# McAfee Exploit Prevention Content 8701

## Release Notes | 2018-10-09

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8701

McAfee Endpoint Security Exploit Prevention: 10.6.0.8701

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 344:*** *New Startup Program Creation*<br>*Description:*<br>- *This event indicates that a new program has been designated to run at startup, or that the startup status of an existing program has been modified.*<br>- *This signature is set to level Low by default*<br><br>*Note: Customer can change the level / reaction-type of this signature based on their requirement.*<br>*This signature is already available on Host Intrusion Prevention and has been newly added to Endpoint Security Exploit Prevention.* | *8.0.0* | *10.5.3* |
| ***Signature 918:*** *Strong Password Enforcement Disabled*<br>*Description:*<br>- *This event indicates an attempt to delete the registry value "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Notification Packages". This registry value determines whether a password filter that prohibits the use of weak passwords is active.*<br>- *This signature is set to level Low by default.*<br><br>*Note: Customer can change the level / reaction-type of this signature based on their requirement.*<br>*This signature is already available on Host Intrusion Prevention and has been newly added to Endpoint Security Exploit Prevention.* | *8.0.0* | *10.5.3* |

| | | |
|---|---|---|
| ***Signature 6119:*** *SMB Double Pulsar Ping*<br>*Description:*<br>- *This event indicates DoublePulsar backdoor activity in the network. DoublePulsar is a backdoor implant tool that allows DLL Injection, execution of arbitrary code.*<br>- *This signature is set to level Low by default.*<br><br>*Note: Customer can change the level / reaction-type of this signature based on their requirement.* | *8.0.0 (Patch 11)* | *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** |
| ***BugFix:*** *The following signatures have been deprecated from content as the platforms affected by the corresponding vulnerabilities are out of scope for Endpoint Security product.* | *NA* | *10.5.3* |

| ***Signature ID*** | ***Signature Name*** | ***Vulnerability Information*** |
|---|---|---|
| 2231 | Vulnerability in SMB Could Allow Remote Code Execution | CVE-2009-3103 |
| 2232 | SMB Buffer Overflow Remote Code Execution Vulnerability | CVE-2008-4834 |
| 2233 | SMB Validation Remote Code Execution Vulnerability | CVE-2008-4835 |
| 3718 | Network Share Provider Denial of Service (SMBdie) | CVE-2002-0724 |
| 3720 | MSSQL Resolution Service Buffer Overflow (Slammer) | CVE-2002-0649 |
| 3721 | RPC DCOM Stack Buffer Overflow (Blaster, Nachi) | CVE-2003-0352 |
| 3722 | RPC Service Denial of Service (WinNuke) | CVE-2002-1561 |
| 3723 | Windows PPTP Server Buffer Overflow | CVE-2002-1214 |
| 3724 | LSASS Dcpromo Log File Buffer Overflow (Sasser) | CVE-2003-0533 |
| 3725 | IP Options Validation Overflow | CVE-2005-0048 |
| 3801 | Vulnerability in TCP/IP Could Allow Remote Code Execution | CVE-2006-2379 |

| | | |
|---|---|---|
| 3802 | Vulnerability in Server Service Could Allow Remote Code Execution | CVE-2006-1314 |
| 3803 | Vulnerabilities in DNS Resolution Could Allow Remote Code Execution | CVE-2006-3441 |
| 3804 | Vulnerability in Server Service Could Allow Denial of Service | CVE-2006-3942 |
| 3806 | FTP Username/Password Overflow | CVE-1999-0256 |
| 3845 | Vulnerability in Universal Plug and Play (UPnP) Service Could Allow Remote Code Execution | CVE-2007-1204 |
| 3846 | Vulnerability in processing FTP Reply Could Allow Remote Code Execution | CVE-2007-0217 |
| 6029 | SMB Buffer Underflow Vulnerability | CVE-2008-4038 |
| 6022 | Vulnerability in SMB Could Allow Denial of Service | CVE-2009-3676 |

*Note: This change is not applicable for Host Intrusion Prevention product and applicable only for Endpoint Security product.*

*Please refer to the below KB for the list of Platforms supported by Endpoint Security Product*
https://kc.mcafee.com/corporate/index?page=content&id=KB82761

| 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-2018-8491*<br>- *CVE-2018-8460* | *8.0.0* | *10.2.0* |
| ***Coverage by GPEP:*** *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:*<br>- *CVE-2018-8453* | *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’