Trellix Exploit Prevention Content 14101

Release Notes | 2026-10-14

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.7.0.14101[1]

Trellix Host Intrusion Prevention: 8.0.0.14101[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 6356: *T1564.003 - Suspicious Headless Conhost Execution Via System Utilities* *Description:* *- This event indicates that an attempt to run conhost in headless mode from system utilities. This suppresses the creation of the graphical terminal window allowing console applications and child processes to execute entirely in the background. This is associated with MITRE ATT&CK Tactic(s): Persistence, Privilege Escalation, Defense Evasion and Technique(s): T1564.003.* *- The signature is disabled by default.* *Note: Customers can change the level/reaction-type of this signature based on their requirement.*	*10.7.0*	*Not Applicable*
Signature 6357: *Dll SideLoading Attempt By HWMonitor* *Description:* *- This event indicates that an attempt is made by HWMonitor binary to load unsigned cryptbase.dll. The behavior indicates a dll hijacking or a sideloading attempt. This is associated with MITRE ATT&CK Tactic(s): Persistence, Privilege Escalation, Defense Evasion and Technique(s): T1574.001.* *- The signature is disabled by default.* *Note: Customers can change the level/reaction-type of this signature based on their requirement.*	*10.7.0*	*Not Applicable*
Signature 6358: *Dll SideLoading Attempt By Mp3tag - The Universal Tag Editor* *Description:* *- This event indicates that an attempt is made by Mp3tag - the*	*10.7.0*	*Not Applicable*

universal Tag editor binary to load unsigned tak_deco_lib.dll. The behavior indicates a dll hijacking or a sideloading attempt. This is associated with MITRE ATT&CK Tactic(s): Persistence, Privilege Escalation, Defense Evasion and Technique(s): T1574.001. *- The signature is disabled by default.* *Note: Customers can change the level/reaction-type of this signature based on their requirement.*		
Signature 6359: *Dll SideLoading Attempt By Email Protection* *Description:* *- This event indicates that an attempt is made by Email Protection binary to load unsigned scansts.dll. The behavior indicates a dll hijacking or a sideloading attempt. This is associated with MITRE ATT&CK Tactic(s): Persistence, Privilege Escalation, Defense Evasion and Technique(s): T1574.001.* *- The signature is disabled by default.* *Note: Customers can change the level/reaction-type of this signature based on their requirement.*	*10.7.0*	*Not Applicable*
Signature 6360: *Dll SideLoading Attempt By Antimalware Core Service* *Description:* *- This event indicates that an attempt is made by Antimalware Core Service binary to load unsigned mpclient.dll. The behavior indicates a dll hijacking or a sideloading attempt. This is associated with MITRE ATT&CK Tactic(s): Persistence, Privilege Escalation, Defense Evasion and Technique(s): T1574.001.* *- The signature is disabled by default.* *Note: Customers can change the level/reaction-type of this signature based on their requirement.*	*10.7.0*	*Not Applicable*
Signature 6361: *Dll SideLoading Attempt By LockScreenContent Server* *Description:* *- This event indicates that an attempt is made by LockScreenContent Server to load DUI70.dll from an unexpected location. The behavior indicates a dll hijacking or a sideloading attempt. This is associated with MITRE ATT&CK Tactic(s): Persistence, Privilege Escalation, Defense Evasion and Technique(s): T1574.001.* *- The signature is disabled by default.* *Note: Customers can change the level/reaction-type of this signature based on their requirement.*	*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.