Trellix Exploit Prevention Content 00286

Release Notes | 2023-07-11

Content package version for –

Trellix Endpoint Security Exploit Prevention for Linux: 10.7.0.00286[1]

[1] - Applicable on Trellix Endpoint Security for Linux for version 10.7.2 and later

Please see KB95499 for certificate details and more information about the Trellix rebranding efforts.

New Linux Signatures	Minimum Supported Product version Endpoint Security Exploit Prevention for Linux
***Signature 50034**: T1036.006 - Masquerading: Space After Filename* *Description:* - *This event indicates an attempt to create a file with trailing space. Adversary can hide a program's true filetype by changing the extension of a file.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement. This is a monitoring / telemetry signature and customers are advised to enable this signature on basis of their requirement.*	*10.7.2*
***Signature 50035:** T1070.002 - Clearing Linux System Log Files* *Description:* - *This event indicates an attempt to clear linux system log files. Adversary may clear system logs to hide evidence of an intrusion.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement. This is a monitoring / telemetry signature and customers are advised to enable this signature on basis of their requirement.*	*10.7.2*

Updated Linux Signatures	Minimum Supported Product version Endpoint Security Exploit Prevention for Linux
False Positive Reduction: Below Signature has been modified to reduce the false positives	
***Signature 50007**: T1564.001 - Hidden file created in a hidden directory*	*10.7.2*

NOTE: Refer to the KB for the default Reaction-type associated with Signature severity levels for all supported product versions: KB90369 – Exploit Prevention actions based on signature severity level.

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.