*	*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-2018-0955* - *CVE-2018-8114* - *CVE-2018-8122* - *CVE-2018-8174*	*8.0.0*	*10.2.0*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-8147* - *CVE-2018-8148* - *CVE-2018-8162* - *CVE-2018-8161*	*8.0.0*	*10.2.0*
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:*	*8.0.0*	*10.2.0*

- *CVE-2018-8157* - *CVE-2018-8158*		
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-4944* - *CVE-2018-4946* - *CVE-2018-4947* - *CVE-2018-4948* - *CVE-2018-4950* - *CVE-2018-4952* - *CVE-2018-4954* - *CVE-2018-4958* - *CVE-2018-4959* - *CVE-2018-4961* - *CVE-2018-4965* - *CVE-2018-4966* - *CVE-2018-4967* - *CVE-2018-4968* - *CVE-2018-4971* - *CVE-2018-4974* - *CVE-2018-4977* - *CVE-2018-4978* - *CVE-2018-4980* - *CVE-2018-4982* - *CVE-2018-4983* - *CVE-2018-4984* - *CVE-2018-4988* - *CVE-2018-4989* - *CVE-2018-4990*	*8.0.0*	*10.2.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-8120* - *CVE-2018-8124* - *CVE-2018-8164* - *CVE-2018-8165* - *CVE-2018-8166* - *CVE-2018-8167*	*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'