McAfee Exploit Prevention Content 9626

Release Notes | 2019-10-08

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.9626

McAfee Endpoint Security Exploit Prevention: 10.6.0.9626

Note: 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.
Refer to the below KB for more information:
https://kc.mcafee.com/corporate/index?page=content&id=KB91867

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 6139: *Dynamic Data Exchange Vulnerability* *Description:* - *This event indicates an attempt to exploit a Dynamic Data Exchange Vulnerability by which an attacker can gain remote code execution.* - *This signature is Disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*NA*	*10.5.3*
Signature 6140: *Attempt To Load Non-Aslr Dlls To Bypass Exploit Mitigation Techniques* *Description:* - *This event indicates an attempt to load non-aslr dll using which an attacker can bypass exploit mitigation techniques for successful exploitation.* - *This signature is Disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*

Signature 6141: *IE Envelope – MHT Access* *Description:* - *This event will trigger each time the browser attempts to access a file with the MHT file extension by which an attacker can execute a malicious script on the user's system.* - *This signature is Disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.3*
Signature 6143: *Attempt To Dump Password Hash From SAM Database* *Description:* - *This event indicates an attempt to dump the contents of the SAM database of any Windows system. Malicious program accesses the Security Access Manager (SAM), lowers its permissions, and then outputs the password hashes to attacker's screen (or a file, if specified). The hashes can be used in combination with other password-cracking tool to obtain the plain text password for the system.* - *This signature is Disabled 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 6118: *Fileless Threat: Malicious Code Execution Using DotNetToJScript Technique* *Description:* - *The signature is modified to reduce the false positives.*	*NA*	*10.6.0*

Other Changes	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
BugFix: *Trusted application list has been modified to include the below process* - *eqnedt32.exe*	*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:* - *CVE-2019-1060* - *CVE-2019-1238* - *CVE-2019-1239* - *CVE-2019-1358* - *CVE-2019-1359* - *CVE-2019-1371*	*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:* - *CVE-2019-1327* - *CVE-2019-1331*	*8.0.0*	*10.5.0*
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2019-1325* - *CVE-2019-1334* - *CVE-2019-1345* - *CVE-2019-1361* - *CVE-2019-1362* - *CVE-2019-1363* - *CVE-2019-1364*	*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'