



McAfee Exploit Prevention Content 8479

Release Notes | 2018-06-12

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8479

McAfee Endpoint Security Exploit Prevention: 10.5.0.8479

Below is the updated signature information for the McAfee Exploit Prevention content.

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 2812: Distrack malware infection Description: - The Signature has been modified to reduce false positives	8.0.0	10.5.3
Signature 1157: USB Storage Device Inserted (BZ #1231033) Description: - The Signature has been modified to enhance the protection	8.0.0	10.5.3
Signature 6015: Suspicious Function Invocation - Target Address Mismatch (BZ #1240961) Description: - The Signature has been modified to reduce false positives	8.0.0	10.5.0
Signature 413: Suspicious Double File Extension Execution Description: - The Signature has been modified to reduce false positives	8.0.0	10.5.3
Signature 6032: Suspicious Function Invocation - Target Address Mismatch Description: - The Signature has been modified to reduce false positives	8.0.0	10.5.0

Existing coverage for New Vulnerabilities	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
<p>Coverage by GBOP: GBOP Signatures 428, 1146, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none"> - CVE-2018-0978 - CVE-2018-8249 - CVE-2018-8267 - CVE-2018-8210 	8.0.0	10.2.0
<p>Coverage by GBOP: GBOP Signatures 428, 3922, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none"> - CVE-2018-8248 	8.0.0	10.2.0
<p>Coverage by GBOP: GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none"> - CVE-2018-4945 - CVE-2018-5002 	8.0.0	10.2.0
<p>Coverage by GPEP: Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:</p> <ul style="list-style-type: none"> - CVE-2018-8169 - CVE-2018-1036 - CVE-2018-8208 	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'