



McAfee Exploit Prevention Content 8008

Release Notes | 2017-09-12

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8008

McAfee Endpoint Security Exploit Prevention: 10.5.0.8008

Below is the updated signature information for the McAfee Exploit Prevention content.

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
<p>Signature 6087: Powershell Command Restriction - EncodedCommand (BZ# 1204966)</p> <p>Description:</p> <ul style="list-style-type: none"> - The Signature has been modified to enhance the protection 	8.0.0	10.5.0
<p>Signature 8000: Behavior Based Exploit Protection</p> <p>Description:</p> <ul style="list-style-type: none"> - The severity level of the Signature has been modified to level Low by default <p>Note: Customer can change the level of this signature based on their requirement</p>	8.0.0	Not Applicable
<p>Signature 6098: Windows LNK File Remote Code Execution (BZ# 1208004)</p> <p>Description:</p> <ul style="list-style-type: none"> - The Signature has been modified to reduce the false positives 	8.0.0	10.5.0

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention

<p>Inclusion of Host IPS 8.0 Hotfix 1153407</p> <p>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:</p> <ul style="list-style-type: none"> - Patch 7: 8.0.0.3800 - Patch 6: 8.0.0.3500 - Patch 5: 8.0.0.3250 <p>Refer below KB for more details on this hotfix. https://kc.mcafee.com/corporate/index?page=content&id=KB87658</p>	8.0.0	Not Applicable
---	-------	----------------

Existing coverage for New Vulnerabilities	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
<p>Coverage by GBOP: GBOP Signatures 428, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none"> - CVE-2017-11281 - CVE-2017-11282 	8.0.0	10.1
<p>Coverage by GPEP: Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none"> - CVE-2017-8682 	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'