McAfee Exploit Prevention Content 8807

Release Notes | 2018-12-11

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8807

McAfee Endpoint Security Exploit Prevention: 10.6.0.8807

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 6127: *Suspicious LSASS Access from Powershell* *(BZ #1252843, BZ #1260160)* *Description:* - *This event indicates an attempt to access LSASS.EXE through powershell. Malicious programs often attempt to access and read lsass.exe process memory to gain credential information. This is a suspicious activity and signifies infection.* - *This signature is set to level Low by default.* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*NA*	*10.5.3*
Signature 6128: *Cisco Webex Meetings Update Service Privilege Escalation Attack* *(BZ #1258900)* *Description:* - *This event indicates an attempt to exploit a vulnerability in Cisco Webex Meetings Desktop App Update Service. An attacker could exploit this vulnerability by invoking the update service command with a crafted argument. This vulnerability could allow attackers to elevate their privileges and allow them to run arbitrary commands with SYSTEM user privilege.* - *This signature is set to level Low by default.* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*NA*	*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 6013: *Suspicious Function Invocation - CALL Not Found (BZ #1259076)* *Description:* - *The Signature has been modified to reduce false positives*	*8.0.0*	*10.2.0*
Signature 6015: *Suspicious Function Invocation - Target Address Mismatch (BZ #1260419)* *Description:* - *The Signature has been modified to reduce false positives*	*8.0.0*	*10.2.0*

Note: Refer to the KB for the generic recommendation on obsolete Exploit Prevention signatures: https://kc.mcafee.com/corporate/index?page=content&id=KB91128

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:* - *CVE-2018-8631* - *CVE-2018-8643*	*8.0.0*	*10.2.0*
Coverage by GBOP: *GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-8597* - *CVE-2018-8598* - *CVE-2018-8627* - *CVE-2018-8636*	*8.0.0*	*10.2.0*
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-8587*	*8.0.0*	*10.2.0*

- *CVE-2018-8590* - *CVE-2018-8628* - *CVE-2018-12830* - *CVE-2018-15984* - *CVE-2018-15985* - *CVE-2018-15986* - *CVE-2018-15987* - *CVE-2018-15988* - *CVE-2018-15989* - *CVE-2018-15990* - *CVE-2018-15991* - *CVE-2018-15992* - *CVE-2018-15993* - *CVE-2018-15994* - *CVE-2018-15995* - *CVE-2018-15996* - *CVE-2018-15997* - *CVE-2018-15998* - *CVE-2018-15999* - *CVE-2018-16000* - *CVE-2018-16001* - *CVE-2018-16002* - *CVE-2018-16003* - *CVE-2018-16004* - *CVE-2018-16005* - *CVE-2018-16006* - *CVE-2018-16007* - *CVE-2018-16008* - *CVE-2018-16009* - *CVE-2018-16010* - *CVE-2018-16011* - *CVE-2018-16012* - *CVE-2018-16013* - *CVE-2018-16014* - *CVE-2018-16015* - *CVE-2018-16016* - *CVE-2018-16017* - *CVE-2018-16019* - *CVE-2018-16020* - *CVE-2018-16021* - *CVE-2018-16022* - *CVE-2018-16023* - *CVE-2018-16024* - *CVE-2018-16025* - *CVE-2018-16026* - *CVE-2018-16027* - *CVE-2018-16028* - *CVE-2018-16029* - *CVE-2018-16030*		

- *CVE-2018-16031* - *CVE-2018-16032* - *CVE-2018-16033* - *CVE-2018-16034* - *CVE-2018-16035* - *CVE-2018-16036* - *CVE-2018-16037* - *CVE-2018-16038* - *CVE-2018-16039* - *CVE-2018-16040* - *CVE-2018-16041* - *CVE-2018-16043* - *CVE-2018-16046* - *CVE-2018-16047* - *CVE-2018-19698* - *CVE-2018-19699* - *CVE-2018-19700* - *CVE-2018-19701* - *CVE-2018-19702* - *CVE-2018-19703* - *CVE-2018-19704* - *CVE-2018-19705* - *CVE-2018-19706* - *CVE-2018-19707* - *CVE-2018-19708* - *CVE-2018-19709* - *CVE-2018-19710* - *CVE-2018-19711* - *CVE-2018-19712* - *CVE-2018-19713* - *CVE-2018-19714* - *CVE-2018-19715* - *CVE-2018-19716* - *CVE-2018-19717*		
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-0742* - *CVE-2018-8611* - *CVE-2018-8621* - *CVE-2018-8622* - *CVE-2018-8637* - *CVE-2018-8639* - *CVE-2018-8641*	*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’