Trellix Exploit Prevention Content 13722

Release Notes | 2025-04-09

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.7.0.13722[1]

Trellix Host Intrusion Prevention: 8.0.0.13722[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 6297**: DLL SideLoading Attempt By Electronic Arts Binary Detected* ***Description: – *This event indicates that an attempt is made by Electronic Arts Binary to load unsigned EACore.dll.The behavior indicates a dll hijacking or a sideloading attempt.* – *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.0*	*NA*
Signature 6298**: T1218.013 - System Binary Proxy Execution: Maveinject* ***Description: – *This event indicates an attempt to abuse Mavinject.exe by proxy executing Malicious DLL's. Maveinject.exe is the Microsoft Application Virtualization Injector, a Windows utility that can inject code into external processes as part of Microsoft Application Virtualization.* – *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.0*	*NA*
Signature 6286**: Microsoft Install Service Elevation Of Privilege Vulnerability* ***Description: – *This event indicates an attempt to modify WerSvc registry value by windows installer which can enable an attacker to gain SYSTEM privilege.* – *The signature is disabled by default.*	*10.7.0 (Content-13440)*	*8.0.0*

Note: Customer can change the level/reaction-type of this signature based on their requirement.		
Signature 6241**: LSASS Dump From Taskmanager Detected* ***Description: - *This event indicates an attempt to dump Local Security Authority Server service (LSASS) from Task Manager.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.6.0 (Content-12484)*	*8.0.0*

Updated Windows Signatures	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
False Positive Reduction: The below signatures are modified to reduce false positives		
***Signature 6134:** T1562 - Evasion Attempt: Suspicious AMSI DLL Loading Detected*	*10.6.0*	*NA*

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.