McAfee Exploit Prevention Content 9329

Release Notes | 2019-06-11

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.9329

McAfee Endpoint Security Exploit Prevention: 10.6.0.9329

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 2601: *IE Envelope - Source Code File Access* *Description:* - *This event indicates an attempt by Internet Explorer to read a source code file type. In most configurations the browser will not directly access files of this type, and such an operation might suggest that the browser is compromised and that an attacker is attempting to read private information from the machine running the browser. This event will trigger each time the browser attempts to open a file whose extension maps to a known source code file format. These extensions include C, C++, assembly, Java, PERL, Python and Pascal source code files. This event will not be triggered if the source code file accessed is located in a directory used for browser operations, such as the windows system directory or the temporary directories used by the browser.* - *This signature is set to level Low by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.* *This signature is supported on the default content version available with Host Intrusion Prevention Product version 8.0.0 and support is being added for the Endpoint Security Exploit Prevention Product*	*8.0.0*	*10.5.3*
Signature 2602: *IE Envelope - Office Document File Access* *Description:* - *This event indicates an attempt by Internet Explorer to access a Microsoft Office file. In most configurations the browser will not*	*8.0.0*	*10.5.3*

directly access these files, and such an operation might suggest that the browser is compromised and that an attacker is attempting to read private information from the machine running the browser. This event will trigger each time the browser attempts to open a file whose extension indicates is a Microsoft Office file. These extensions include Excel documents, Word documents, and PowerPoint presentations.This event will not be triggered if the file accessed is located in a directory used for browser operations, such as the Windows system directory or the temporary directories used by the browser. - *This signature is set to level Low by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.* *This signature is supported on the default content version available with Host Intrusion Prevention Product version 8.0.0 and support is being added for the Endpoint Security Exploit Prevention Product*		
Signature 2603: *IE Envelope - Confidential Office Doc. File Access* *Description:* - *This event indicates an attempt by Internet Explorer to read a Microsoft Office file. In most configurations the browser should not directly access these files, and such an operation might suggest that the browser is compromised and that an attacker is attempting to read private information from the machine running the browser. This event will trigger each time the browser attempts to open a file whose extension indicates is a Microsoft Office file. These extensions include Microsoft Project and Microsoft Access database files. This event will not be triggered if the file accessed is located in a directory used for browser operations, such as the Windows system directory or the temporary directories used by the browser.* - *This signature is set to level Low by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.* *This signature is supported on the default content version available with Host Intrusion Prevention Product version 8.0.0 and support is being added for the Endpoint Security Exploit Prevention Product*	*8.0.0*	*10.5.3*
Signature 2604: *IE Envelope - Crypto File Access* *Description:* - *This event indicates an attempt by Internet Explorer to read a cryptographic secret file such as a PGP private key or Certificate file. In most situation the browser should not directly access these files, and such an operation might suggest that the browser is compromised and that an attacker is attempting to private information from the machine. The event will trigger each time the browser attempts to open a file whose extension indicates is a*	*8.0.0*	*10.5.3*

cryptographic secret file. These extensions include PGP private keys, PGP encrypted files, and certificate files. This event will not be triggered if the cryptographic secret file accessed is located in a directory used for browser operations such as the windows system directory, or the temporary directories used by the browser. - *This signature is set to level Low by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.* *This signature is supported on the default content version available with Host Intrusion Prevention Product version 8.0.0 and support is being added for the Endpoint Security Exploit Prevention Product*		
Signature 6136: *Privilege escalation attempt using schtasks (CVE-2019-1069)* *Description:* - *This event indicates an attempt to gain higher privilege using the legacy path for task scheduler.* - *This signature is Disabled 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 6133: *Evasion Attempt: Suspicious AMSI DLL Creation Detected* *Description:* - *The signature is modified to enhance the protection* - *The signature is modified to reduce the false positives*	*8.0.0*	*10.5.3*
Signature 6134: *Evasion Attempt: Suspicious AMSI DLL Loading Detected* *Description:* - *The signature is modified to reduce the false positives*	*8.0.0*	*10.5.3*

Deprecated Windows Signatures

The following signatures have been deprecated due to the issues reported related to slowness, hang and crash of Windows Powershell under specific usage of Windows Powershell application or under specific environmental conditions.

Note:
These signatures were released as a part of McAfee Exploit Prevention Content 9246 (May 2019 release package)

Signature ID	Signature Name	Signature Deprecation applicability on	
		Host Intrusion Prevention	Endpoint Security Exploit Prevention
8003	*Fileless Threat: Suspicious Powershell Behavior Detected*	*Yes*	*Yes*
8004	*Fileless Threat: Malicious Powershell Behavior Detected*	*Yes*	*Yes*

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-2019-0920* - *CVE-2019-0988* - *CVE-2019-1005* - *CVE-2019-1055*	*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-2019-1034* - *CVE-2019-1035* - *CVE-2019-7845*	*8.0.0*	*10.2.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2019-0960* - *CVE-2019-0968* - *CVE-2019-0977* - *CVE-2019-1009* - *CVE-2019-1010*	*8.0.0*	*10.2.0*

- *CVE-2019-1011* - *CVE-2019-1012* - *CVE-2019-1013* - *CVE-2019-1014* - *CVE-2019-1015* - *CVE-2019-1016* - *CVE-2019-1017* - *CVE-2019-1039* - *CVE-2019-1041* - *CVE-2019-1065* - *CVE-2019-1065*		

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'