Trellix Exploit Prevention Content 13535

Release Notes | 2024-10-09

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.7.0.13535[1]

Trellix Host Intrusion Prevention: 8.0.0.13535[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 6238**: T1112 - AMSI Bypass - Registry Modification* *Description:* *- This event indicates an attempt to disable AMSI scanning by editing relevant registry key, The Windows Antimalware Scan Interface (AMSI) is a versatile interface standard that allows your applications and services to integrate with any antimalware product that's present on a machine.* *- The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.0 (content: 12450)*	*8.0.0*
***Signature 6240**: Suspicious DLL Loading by calc* *Description:* *- This event indicates an attempt to load Suspicious DLL by calc.* *- The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.0 (content: 12484)*	*8.0.0*
***Signature 6261**: MOVEit Transfer SQLi Vulnerability* *Description:* *- This event indicates an attempt to creation or modification of .aspx files in MOVEit Transfer within wwwroot directory by IIS Worker Process (w3wp). This vulnerability can be exploited to achieve Elevation of Privilege(EOP).* *- The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.0 (content: 12993)*	*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*	*Not Applicable*
Signature 6285: *Microsoft Office Remote Code Execution Vulnerability*	*10.6.0*	*8.0.0*
Security Level Modification: The default security level for below signatures have been modified from 0 (Disabled) to 3 (Medium)		
Signature 6183: *T1056 - Key capture using Powershell detected*	*10.6.0*	*Not Applicable*
Signature 6186: *Malware Behavior: FareIt Ransomware activity detected*	*10.6.0*	*Not Applicable*
Signature 6192: *Malware Behavior: Trickbot variant activity detected*	*10.6.0*	*8.0.0*
Signature 6194: *Malware Behavior: Trickbot variant activity detected 2*	*10.6.0*	*Not Applicable*
Signature 6195: *IIS worker process trying to execute unwanted program*	*10.6.0*	*8.0.0*
Signature 6196: *Credential theft using Powershell detected*	*10.6.0*	*8.0.0*
Signature 6229: *MSDT Remote Code Execution Vulnerability Detected*	*10.6.0*	*Not Applicable*
Signature 6231: *Coinminer Activity Detected*	*10.6.0*	*Not Applicable*
Signature Name Modification: The below signature name has been modified to include MITRE sub-technique ID		
Signature 344: *T1547.001 - New Startup Program Creation*	*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.