Trellix Exploit Prevention Content 00356

Release Notes | 2024-09-17

Content package version for –

Trellix Endpoint Security Exploit Prevention for Linux: 10.7.0.00356[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 50049*: T1048 - Exfiltration Over Alternative Protocol: curl* *Description:* - *This event indicates an attempt by adversaries to steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.* - *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 50050: *T1485 - Data Destruction: dd* *Description:* - *This event indicates an attempt by adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.* - *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 50051: *T1555.003 - Credentials from Web Browsers* *Description:* - *This event indicates an attempt by adversaries to acquire credentials from web browsers by reading files specific to the target browser. Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future.* - *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.