Trellix Exploit Prevention Content 00337

Release Notes | 2024-05-21

Content package version for –

Trellix Endpoint Security Exploit Prevention for Linux: 10.7.0.00337[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 50044**: Possible AcidPour Trojan Infection Detected* *Description:* - *This event indicates a possible AcidPour Trojan Infection. AcidPour is a Trojan that targets the Linux platform. AcidPour looks to wipe systems that rely on flash memory. That could include some embedded devices, network attached storage devices, RAID arrays, and some networking devices.* - *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 50045**: Possible ZipLine Trojan Infection Detected* *Description:* - *This event indicates a possible ZipLine Trojan Infection. ZipLine is a Trojan that targets the Linux platform.ZipLine makes use of extensive functionality to ensure the authentication of its custom protocol used to establish command and control (C2).* - *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 50046**: Possible XZBackdoor Infection Detected* *Description:* - *This event indicates a possible XZBackdoor Infection. XZBackdoor is a Backdoor that targets the Linux platform. Malicious code added to xz Utils versions 5.6.0 and 5.6.1 modified the way the software functions. The backdoor manipulate sshd, the executable file used to make remote SSH connections.* - *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 50047: *Possible XZBackdoor Infection Detected II* *Description:* - *This event indicates a possible XZBackdoor Infection. XZBackdoor is a Backdoor that targets the Linux platform. Malicious code added to xz Utils versions 5.6.0 and 5.6.1 modified the way the software functions. The backdoor manipulate sshd, the executable file used to make remote SSH connections.* - *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 50048: *Vulnerability In Runc Allow Container Escape* *Description:* - *This event indicates an attempt to exploit a vulnerability in Runc that could allow attackers to cause Container Escape.* - *The signature is disabled by default.* *Note: Customer can change the level/reaction-type of this signature based on their requirement.*	*10.7.16*

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.