# McAfee Exploit Prevention Content 7796

# Release Notes | 2017-06-15

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.7796

McAfee Endpoint Security Exploit Prevention: 10.5.0.7796

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 6096**: Powershell Command Restriction - InvokeExpression*<br>*Description:*<br>- *This event indicates an attempt to execute powershell with InvokeExpression parameter.*<br>- *This signature is Disabled by default*<br>*Note: Customer can change the level of this signature based on their requirement.* | *8.0.0* | *10.5.1* |

| Updated Windows Signatures | Minimum Supported Product version | |
|---|---|---|
| | Host Intrusion Prevention | Endpoint Security Exploit Prevention |
| ***Signature 6048**: Suspicious Function Invocation - Different Stack*<br>*Description :*<br>- *This signature has been modified to support all 32-bit processes*<br>- *Signature Description has been modified to remove the specific processes coverage information as it provides generic protection* | *8.0.0 (McAfee Host Intrusion Prevention Content: 8.0.0.7767)* | *10.1* |

| Other Changes | Minimum Supported Product version | |
|---|---|---|
| | Host Intrusion Prevention | Endpoint Security Exploit Prevention |
| ***BugFix:*** *Endpoint Security Exploit prevention content has been modified to provide GBOP coverage for 32-bit Microsoft Edge browser.*<br><br>*The affected Signatures are:*<br>*428 - Generic Buffer Overflow*<br>*6012 - Suspicious Function Invocation - Return to API*<br>*6013 - Suspicious Function Invocation - CALL Not Found*<br>*6014 - Suspicious Function Invocation - Return Address Not Readable*<br>*6015 - Suspicious Function Invocation - Target Address Mismatch*<br>*6047 - Illegal Execution - Writable Memory*<br>*6048 - Suspicious Function Invocation - Different Stack*<br>*6049 - Suspicious Function Invocation - No Module* | *Not Applicable* | *10.5.1* |
| ***BugFix:*** *Exploit Prevention Content's Application Protection List has been modified to include the below processes:*<br>- *MicrosoftEdge.exe*<br>- *MicrosoftEdgeCP.exe*<br>- *RuntimeBroker.exe* | *Not Applicable* | *10.5.1* |
| ***BugFix****: SQL injection support has been added for the below Microsoft SQL server versions*<br>- *2014.120.5000.0, 32 bit*<br>- *2014.120.5000.0, 64 bit* | *8.0.0* | *Not Applicable* |
| ***Inclusion of Host IPS 8.0 Hotfix 1153407***<br>*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:*<br>*- Patch 7: 8.0.0.3800*<br>*- Patch 6: 8.0.0.3500*<br>*- Patch 5: 8.0.0.3250*<br><br>*Refer below KB for more details on this hotfix.*<br>*https://kc.mcafee.com/corporate/index?page=content&id=KB87658* | *8.0.0* | *Not Applicable* |

| Existing coverage for New Vulnerabilities | Minimum Supported Product version | |
|---|---|---|
| | Host Intrusion Prevention | Endpoint Security Exploit Prevention |
| ***Coverage by GBOP:*** *GBOP Signatures 428, 1146, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:*<br>- *CVE-2017-0291*<br>- *CVE-2017-0292*<br>- *CVE-2017-8517*<br>- *CVE-2017-8519*<br>- *CVE-2017-8522*<br>- *CVE-2017-8524*<br>- *CVE-2017-8547*<br>- *CVE-2017-8548*<br>- *CVE-2017-8549* | *8.0.0* | *10.1* |
| ***Coverage by GBOP:*** *GBOP Signatures 428, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:*<br>- *CVE-2017-8506*<br>- *CVE-2017-8507*<br>- *CVE-2017-8509*<br>- *CVE-2017-8510*<br>- *CVE-2017-8511*<br>- *CVE-2017-8512* | *8.0.0* | *10.1* |
| ***Coverage by GBOP:*** *GBOP Signatures 428, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:*<br>- *CVE-2017-0283*<br>- *CVE-2017-0294*<br>- *CVE-2017-8513*<br>- *CVE-2017-8528*<br>- *CVE-2017-3075*<br>- *CVE-2017-3076*<br>- *CVE-2017-3077*<br>- *CVE-2017-3078*<br>- *CVE-2017-3079*<br>- *CVE-2017-3081*<br>- *CVE-2017-3082*<br>- *CVE-2017-3083*<br>- *CVE-2017-3084* | *8.0.0* | *10.1* |

| | | |
|---|---|---|
| ***Coverage by GBOP:*** *GBOP Signatures 428, 6012, 6013, 6014, 6015, 6047, 6048 and 6049 are expected to cover the below vulnerabilities:*<br>- *CVE-2017-8496*<br>- *CVE-2017-8497*<br>- *CVE-2017-8499*<br>- *CVE-2017-8520*<br>- *CVE-2017-8521* | *Not Applicable* | *10.5.1* |
| ***Coverage by GPEP:*** *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:*<br>- *CVE-2017-0296*<br>- *CVE-2017-0297*<br>- *CVE-2017-8465*<br>- *CVE-2017-8466*<br>- *CVE-2017-8468*<br>- *CVE-2017-8494* | *8.0.0* | *10.1* |
| ***Coverage by Other Signatures:***<br>*IIS Cross-Site Scripting Signature (Signature 940) is expected to cover the below vulnerability:*<br>- *CVE-2017-8514*<br>- *CVE-2017-8551* | *8.0.0* | *Not Applicable* |

## 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'