# Trellix Exploit Prevention Content 13401

## Release Notes | 2024-05-15

Content package version for –

Trellix Endpoint Security Exploit Prevention: 10.6.0.13401[1]

Trellix Host Intrusion Prevention: 8.0.0.13401[2]

[1] – Applicable on all versions of Trellix Endpoint Security Exploit Prevention including version 10.7.x

[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 6282: ConnectWise ScreenConnect Path-Traversal Vulnerability*<br><br>*Description:*<br>*- This event indicates an attempt to create or modify .aspx/.ashx files for ScreenConnect application within App_Extensions directory. This vulnerability can be exploited to achieve Elevation of Privilege(EOP)*<br>.<br>*- The signature is disabled by default.*<br><br>*Note: Customer can change the level/reaction-type of this signature based on their requirement.* | *10.6.0* | *Not Applicable* |
| *Signature 6283: Malware Behavior: Pikabot Malware Activity Detected*<br><br>*Description:*<br>*- This event indicates Execution of Vbscript/Javascript by Microsoft Excel from UNC path. This behavior is observed in few variants of Pikabot malware.*<br>.<br>*- The signature is disabled by default.*<br><br>*Note: Customer can change the level/reaction-type of this signature based on their requirement.* | *10.6.0* | *Not Applicable* |
| *Signature 6284: Possible SAM DataBase Access Using Esentutl*<br><br>*Description:*<br>*- This event indicates an attempt to access SAM database using esentutl.exe, using SAM database an attacker can dump the credentials.* | *10.6.0* | *Not Applicable* |

| | | |
|---|---|---|
| *- The signature is disabled by default.*<br><br>*Note: Customer can change the level/reaction-type of this signature based on their requirement.* | | |

| Updated Windows Signatures & Other changes | Minimum Supported Product version | |
|---|---|---|
| | Endpoint Security Exploit Prevention | Host Intrusion Prevention |
| Extended Coverage: The below signatures are modified to improve the coverage. | | |
| *Signature 6232*: GootKit Trojan Detected | *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.