Trend Micro™ TippingPoint™ Threat Protection System Release Notes

Version 6.4.0

To ensure that you have the latest versions of product documentation, visit the Online Help Center.

Important note

This release is supported on 1100TX, 5500TX, 8200TX, 8400TX, 8600TXE, 9200TXE, and vTPS devices only.

- TPS devices running TOS v5.5.4 or earlier and all TX-Series devices must first migrate to v5.5.5 before upgrading to v6.4.0. Learn more.

- If you are upgrading from an earlier, nonsequential TOS, refer to the release notes of any interim releases for additional enhancements.

- Use SMS v6.4.0 and later to manage a TPS device with this release.

- This release ships with Digital Vaccine (DV) versions 3.2.0.9972 and 4.0.0.9972.

- For information about third party and open source licenses, refer to the *Third-Party Licensing* document.

Release contents

Description	Reference
Support for a new type of Reputation filtering enables users to alert and/or block malicious files according to their hash values. You can add as many as 35,000 SHA-1 or SHA-256 file hashes of any type to the Reputation Database. In this release, file hash is applied to http (or https when decrypting) get requests, for all files except the following: • HTML • Audio or video • Font • Files larger than 50 MB	New
Enhancements to the `physical-media` command include new speeds and Forward Error Correction (FEC) mode settings: • 1000full • 10000full • 25000full • 40000full • 100000full • fec-off • fec-on • fec-default • auto-neg FEC mode settings enable you to avoid and correct mismatches that result in downed links between your devices and their link partners. Learn more about configuring and toggling these settings in the *TPS Command Line Interface Reference*.	New
TPS devices now support Inspection of HTTP/2 traffic when decrypting traffic. HTTP/2 traffic sent in clear text from a third-party decryption engine will be inspected without HTTP/2 decoding. Enabling HTTP/2 decryption requires first disabling the HTTP/2 downgrade option in the client or server SSL proxy.	New
Port configuration is now preserved when swapping I/O modules of the same type. This does not apply to swapping different I/O module types.	TIP-118081 PCT-21764
All members of a stack now report per-device license utilization, and the `show np throughput-utilization` command now displays accurate values.	TIP-108306 TIP-118564 PCT-11132 PCT-24556
A segmentation fault that caused devices to enter Layer-2 Fallback has been repaired.	TIP-128892 PCT-42057

An issue that caused other members of a stack to go into a non-communicative state when one device in the stack gets replaced has been repaired.	TIP-115223 PCT-18601
This release fixes an issue where 8600TXE devices would fail to power on after halting the system while power remained applied for a prolonged period of time.	TIP-128331 PCT-43215
Addressed a rare condition that could cause Layer-2 Fallback when a server-initiated renegotiation occurred during certificate replacement.	TIP-126622 PCT-39294
This release addresses a rare race condition on the TPS device that could occur during a policy configuration change.	TIP-126254 PCT-38255
This release fixes an issue with TPS device packet capture where additional bytes appeared to be captured that were not on the wire.	TIP-124302 PCT-33950
A timing issue that prevented TPS devices from completing its boot-up has been repaired.	TIP-122303 TIP-120158 PCT-27139
This release repairs an issue on TXE platforms that prevented Layer-2 Fallback from functioning unless a cold boot was also performed after an I/O module was hot-swapped.	TIP-119635 PCT-23736
A TRHA configuration issue with certain IP address pairs no longer fails if both devices are running TOS v6.4.0 or later.	TIP-128466
SNMP timeout messages changed from an error level to a warning level message.	TIP-128304
An issue that caused `SOAP Daemon: Fault returned to SMS` ‘`Error getting noisy security policies from TOS`’ to repeatedly display in the system log has been fixed.	TIP-112692 TIP-117214 PCT-1740 SEG-170389
Compatibility issues with the SFP28 management interface and older 10Gbps transceivers have been repaired.	TIP-109831 PCT-17094
Improvements were made to the TOS upgrade process to address a rare case where a device could fail to boot after a TOS upgrade.	TIP-113364 PCT-15152

Known issues

Description	Reference
A known issue with the TPS device's SFP Module (TPNN0068) prevents the ability to configure Auto-Negotiation on a 1 GbE Fiber SFP. You can set the speed on the peer devices with Auto-Negotiation disabled. To use Auto-Negotiation on a 1 GbE fiber connection, the device's SFP+ Module (TPNN0060) supports 1GbE Fiber SFPs and can be used with Auto-Negotiation in TOS v6.1.0 or later.	TIP-92585 TIP-93209 SEG-183369
When hot-swapping IOMs, wait 2 minutes after inserting the first IOM before inserting a second IOM. This gives the system time to complete setup of the first IO module.	TIP-129729
When restoring a snapshot from SMS after changing the masterkey, wait a few minutes before attempting to restore the snapshot so that the SMS and the device can properly sync up.	TIP-129644
The `show health interfaces` and `show health all` commands do not display the correct number of unused ports. For an accurate display of port status, use your SMS interface (**Devices > Ports**). .	TIP-121880
Under some circumstances, removing a device from a stack can cause the device that preceded it in the stack ring to generate a stack-size configuration error.	TIP-88908
For SSL server proxy configuration, select *either* RSA *or* ECDSA. Using both types of certificates can cause connection issues.	TIP-116544
When you edit a stack name, resilience and SRD will not work in TOS v6.4.0. You will have to delete the stack and re-create it to change these values.	TIP-131001

Product support

For assistance, call one of the TippingPoint numbers on the *Contact Support site*.