Trellix Exploit Prevention Content 13468

Release Notes | 2024-08-14

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.7.0.13468[1]

Trellix Host Intrusion Prevention: 8.0.0.13468[2]

[1] - Applicable on all versions of Trellix Endpoint Security Exploit Prevention

[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
***Signature 6287**: T1037.001 - Boot or Logon Initialization Scripts Used For Persistence* *Description:* *- This event indicates an attempt to create UserInitMprLogonScript registry key by windows script host or programs which can write key and value in windows registry which can enable an attacker to gain persistence.* *- The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.0*	*Not Applicable*

Updated Windows Signatures & Other changes	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
Extended Coverage: The below signature is modified to reduce false positives		
***Signature 6133**: T1562 - Evasion Attempt: Suspicious AMSI DLL Creation Detected*	*10.7.0*	*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.