# McAfee Exploit Prevention Content 9418

## Release Notes | 2019-07-09

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.9418

McAfee Endpoint Security Exploit Prevention: 10.6.0.9418

**Note:** McAfee V3 Virus Definition Updates (DATs) version 3668 or above is a mandatory pre-requisite for this Exploit prevention content update on McAfee Endpoint Security versions 10.5.2, 10.5.5 and 10.6.0.
Refer to the below KB for more information:
https://kc.mcafee.com/corporate/index?page=content&id=KB91649

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 2660:*** *IE Envelope – HTML Application Execution*<br>*Description:*<br>- *This event indicates an attempt to execute an HTML application. HTML applications can have the same features that normal HTML pages can, but they run with full user permissions and can execute any operation the user is allowed. Most web sites do not use HTML application functionality and therefore restricting this functionality should not reduce the user's browsing experience. On the other hand, attackers often attempt to use functionality in order to execute malicious code with fewer restrictions. Running an HTML application allows an attacker to access all files, as well as execute any application available to the user. This event will trigger each time the browser attempts to access a file with the HTML application file extension or attempts to execute the HTML application run time process.*<br>- *This signature is set to level Medium by default.*<br>*Note: Customer can change the level/reaction-type of this signature based on their requirement.*<br>*This signature is supported on the default content version available with Host Intrusion Prevention Product version 8.0.0 and support is being added for the Endpoint Security Exploit Prevention Product* | *8.0.0* | *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=KB90369

| Updated Windows Signatures | Minimum Supported Product version | |
|---|---|---|
| | Host Intrusion Prevention | Endpoint Security Exploit Prevention |
| ***Signature 6070:*** *Hidden Powershell Detected*<br>*Description:*<br>- *The signature is modified to reduce the false positives* | *NA* | *10.5.3* |
| ***Signature 6073:*** *Execution Policy Bypass in Powershell*<br>*Description:*<br>- *The signature is modified to reduce the false positives* | *NA* | *10.5.3* |
| ***Signature 6081:*** *Powershell Command Restriction - NoProfile*<br>*Description:*<br>- *The signature is modified to reduce the false positives* | *NA* | *10.5.3* |
| ***Signature 6082:*** *Powershell Command Restriction - ExecutionPolicy Unrestricted*<br>*Description:*<br>- *The signature is modified to reduce the false positives* | *NA* | *10.5.3* |
| ***Signature 6087:*** *PowerShell Command Restriction – EncodedCommand*<br>*Description:*<br>- *The signature is modified to enhance the protection* | *8.0.0* | *10.5.3* |
| ***Signature 6135:*** *Unmanaged PowerShell Detected*<br>*Description:*<br>- *The signature is modified to reduce the false positives* | *8.0.0* | *10.5.3* |

| Other Changes | Minimum Supported Product version | |
|---|---|---|
| | Host Intrusion Prevention | Endpoint Security Exploit Prevention |
| ***BugFix:*** *McAfee Host Intrusion Prevention content and Endpoint Security Exploit Prevention content packages are signed with new McAfee certificates*<br>*Refer to the below KB for more information:*<br>*https://kc.mcafee.com/corporate/index?page=content&id=KB91649* | *8.0.0* | *10.5.0* |

| 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, 6014 and 6048 are expected to cover the below vulnerabilities:*<br>- *CVE-2019-1056*<br>- *CVE-2019-1063* | *8.0.0* | *10.5.0* |
| ***Coverage by GBOP:*** *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:*<br>- *CVE-2019-1110*<br>- *CVE-2019-1111*<br>- *CVE-2019-1112* | *8.0.0* | *10.5.0* |
| ***Coverage by GPEP:*** *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:*<br>- *CVE-2019-1067*<br>- *CVE-2019-1071*<br>- *CVE-2019-1073*<br>- *CVE-2019-1094*<br>- *CVE-2019-1095*<br>- *CVE-2019-1096*<br>- *CVE-2019-1098*<br>- *CVE-2019-1099*<br>- *CVE-2019-1100*<br>- *CVE-2019-1101*<br>- *CVE-2019-1102*<br>- *CVE-2019-1132* | *8.0.0* | *10.5.0* |

## 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'