



Trellix Exploit Prevention Content 13082

Release Notes | 2023-09-13

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.6.0.13082¹

Trellix Host Intrusion Prevention: 8.0.0.13082²

¹ – Applicable on all versions of Trellix Endpoint Security Exploit Prevention including version 10.7.x

² – Applicable on all versions of Trellix Host Intrusion Prevention content including Host IPS 8.0 Patch 16.

Please see [KB95499](#) for certificate details and more information about the Trellix rebranding efforts.

New Windows Signatures	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
<p>Signature 6265: T1562 – AMSI Bypass – AmsiOpenSession Memory Patch</p> <p><i>Description:</i></p> <ul style="list-style-type: none">- This event indicates an attempt to disable amsi scan by patching AmsiOpenSession Memory.- The signature is disabled by default. <p><i>Note:</i> Customer can change the level/reaction-type of this signature based on their requirement</p>	10.6.0	8.0.0

Updated Windows Signatures	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
Extended Coverage: The below signature is modified to reduce false positives (Bug Fix)		
Signature 6210: Print Spooler loading malicious dll detected	10.6.0	8.0.0
Signature 6248: T1562 – AMSI Bypass – AmsiScanBuffer Memory Patch	10.6.0	8.0.0
Signature 6256: T1562 – AMSI Bypass – DllGetClassObject Memory Patch	10.6.0	8.0.0

Other changes	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
Rebrand Changes: The Below listed EP content Binaries have been rebranded from McAfee to Trellix for company name and copy rights have been updated to Musarubra US LLC <ul style="list-style-type: none"> - HIPHandlers.dll - HIPHandlers64.dll 	10.6.0	8.0.0
Inclusion of NIPS Driver Update: Drivers for Network Intrusion Prevention feature have been upgraded and rebranded from McAfee to Trellix for company name and copy rights have been updated to Musarubra US LLC <ul style="list-style-type: none"> - MfeEpNfcp.sys <p>No action is needed from customer as new driver will be upgraded automatically with this month's content update.</p>	10.6.0	Not Applicable

NOTE:

1. For more information on the deprecation of applicable signatures, see: [KB94952 - List of obsolete signatures deprecated from Exploit Prevention and Host Intrusion Prevention as of June 2022 content.](#)
2. For more information on the default Reaction-type associated with Signature severity levels for all supported product versions, see: [KB90369 - Exploit Prevention actions based on signature severity level.](#)
3. Trellix maintains additional Expert Rules for use in Trellix Endpoint Security's Exploit Prevention policy that can provide increased coverage for more specific requirements. For more information, see [Trellix ExpertRules GitHub Repository.](#)
IMPORTANT: Trellix recommends testing Expert Rules in a non-production test environment to ensure rule integrity, and to prevent conflicts with unique environment configurations. Customers should exercise caution when deploying Expert Rules in their environment.
4. Expert Rules are not available by default with the Content, customers need to configure and deploy the rules according to their requirements.

HOW TO UPDATE

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

1. Trellix Endpoint Security Exploit Prevention:

[KB92136 - Exploit Prevention signature content updates and remediation rollback version for troubleshooting.](#)

2. Trellix Host Intrusion Prevention:

[KB53092 - Information about Host IPS signature content updates](#)