McAfee Exploit Prevention Content 11662

Release Notes | 2021-08-10

Content package version for –

McAfee Endpoint Security Exploit Prevention: 10.6.0.11662[1]

McAfee Host Intrusion Prevention: 8.0.0.11662[2]

[1] - Applicable on all versions of McAfee Endpoint Security Exploit Prevention including version 10.7.x

[2] - Applicable on all versions of McAfee Host Intrusion Prevention content including Host IPS 8.0 Patch 16.

IMPORTANT: McAfee V3 Virus Definition Updates (DATs) version 3786 or above is a mandatory prerequisite for this Exploit prevention content update on McAfee Endpoint Security versions 10.5.x and 10.6.x only.
Refer to the below KB for more information:
https://kc.mcafee.com/corporate/index?page=content&id=KB91867

IMPORTANT: Either of the below McAfee Host IPS 8.0 Extension packages is a mandatory prerequisite for receiving the new security or policy updates for this content

1. Host IPS 8.0 Patch 15 Extension (build 8.0.0.1334) – Applicable for Host IPS 8.0 Patch 15 and below
2. Host IPS 8.0 Patch 14 Extension Hotfix 114831 (build 8.0.0.1326) – Applicable for Host IPS 8.0 Patch 14 and below

Refer to the below KB for more information:
https://kc.mcafee.com/corporate/index?page=content&id=KB92596

New Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 6211: *T1220/T1218.005: MSHTA abuse – proxy execution of malicious content* *Description:* - *This event indicates an attempt to execute an obfuscated xsl/jar payload from a spearphishing link. This is an access protection signature and can be used by customers who want to restrict execution of xsl scripts / jar payloads from hta file.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.6.0*

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 Description Modification: *The signature description has been modified for the below signatures.*		
Signature 6209: *Creation of Suspicious DLL through SPOOLSV*	*8.0.0*	*10.6.0*
False Positive Reduction: *The below signature has been modified to reduce the false positives*		
Signature 6013: *Suspicious Function Invocation- CALL Not Found*	*8.0.0*	*10.6.0*

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:* - *CVE-2021-34480*	*8.0.0*	*10.6.0*
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2021-34535*	*8.0.0*	*10.6.0*

How to Update

Please find below the KB article reference on how to update the content for following products:

1. McAfee Endpoint Security Exploit Prevention:
https://kc.mcafee.com/corporate/index?page=content&id=KB92136
2. McAfee Host Intrusion Prevention:
https://kc.mcafee.com/corporate/index?page=content&id=KB53092