McAfee Exploit Prevention Content 8137

Release Notes | 2017-11-14

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8137

McAfee Endpoint Security Exploit Prevention: 10.5.0.8137

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 6100**: SMBLoris attack detected* *Description:* - *This event indicates an attempt to do a SmbLoris attack* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement.*	*8.0.0 Patch 9*	*10.5.3*
***Signature 1157**: USB Storage Device Inserted* *Description:* - *This event indicates that a USB jumpdrive or other USB storage device was inserted* - *This signature is Low by default* *Note: This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 5.0.0.1)*	*10.5.3*
***Signature 6088**: Microsoft Office DLL planting vulnerability* *Description:* - *This event indicates an attempt to exploit a vulnerability that exist in Microsoft Office which loads a malicious DLL* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 8.0.0.7510)*	*10.5.3*
***Signature 6089**: Microsoft Office DLL side load vulnerability* *Description:* - *This event indicates an attempt to exploit a vulnerability that exist in Microsoft Office which loads a malicious DLL.* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 8.0.0.7616)*	*10.5.3*

***Signature 6093**: Microsoft Office OneNote DLL side load vulnerability* *Description:* - *This event indicates an attempt to exploit a vulnerability that exist in Microsoft Office OneNote which loads a malicious DLL* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 8.0.0.7767)*	*10.5.3*
***Signature 6094**: Adobe Acrobat Reader DLL side load vulnerability* *Description:* - *This event indicates an attempt to exploit a vulnerability that exist in Adobe Acrobat Reader which loads a malicious DLL* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 8.0.0.7767)*	*10.5.3*
***Signature 2856**: Microsoft Office Remote Code Execution* *Description:* - *This event indicates that, a remote code execution attack was attempted against the system through a vulnerability in MS Word CVE-2015-0097* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 8.0.0.6331)*	*10.5.3*
***Signature 6076**: Microsoft Windows media centre MCL Vulnerability* *Description:* - *This event indicates an attempt to exploit Microsoft Windows media centre MCL Vulnerability* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 8.0.0.7245)*	*10.5.3*
***Signature 6077**: Microsoft Visio DLL Hijacking Vulnerability* *Description:* - *This event indicates an attempt to exploit a vulnerability in Visio 2016 which leads to DLL Hijacking* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 8.0.0.7304)*	*10.5.3*
***Signature 3821**: Vulnerability in Microsoft Word Macro Security* *Description:* - *This event indicates that Microsoft Word tried to open a file with the extension 'docm'* - *This signature is Medium by default* *Note: This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 6.0.0.877)*	*10.5.3*
***Signature 3809**: Microsoft Outlook VEVENT Vulnerability* *Description:* - *This event indicates an attempt to open a .iCal Meeting request file.* - *This signature is Medium by default* *Note: This change is applicable only for Endpoint Security Exploit Prevention*	*8.0.0 (Content: 6.0.0.826)*	*10.5.3*

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Signature 2787**: W32/Yunsip Infection* *Description:* - *The Signature has been modified to reduce the false positives*	*8.0.0*	*Not Applicable*
***Signature 6079**: Suspicious LSASS Access Detected* *Description:* - *The Signature has been modified to enhance the protection.*	*8.0.0*	*10.5.0*

Updated Non-Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Signature 1051**: Linux Agent Shielding - File Mod* *Description:* - *Two new instances of the Signature have been added to enhance the protection.* - *Two existing obsolete instances of the Signature have been removed.*	*8.0.0*	*Not Applicable*

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***BugFix**: Exploit Prevention Content's Application Protection List has been modified to include the below processes:* *- CoolReader.exe* *- CoolPDFReader.exe*	*8.0.0*	*10.2*
Inclusion of Host IPS 8.0 Hotfix 1153407 *This content update also applies a Host IPS hotfix 1153407 on the client systems running Host IPS 8.0 Patch 5, Patch 6 or Patch 7 only. Successful installation of hotfix displays a different client version depending on which patch version is installed as indicated below:* *- Patch 7: 8.0.0.3800* *- Patch 6: 8.0.0.3500* *- Patch 5: 8.0.0.3250* *Refer below KB for more details on this hotfix.* *https://kc.mcafee.com/corporate/index?page=content&id=KB87658*	*8.0.0*	*Not Applicable*

Existing coverage for New Vulnerabilities	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2017-11856* - *CVE-2017-11869*	*8.0.0*	*10.2*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2017-11878*	*8.0.0*	*10.2*
Coverage by GBOP: *GBOP Signatures 428, 3754, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2017-11854*	*8.0.0*	*10.2*
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014, 6047, 6048 and 6049 are expected to cover the below vulnerabilities:* - *CVE-2017-11215* - *CVE-2017-11225* - *CVE-2017-16360* - *CVE-2017-16368* - *CVE-2017-16379* - *CVE-2017-16381* - *CVE-2017-16383* - *CVE-2017-16385* - *CVE-2017-16388* - *CVE-2017-16389* - *CVE-2017-16390* - *CVE-2017-16391* - *CVE-2017-16392* - *CVE-2017-16393* - *CVE-2017-16395* - *CVE-2017-16396* - *CVE-2017-16398* - *CVE-2017-16404* - *CVE-2017-16407*	*8.0.0*	*10.2*

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'