



McAfee Exploit Prevention Content 7691

Release Notes | 2017-04-11

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7691

Endpoint Security Exploit Prevention: 10.5.0.7691

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 6090 : Self Protection - Double Agent Description : <ul style="list-style-type: none">- This event indicates double agent attack attempt to bypass self-protection.- This signature is set to level High by default	8.0.0	Not Applicable
Signature 6091 : IMFEO registry protection Description: <ul style="list-style-type: none">- This event indicates that an attempt was made to modify Image File Execution Options registry key by a non-trusted process.- This signature is set to level High by default	8.0.0	Not Applicable

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
<p>Coverage by GBOP: GBOP Signatures 428, 1146, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none">- CVE-2017-0158- CVE-2017-0201- CVE-2017-0202 <p>Coverage by GBOP: GBOP Signatures 428, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none">- CVE-2017-0194 <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-2017-0166- CVE-2017-0192 <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-2017-0156	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'