



McAfee Exploit Prevention Content 8190

Release Notes | 2018-01-18

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8190

McAfee Endpoint Security Exploit Prevention: 10.5.0.8190

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
<p>Signature 2812: <i>Distrack malware infection</i></p> <p><i>Description:</i></p> <ul style="list-style-type: none"> - This event indicates an attempt by the distrack malware to infect the system - This signature is Disabled by default <p><i>Note:</i> Customer can change the level of this signature based on their requirement. This change is applicable only for Endpoint Security Exploit Prevention</p>	8.0.0 (Content: 8.0.0.4634)	10.5.3
<p>Signature 6108: <i>Powershell - Suspicious downloadstring script execution</i></p> <p><i>Description:</i></p> <ul style="list-style-type: none"> - This event indicates that Windows powershell is used for downloading and executing suspicious script. - This signature is set to Low by default <p><i>Note:</i> Customer can change the level of this signature based on their requirement</p>	8.0.0	10.2.0
<p>Signature 6109: <i>Powershell - Suspicious wmi script execution</i></p> <p><i>Description:</i></p> <ul style="list-style-type: none"> - This event indicates that Windows powershell is used for executing suspicious script - This signature is set to Low by default <p><i>Note:</i> Customer can change the level of this signature based on their requirement</p>	8.0.0	10.2.0

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
<p>Signature 2787: W32/Yunsip Infection</p> <p>Description:</p> <ul style="list-style-type: none"> - The Signature has been modified to reduce the false positives 	8.0.0	Not Applicable

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.</p> <p>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-2018-0762 - CVE-2018-0772 	8.0.0	10.2.0
<p>Coverage by GBOP: GBOP Signatures 428, 3754, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none"> - CVE-2018-0792 - CVE-2018-0794 - CVE-2018-0797 - CVE-2018-0804 	8.0.0	10.2.0

