McAfee Exploit Prevention Content 7796

Release Notes | 2017-06-15

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7796

McAfee Endpoint Security Exploit Prevention: 10.5.0.7796

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 6096**: Powershell Command Restriction - InvokeExpression* *Description:* - *This event indicates an attempt to execute powershell with InvokeExpression parameter.* - *This signature is Disabled by default* *Note: Customer can change the level of this signature based on their requirement.*	*8.0.0*	*10.5.1*

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
***Signature 6048**: Suspicious Function Invocation - Different Stack* *Description :* - *This signature has been modified to support all 32-bit processes* - *Signature Description has been modified to remove the specific processes coverage information as it provides generic protection*	*8.0.0 (McAfee Host Intrusion Prevention Content: 8.0.0.7767)*	*10.1*

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
BugFix: *Endpoint Security Exploit prevention content has been modified to provide GBOP coverage for 32-bit Microsoft Edge browser.* *The affected Signatures are:* *428 - Generic Buffer Overflow* *6012 - Suspicious Function Invocation - Return to API* *6013 - Suspicious Function Invocation - CALL Not Found* *6014 - Suspicious Function Invocation - Return Address Not Readable* *6015 - Suspicious Function Invocation - Target Address Mismatch* *6047 - Illegal Execution - Writable Memory* *6048 - Suspicious Function Invocation - Different Stack* *6049 - Suspicious Function Invocation - No Module*	*Not Applicable*	*10.5.1*
BugFix: *Exploit Prevention Content's Application Protection List has been modified to include the below processes:* - *MicrosoftEdge.exe* - *MicrosoftEdgeCP.exe* - *RuntimeBroker.exe*	*Not Applicable*	*10.5.1*
BugFix*: SQL injection support has been added for the below Microsoft SQL server versions* - *2014.120.5000.0, 32 bit* - *2014.120.5000.0, 64 bit*	*8.0.0*	*Not Applicable*
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, 1146, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-0291* - *CVE-2017-0292* - *CVE-2017-8517* - *CVE-2017-8519* - *CVE-2017-8522* - *CVE-2017-8524* - *CVE-2017-8547* - *CVE-2017-8548* - *CVE-2017-8549*	*8.0.0*	*10.1*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-8506* - *CVE-2017-8507* - *CVE-2017-8509* - *CVE-2017-8510* - *CVE-2017-8511* - *CVE-2017-8512*	*8.0.0*	*10.1*
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:* - *CVE-2017-0283* - *CVE-2017-0294* - *CVE-2017-8513* - *CVE-2017-8528* - *CVE-2017-3075* - *CVE-2017-3076* - *CVE-2017-3077* - *CVE-2017-3078* - *CVE-2017-3079* - *CVE-2017-3081* - *CVE-2017-3082* - *CVE-2017-3083* - *CVE-2017-3084*	*8.0.0*	*10.1*

Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014, 6015, 6047, 6048 and 6049 are expected to cover the below vulnerabilities:* - *CVE-2017-8496* - *CVE-2017-8497* - *CVE-2017-8499* - *CVE-2017-8520* - *CVE-2017-8521*	*Not Applicable*	*10.5.1*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2017-0296* - *CVE-2017-0297* - *CVE-2017-8465* - *CVE-2017-8466* - *CVE-2017-8468* - *CVE-2017-8494*	*8.0.0*	*10.1*
Coverage by Other Signatures: *IIS Cross-Site Scripting Signature (Signature 940) is expected to cover the below vulnerability:* - *CVE-2017-8514* - *CVE-2017-8551*	*8.0.0*	*Not Applicable*

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'