McAfee Exploit Prevention Content 9246

Release Notes | 2019-05-14

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.9246

McAfee Endpoint Security Exploit Prevention: 10.6.0.9246

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 6133: *Evasion Attempt: Suspicious AMSI DLL Creation Detected* *Description:* - *This event indicates an attempt to create a copy of malicious AMSI.DLL into user's profile folder. This could lead to protection evasion of Microsoft Anti Malware Interface.* - *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*
Signature 6134: *Evasion Attempt: Suspicious AMSI DLL Loading Detected* *Description:* - *This event indicates an attempt to load amsi.dll from an unexpected location. Amsi.dll is expected to be loaded only by valid applications such as cscript, wscript, PowerShell, office. This could be an attempt to evade protection provided by Microsoft Anti Malware Interface.* - *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*
Signature 6135: *Unmanaged PowerShell Detected* *Description:* - *This event indicates an attempt to launch unmanaged PowerShell. This is usually used by attackers to evade security mechanism applicable to PowerShell.* - *This signature is Disabled by default.*	*8.0.0*	*10.5.3*

Note: Customer can change the level/reaction-type of this signature based on their requirement.		
Signature 8003: *Fileless Threat: Suspicious PowerShell Behavior Detected* *Description:* - *The pre-installed and versatile Windows PowerShell has become one of the most popular choices in cyber criminal's arsenals. Especially for file-less attacks, where no file is written to disk, such PowerShell payloads have become very popular. This event indicates Suspicious activity through PowerShell.* - *This signature is set to level Low by default.* *Note: This Signature is supported on Windows 8, Windows 2012 Server and above platforms.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.0*
Signature 8004: *Fileless Threat: Malicious PowerShell Behavior Detected* *Description:* - *The pre-installed and versatile Windows PowerShell has become one of the most popular choices in cyber criminal's arsenals. Especially for file-less attacks, where no file is written to disk, such PowerShell payloads have become very popular. This event indicates Malicious activity through PowerShell.* - *This signature is set to level Low by default.* *Note: This Signature is supported on Windows 8, Windows 2012 Server and above platforms.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.0*

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 3829: *Sticky Keys File Replacement Backdoor* *Description:* - *The default severity level has been modified to High*	*NA*	*10.5.3*

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
BugFix: Inclusion of New McAfee Certificates *Both Endpoint Security Exploit Prevention Content and Host Intrusion Prevention Content have been modified to support the new McAfee Certificate signer. Trusted application list has been modified to support the new McAfee Certificate Signer.*	*8.0.0*	*10.2.0*

Deprecation Notification

The following signatures have been identified as potential candidates for deprecation as the platforms affected by the corresponding vulnerabilities are out of scope for Endpoint Security product.

Note:
The below listed signatures are already disabled in content and no changes are made to these signatures in this release
The below listed signatures will get deprecated from Endpoint Security Exploit Prevention Content in future releases.
Host Intrusion Prevention will not be affected by this change.

Signature ID	Signature Name	Vulnerability Information	Signature Deprecation applicability on	
			Host Intrusion Prevention	Endpoint Security Exploit Prevention
3762	*IE Source URL NULL Dereference Vulnerability*	*CVE-2006-3427*	*No*	*Yes*
3766	*Windows Server Service Buffer Overflow Vulnerability (1)*	*CVE-2006-3439*	*No*	*Yes*
3776	*Microsoft Internet Explorer Vector Markup Language Vulnerability (2)*	*CVE-2006-4868* *CVE-2007-1749*	*No*	*Yes*
3785	*Microsoft XML Core Services Vulnerability*	*CVE-2006-5745*	*No*	*Yes*
3786	*Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution (2)*	*CVE-2006-4704*	*No*	*Yes*
3791	*Vulnerability in Microsoft Rich Edit and Microsoft MFC*	*CVE-2007-0025*	*No*	*Yes*

		CVE-2007-0026 *CVE-2006-1311*		
3800	*Vulnerability in Windows Media Player Could Allow Remote Code Execution (2)*	*CVE-2006-6134*	*No*	*Yes*
3816	*COM Object Instantiation Memory Corruption Vulnerability (4)*	*CVE-2007-0218*	*No*	*Yes*
3822	*Vulnerability in Windows Shell Could Allow Elevation of Privilege*	*CVE-2007-0211*	*No*	*Yes*
3838	*Windows Animated Cursor Handling vulnerability*	*CVE-2007-0038*	*No*	*Yes*
3843	*Internet Explorer CSS Memory Corruption Vulnerability*	*CVE-2007-0945*	*No*	*Yes*
3877	*Vulnerability in Message Queuing Service Could Allow Remote Code Execution*	*CVE-2007-3039*	*No*	*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-2019-0884* - *CVE-2019-0911* - *CVE-2019-0918*	*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-2019-0885* - *CVE-2019-0953* - *CVE-2019-7140* - *CVE-2019-7141* - *CVE-2019-7142* - *CVE-2019-7143* - *CVE-2019-7144* - *CVE-2019-7145* - *CVE-2019-7759* - *CVE-2019-7760* - *CVE-2019-7761* - *CVE-2019-7762* - *CVE-2019-7763* - *CVE-2019-7764* - *CVE-2019-7765*	*8.0.0*	*10.2.0*

- *CVE-2019-7766* - *CVE-2019-7767* - *CVE-2019-7768* - *CVE-2019-7769* - *CVE-2019-7770* - *CVE-2019-7771* - *CVE-2019-7772* - *CVE-2019-7773* - *CVE-2019-7774* - *CVE-2019-7775* - *CVE-2019-7776* - *CVE-2019-7777* - *CVE-2019-7778* - *CVE-2019-7780* - *CVE-2019-7781* - *CVE-2019-7782* - *CVE-2019-7783* - *CVE-2019-7784* - *CVE-2019-7785* - *CVE-2019-7786* - *CVE-2019-7787* - *CVE-2019-7788* - *CVE-2019-7789* - *CVE-2019-7790* - *CVE-2019-7791* - *CVE-2019-7792* - *CVE-2019-7793* - *CVE-2019-7794* - *CVE-2019-7795* - *CVE-2019-7796* - *CVE-2019-7797* - *CVE-2019-7798* - *CVE-2019-7799* - *CVE-2019-7800* - *CVE-2019-7801* - *CVE-2019-7802* - *CVE-2019-7803* - *CVE-2019-7804* - *CVE-2019-7805* - *CVE-2019-7806* - *CVE-2019-7807* - *CVE-2019-7808* - *CVE-2019-7809* - *CVE-2019-7810* - *CVE-2019-7811* - *CVE-2019-7812* - *CVE-2019-7813* - *CVE-2019-7814* - *CVE-2019-7817*		

- *CVE-2019-7818* - *CVE-2019-7819* - *CVE-2019-7820* - *CVE-2019-7821* - *CVE-2019-7822* - *CVE-2019-7823* - *CVE-2019-7825* - *CVE-2019-7826* - *CVE-2019-7827* - *CVE-2019-7828* - *CVE-2019-7829* - *CVE-2019-7830* - *CVE-2019-7831* - *CVE-2019-7832* - *CVE-2019-7833* - *CVE-2019-7834* - *CVE-2019-7835* - *CVE-2019-7836* - *CVE-2019-7841* - *CVE-2019-7837*		
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2019-0707* - *CVE-2019-0758* - *CVE-2019-0881* - *CVE-2019-0882* - *CVE-2019-0892* - *CVE-2019-0903* - *CVE-2019-0961*	*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'