Trellix Exploit Prevention Content 00368

Release Notes | 2025-02-27

Content package version for –

Trellix Endpoint Security Exploit Prevention for Linux: 10.7.0.00368[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 50052*: Possible Perfctl Trojan Infection Detected* *Description:* - *This event indicates a possible Perfctl Trojan Infection. Perfctl primarily targets Linux servers connected to the internet, exploiting vulnerabilities and misconfigurations to gain initial access.* - *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 50053: *Possible WolfsBane Backdoor Infection Detected* *Description:* - *This event indicates a possible WolfsBane Backdoor Infection. WolfsBane is a Backdoor that targets the Linux platform.WolfsBane serves as a stealthy loader designed to infiltrate targeted systems and enable the deployment of additional malware modules.* - *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 50054: *Possible Hadooken Trojan Infection Detected* *Description:* - *This event indicates a possible Hadooken Trojan Infection. Hadooken Upon execution on the vulnerable server instances drops two distinct payloads - Tsunami malware and another binary used for mining cryptocurrency.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	***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.