



## McAfee Exploit Prevention Content 7510

### Release Notes | 2017-01-10

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7510

Endpoint Security Exploit Prevention: 10.5.0.7510

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 6088:</b> Microsoft Office DLL planting vulnerability (CVE-2016-7275)</p> <p>Description:</p> <ul style="list-style-type: none"> <li>- This event indicates an attempt to exploit a vulnerability that exist in Microsoft Office which loads a malicious DLL</li> <li>- This signature is Disabled by default</li> </ul> <p>Note: Customer can change the level of this signature based on their requirement.</p>	8.0.0	Not Applicable

---

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
<p><b>Signature 907:</b> PWDump Tool Activation</p> <p>Description:</p> <ul style="list-style-type: none"> <li>- Incorrect CVE info has been removed from the Signature description</li> </ul>	8.0.0	Not Applicable
<p><b>Signature 1148:</b> CMD Tool Access by a Network Aware Application</p> <p>Description:</p>	8.0.0	Not Applicable

<ul style="list-style-type: none"> <li>- Due to generic nature of the signature resulting in large number of triggers, default severity level of this signature has been modified from Informational to Disabled</li> </ul> <p>Note: Customer can change the level of this signature based on their requirement.</p>		
<p><b>Signature 6013:</b> Suspicious Function Invocation - CALL Not Found</p> <p>Description:</p> <ul style="list-style-type: none"> <li>- This signature has been modified to reduce the false positives</li> </ul>	8.0.0	10.1
<p><b>Signature 6015:</b> Suspicious Function Invocation - Target Address Mismatch</p> <p>Description:</p> <ul style="list-style-type: none"> <li>- This signature has been modified to reduce the false positives</li> </ul>	8.0.0	10.5
<p><b>Signature 6060:</b> PDF Sandbox Escape Malicious CopyFile</p> <p>Description:</p> <ul style="list-style-type: none"> <li>- This signature has been modified to improve coverage</li> </ul>	8.0.0	10.5
<p><b>Signature 6075:</b> Remote script execution by core windows utility</p> <p>Description:</p> <ul style="list-style-type: none"> <li>- 64 bit support has been added for this signature</li> </ul>	8.0.0	10.5
<p><b>Enhancement:</b> Buffer Overflow protection enhancement</p> <p>Description:</p> <ul style="list-style-type: none"> <li>- Buffer Overflow signatures have been modified to enhance the protection</li> <li>- This update is applicable for all Buffer Overflow class signatures</li> </ul>	8.0.0	10.1

---

## 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><b>Coverage by GBOP:</b> GBOP Signatures 428, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerability:</p> <ul style="list-style-type: none"> <li>- CVE-2017-0003</li> </ul>	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'