Trellix Exploit Prevention Content 13440

Release Notes | 2024-07-10

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.7.0.13440[1]

Trellix Host Intrusion Prevention: 8.0.0.13440[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 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.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.0*	*Not Applicable*

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 6135**: T1059.001 - Unmanaged Powershell Detected*	*10.7.0*	*Not Applicable*
***Signature 6151**: T1059.001 - Unmanaged Powershell Detected - II*	*10.7.0*	*Not Applicable*

Existing coverage for New Vulnerabilities	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention

***Coverage**: Exploit Prevention (Signature 6281) is expected to cover the below vulnerabilities:* - *CVE-2024-38021*	*10.7.0*	*8.0.0*
***Coverage by GPEP**: Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2024-38059* - *CVE-2024-38085*	*10.7.0*	*8.0.0*

Other changes	Minimum Supported Product version	
	Endpoint Security Exploit Prevention	Host Intrusion Prevention
Signature Name Modification*: The below signature names have been updated with suitable Mitre technique ID's*		
***Old name - Signature 6135:** Unmanaged Powershell Detected* ***New name - Signature 6135**: T1059.001 - Unmanaged Powershell Detected*	*10.7.0*	*Not Applicable*
***Old name - Signature 6143**: Attempt to Dump Password Hash from SAM Database* ***New name - Signature 6143**: T1552.002 - Attempt to Dump Password Hash from SAM Database*	*10.7.0*	*Not Applicable*
***Old name - Signature 6151**: - Unmanaged Powershell Detected - II* ***New name - Signature 6151**: T1059.001 - Unmanaged Powershell Detected – II*	*10.7.0*	*Not Applicable*
***Old name - Signature 6252**: Suspicious Lsass Read Access Detected* ***New name - Signature 6252**: T1003.001 - Suspicious Lsass Read Access 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.