McAfee Exploit Prevention Content 8966

Release Notes | 2019-02-12

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8966

McAfee Endpoint Security Exploit Prevention: 10.6.0.8966

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 2226: *Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution* *Description:* - *This event indicates an attempt to exploit a vulnerability in Microsoft Office Publisher that could allow remote code execution* - *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 2720: *Outlook Envelope - Windows Executable Mod.* *Description:* - *This event indicates an attempt by the Outlook mail client to modify windows system executables. In most configurations Outlook will not modify system executables directly, and an attempt to do so might suggest that Outlook is compromised and that an attacker is attempting to use Outlook to further compromise the machine. This event will trigger each time Outlook attempts to modify an executable in the %SystemRoot% or %SystemRoot%\system32 directories.* - *This signature is set to level Medium by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*
Signature 2721: *Outlook Envelope - Abnormal Executable Mod.* *Description:* - *This event indicates an attempt by the Outlook mail client to modify system executables. In most configurations Outlook will not modify*	*8.0.0*	*10.5.3*

system executables directly, and an attempt to do so might suggest that Outlook is compromised and that an attacker is attempting to use Outlook to further compromise the machine. This event will trigger each time Outlook attempts to modify an executable in the system root drive, temp directories or the special system directory used to cache downloaded Active-X components (%SystemRoot%\Downloaded Program Files) - *This signature is set to level Medium by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*		
Signature 2760: *Outlook Envelope - HTML Application Execution* *Description:* - *This event indicates an attempt to execute an HTML application. HTML applications can have the same features that normal HTML pages do, but run with full user permissions and can perform any operation the user is allowed. Most web sites do not use this functionality and therefore restricting this functionality should not reduce the Outlook user's experience. On the other hand, attackers commonly attempt to use this capability to execute their malicious code with greater privileges. Running an HTML application allows an attacker to act as the user, including accessing any files or application to which the user has permissions. This event will trigger each time Outlook attempts to access a files with the HTML application file extension. Additionally, this event will trigger if Outlook attempts to execute the HTML application run time process.* - *This signature is set to level Medium by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*
Signature 2761: *Outlook Envelope - Suspicious Executable Mod.* *Description:* - *This event indicates an attempt by the Outlook mail client to modify an executable. In most configurations Outlook should not modify executables directly, and such an operation might suggest that Outlook has been compromised and the attacker is attempting to use it to further compromise the machine. This event will trigger each time Outlook attempts to modify an executable that belongs to a set of executables (such as notepad.exe or wmplayer.exe) commonly executed by Internet Explorer. Successfully modifying these files can provide an easy way for an attacker to load and execute their malicious code on a target system.* - *This signature is set to level Medium by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*

Signature 2762: *Outlook Envelope - Compiled Help File Execution* *Description:* - *This event indicates an attempt by the Outlook mail client to execute a compiled help (.CHM) file. Compiled help files have the capability to execute arbitrary applications and therefore could be used maliciously by an attacker in order to execute their code with full user privileges. Most web sites do not use compiled help files and therefore blocking processing of these files should not reduce the user's browsing experience. This event will trigger each time Outlook attempts to access a file with the compiled help file extension. Additionally, this event will trigger if Outlook attempts to execute the compiled help files run time process.* - *This signature is set to level Medium by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*
Signature 2763: *Outlook Envelope - NTVDM Execution* *Description:* - *This event indicates an attempt by the Outlook mail client to execute the NT virtual DOS machine (NTVDM). The NTVDM can be used to execute older MS-DOS executables under the windows operating system. Modern application do not require support for this executable format. An attacker may have malicious code available in this format, so disabling this capability can render many attack tools useless. This event will trigger each time Outlook attempts to execute the NTVDM run time process.* - *This signature is set to level Medium by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*
Signature 2785: *Windows Power Point Insecure DLL loading Vulnerability* *Description:* - *This event indicates an attempt to exploit a vulnerability exists in Microsoft Power Point that loads malicious DLLs.* - *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=KB67561

Updated Windows Signatures	**Minimum Supported Product version**	
	Host Intrusion Prevention	**Endpoint Security Exploit Prevention**

Signature 344: *New Startup Program Creation* *Description:* - *The Signature has been modified to reduce false positives.*	*Not Applicable*	*10.5.3*
Signature 3829: *Sticky Keys File Replacement Backdoor* *(BZ #1265155)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*Not Applicable*
Signature 6070: *Hidden Powershell Detected* *(BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6073: *Execution Policy Bypass in Powershell* *(BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6081: *Powershell Command Restriction – NoProfile* *(BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6082: *Powershell Command Restriction - ExecutionPolicy Unrestricted* *(BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6083: *Powershell Command Restriction – NonInteractive* *(BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6084: *Powershell Command Restriction – NoLogo* *(BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6085: *Powershell Command Restriction – File* *(BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6086: *Powershell Command Restriction – Command* *(BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*

Signature 6087: *Powershell Command Restriction – EncodedCommand (BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6096: *Powershell Command Restriction – InvokeExpression (BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6108: *Powershell - Suspicious downloadstring script execution (BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*8.0.0*	*10.2.0*
Signature 6109: *Powershell - Suspicious wmi script execution (BZ #1227530)* *Description:* - *The Signature has been modified to reduce false positives.*	*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, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2019-0669* - *CVE-2019-0684*	*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-2019-7018* - *CVE-2019-7025* - *CVE-2019-7026* - *CVE-2019-7029* - *CVE-2019-7031* - *CVE-2019-7040* - *CVE-2019-7043* - *CVE-2019-7044* - *CVE-2019-7048* - *CVE-2019-7050* - *CVE-2019-7062* - *CVE-2019-7068* - *CVE-2019-7070*	*8.0.0*	*10.2.0*

- *CVE-2019-7072* - *CVE-2019-7075* - *CVE-2019-7077* - *CVE-2019-7078* - *CVE-2019-7080* - *CVE-2019-7082* - *CVE-2019-7083* - *CVE-2019-7084*		
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-0742* - *CVE-2019-0602* - *CVE-2019-0615* - *CVE-2019-0616* - *CVE-2019-0618* - *CVE-2019-0619* - *CVE-2019-0621* - *CVE-2019-0623* - *CVE-2019-0628* - *CVE-2019-0656* - *CVE-2019-0661*	*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'