Trend Micro™ TippingPoint™ Threat Protection System Release Notes

Version 6.3.0

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 v6.3.0. 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 v6.3.0 and later to manage a TPS device with this release.
- This release ships with Digital Vaccine (DV) version 4.0.0.9889. For users upgrading from a TOS with DV version 3.2.0.xxxx, the DV automatically converts to version 4.0.0.9889. For users upgrading from TOS v6.x with a DV build version that is higher than the version packaged with TOS v6.3.0, the higher DV version will be maintained.
- For information about third party and open source licenses, refer to the *Third-Party Licensing* document.

Important: Users can continue to use the CLI interface to manage their v6.3.0 devices; however, the Local Security Manager (LSM) interface is no longer available.

Release contents

Description	Reference
This release expands TXE-Series TPS devices to include the new TPS 8600TXE model.	New
This release introduces Network Sensor support for TXE-Series TPS devices. Network Sensor collects telemetry about traffic going through your network and reports it to Trend Vision One™ for further threat analysis and visibility. Network Sensor requires the following: • Device management by an SMS configured for Trend Vision One integration. The **Security Policy and Inventory** option must be set to **Enabled**. Learn more about integrating your SMS with Trend Vision One from the *Integrating SMS with Trend Vision One Software Guide.* • Each SMS-managed device's SSD user disk must be mounted with at least 50 GB (of 240 GB) space available. • A direct internet connection to enable data sharing with Trend Vision One. • A reboot after NS installation is complete. A reboot is also required after Network Sensor is uninstalled. **Note:** After Network Sensor is installed, you cannot roll back to a build earlier than TOS v6.2.0 without first uninstalling Network Sensor, which also requires a reboot. Running Network Sensor can result in reduced throughput capacity.	New
A preemptive validation now prevents attempts to upgrade to or from a TOS that is not part of the supported migration path.	New
TXE devices add support for the 6-Segment Gig-T Copper Bypass IOM. The ports on this module cannot be configured for manual speed. Auto-negotiation is always set to **On**, and the only supported speed is 1G. Consequently, the SMS client displays the **Auto-negotiation** checkbox as unconfigurable. **Important:** Make sure that your device is upgraded to TOS v6.3.0 before installing this module.	New
You no longer have to enter the `user-disk insert` and `user-disk remove` commands in order to insert and remove an SSD module from a TXE device. However, you must still enter `user-disk unmount` before removing, and `user-disk mount` after inserting.	New
Unsupported configurations have been removed from the OVF template.	TIP-116326 PCT-20134
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 repairs a condition that prevented a TPS device from communicating with the SMS.	TIP-110110 PCT-17077
Port mirroring on a TXE device no longer causes packet loss when the target port speed is exceeded.	TIP-108848 PCT-4323

A condition that caused the system log to get spammed with repetitive messages no longer occurs after a TOS upgrade.	TIP-108847 PCT-5600
The default forward error correction (FEC) setting has been changed to **Enabled**. This fixes an issue that prevented a bypass IOM of a TXE device from establishing a link to its link partner.	TIP- 108846 PCT-11277
The fan speeds of 5500TX and 1100TX devices now run at a higher rate in accordance with updated thermal recommendations. The ZPHA bypass I/O modules for these devices now automatically switch to the bypass state in the event of a full system lockup or crash, keeping the network intact.	TIP-108843 PCT-8382
Time zone data file has been updated to tzdata-2023d.	TIP-106803 PCT-8236
Reputation leaks caused by a TCP Handshake issue with the TCP Proxy no longer occur.	TIP-106049 PCT-5500
Inserting a new I/O module can cause system resources to be depleted when Inspection Bypass is configured for all interfaces. This prevents the inspection bypass rules from being applied, and a configuration rollback causes startup to fail. With this release, you are alerted when bypass resources are exceeded, and you are prompted to reconfigure your bypass rules. To avoid your device from being taxed this way, consolidate your bypass rules to only essential interfaces before inserting an I/O module. You can refine your bypass rules by deselecting at least one segment interface using the SMS client (**Devices > All Devices >** *Devicename* **> Inspection Bypass**) before inserting an I/O module. Alternatively, you can use the CLI to enter a command such as the following: `device{running-inspection-bypass-rule-1}ports 1-1A 1-1B 2-1A`	TIP-101751
When devices are stacked, the value for Tier 1 Bypass Mbps in the output of "Show NP Tier Stats" is reported correctly.	TIP-105781 PCT-5752

Known issues

Description	Reference
If you insert an IOM into a running TXE device without cycling through a cold boot afterwards, Layer-2 Fallback (L2FB) for the segments on that specific IOM will not work. Despite being fully functional from an inspection point of view, the segments on that module will not pass traffic if the device enters L2FB for any reason (including user-initiated L2FB, automatic L2FB during a warm reboot, and automatic L2FB caused by specific events). To avoid this issue, take one of the following actions: • Insert an IOM only while the TXE device is powered off. • Whenever you insert an IOM while the TXE device is running, make sure the device goes through a complete power cycle afterwards. • From the device CLI, enter `reboot full` after inserting an IOM into a running TXE device.	TIP-119635 PCT-23736

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
TXE-Series devices with 25 GE and 100 GE IOMs will default to the following nonconfigurable Forward Error Correction (FEC) settings based on the port's XCVR type: • 100GE-SR4 - CL91 FEC Enabled • 100GE-LR4 - FEC Disabled • 25GE-SR - CL108 FEC Enabled • 25GE-LR - FEC Disabled If the link partner device does not use the same FEC settings as listed above for a given link, then that link cannot be established. Changing the FEC settings on the link partner device to match these settings will allow the link to be established.	TIP-107847
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

Product support

For assistance, contact the *Technical Assistance Center (TAC)*.

© Copyright 2024 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks of their respective owners.