McAfee Exploit Prevention Content 11598

Release Notes | 2021-07-13

Content package version for –

McAfee Endpoint Security Exploit Prevention: 10.6.0.11598[1]

McAfee Host Intrusion Prevention: 8.0.0.11598[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 6209: *Creation of Suspicious DLL through SPOOLSV (CVE-2021-1675, CVE-2021-34527)* *Description:* - *This event indicates an attempt to create a suspicious DLL in printer driver folder by SPOOLSV.EXE. This behavior is observed during exploitation through Print Nightmare. Customers are advised to enable the signature only as a temporary stop-gap measure on vulnerable OS platforms and disable printer service where possible.* - *The signature is disabled by default.* *Note:*	*8.0.0*	*10.6.0*

- *Customers not yet able to patch vulnerable OS platforms or disable printer services may enable this signature; it is intended as a temporary stop-gap measure only.* - *Customer can change the level/reaction-type of this signature based on their requirement*		

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**
False Positive Reduction: *The below signatures are modified to reduce the false positives*		
Signature 6113: *T1055 - Fileless Threat: Reflective Self Injection*	*8.0.0*	*10.6.0*
Signature 6151: *Unmanaged Powershell Detected - II*	*Not Applicable*	*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, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2021-34448* - *CVE-2021-28640* - *CVE-2021-28635*	*8.0.0*	*10.6.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2021-31979* - *CVE-2021-33771* - *CVE-2021-34449*	*8.0.0*	*10.6.0*
Coverage by Access Protection: *IIS worker process trying to execute unwanted program (Signature 6195) is expected to cover the below vulnerabilities:* - *CVE-2021-34467*	*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