Trellix Exploit Prevention Content 00307

Release Notes | 2024-02-08

Content package version for –

Trellix Endpoint Security Exploit Prevention for Linux: 10.7.0.00307[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 50040**: Possible SideCopy Trojan Infection Detected* *Description:* - *This event indicates a possible SideCopy Trojan Infection. SideCopy is a Advanced Persistent Threat group that has been targeting South Asian countries.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.16*
***Signature 50041**: Possible DDoS Agent Trojan Infection Detected* *Description:* - *This event indicates a possible DDos Trojan Infection. The Malware is capable of launching DDos attack from infected machines.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.2*
***Signature 50042**: Possible Chaos Trojan Infection Detected* *Description:* - *This event indicates a possible Chaos Trojan Infection. Chaos is a Remote Administration Trojan that targets the Linux platform.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.2*
***Signature 50043**: Possible NKAbuse Trojan Infection Detected* *Description:* - *This event indicates a possible NKAbuse Trojan Infection. NKAbuse is a Backdoor that targets the Linux platform.* - *The signature is disabled by default.*	*10.7.2*

Note: Customer can change the level/reaction-type of this signature based on their requirement.	

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.