McAfee Exploit Prevention Content 7510

Release Notes | 2017-01-10

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7510

Endpoint Security Exploit Prevention: 10.5.0.7510

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 6088**: Microsoft Office DLL planting vulnerability (CVE-2016-7275)* *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.*	*8.0.0*	*Not Applicable*

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Signature 907**: PWDump Tool Activation* *Description:* - *Incorrect CVE info has been removed from the Signature description*	*8.0.0*	*Not Applicable*
***Signature 1148**: CMD Tool Access by a Network Aware Application* *Description:*	*8.0.0*	*Not Applicable*

- *Due to generic nature of the signature resulting in large number of triggers, default severity level of this signature has been modified from Informational to Disabled* *Note: Customer can change the level of this signature based on their requirement.*		
***Signature 6013**: Suspicious Function Invocation - CALL Not Found* *Description:* - *This signature has been modified to reduce the false positives*	*8.0.0*	*10.1*
***Signature 6015**: Suspicious Function Invocation - Target Address Mismatch* *Description:* - *This signature has been modified to reduce the false positives*	*8.0.0*	*10.5*
***Signature 6060**: PDF Sandbox Escape Malicious CopyFile* *Description:* - *This signature has been modified to improve coverage*	*8.0.0*	*10.5*
***Signature 6075**: Remote script execution by core windows utility* *Description:* - *64 bit support has been added for this signature*	*8.0.0*	*10.5*
***Enhancement:** Buffer Overflow protection enhancement* *Description:* - *Buffer Overflow signatures have been modified to enhance the protection* - *This update is applicable for all Buffer Overflow class signatures*	*8.0.0*	*10.1*

Other Changes

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

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 and 6014 are expected to cover the below vulnerability:* - *CVE-2017-0003*	*8.0.0*	*10.1*

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'