



## McAfee Exploit Prevention Content 8841

### Release Notes | 2019-01-08

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8841

McAfee Endpoint Security Exploit Prevention: 10.6.0.8841

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><b>Signature 2816:</b> Windows Live Mail dwmapi DLL Hijacking Vulnerability</p> <p><i>Description:</i></p> <ul style="list-style-type: none"> <li>- This event indicates an attempt to exploit a vulnerability that exists in Windows Live Mail which loads malicious DLLs.</li> </ul> <p><i>Note:</i> Customer can change the level/reaction-type of this signature based on their requirement.</p>	8.0.0 (Content: 8.0.0.4587)	10.5.3

**Note:** Refer to the KB for the default Reaction-type associated with Signature severity level for all supported Product versions: <https://kc.mcafee.com/corporate/index?page=content&id=KB67561>

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
<p><b>Signature 6091:</b> IMFEO registry protection (BZ #1261506)</p> <p><i>Description:</i></p> <ul style="list-style-type: none"> <li>- The Signature has been modified to reduce false positives.</li> </ul> <p><i>Note:</i> Customer can change the level/reaction-type of this signature based on their requirement.</p>	8.0.0	NA
<p><b>BugFix:</b> Minimum supported content version is corrected for all Endpoint Security Exploit Prevention signatures.</p>	NA	10.2.0

Existing coverage for New Vulnerabilities	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
<p><b>Coverage by GBOP:</b> GBOP Signatures 428, 1146, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerability:</p> <ul style="list-style-type: none"> <li>- CVE-2019-0541</li> </ul>	8.0.0	10.2.0
<p><b>Coverage by GBOP:</b> GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerability:</p> <ul style="list-style-type: none"> <li>- CVE-2019-0585</li> </ul>	8.0.0	10.2.0

## 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'