Trend Micro™ TippingPoint™ Threat Protection System Release Notes

Version 6.1.0

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, and 9200TXE TPS devices only.

- TPS devices running TOS v5.5.4 or earlier must first migrate to v5.5.5 before upgrading to v6.1.0. Learn more.
- Beginning with the previous TOS v6.0.0 release, a new cryptographic engine was introduced in TPS devices that removed or disabled weak cryptographic algorithms that are not FIPS-approved, such as cipher suites that use DES-symmetric encryption algorithm or SHA-1 hashing. Although this new engine is still FIPS-capable, official FIPS certification by the FIPS certification authority is currently in progress. Consequently, TOS v6.1.0 does not officially support FIPS mode. A v5.5.5 device with FIPS mode configured will continue to use only FIPS-approved cryptographic algorithms after they upgrade their devices to TOS v6.0.0 and later releases, including this one.
- If you are upgrading from an earlier, nonsequential TOS, refer to the release notes of any interim releases for additional enhancements.
- Use SMS v6.1.0 and later to manage a TPS device with this release.
- For information about third party and open source licenses, refer to the *Third-Party Licensing* document under the Documentation node on the Threat Management Center (TMC).

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

Release contents

Description	Reference
TLS performance enhancements for the 9200TXE device include: • TLS Inspection Throughput: 40 Gbps (up from 25 Gbps) • TLS Connections per second: 20,000 (up from 10,000) • Maximum imported TLS Certificates: 2,500 (up from 1,000)	New
This release enhances SSH by removing weak algorithms. The improved SSH configuration replaces the existing one when you upgrade the device to v6.1.0. You can use the CLI to add and remove any supported algorithms.	New
TXE devices add support for the following bypass I/O modules: • 2-Segment 40 GbE SR4 Bypass • 2-Segment 40 GbE LR4 Bypass • 4-Segment 10 GbE SR Bypass • 4-Segment 10 GbE LR Bypass • 4-Segment 1 GbE SX Bypass • 4-Segment 1 GbE LX Bypass **Important:** Make sure that you upgrade to TOS v6.1.0 before installing any of these modules. For more information on these modules, refer to the *TPS Hardware Specification and Installation Guide*.	New
All devices running TPS TOS v6.1.0 use Digital Vaccine (DV) v4.0.0.9811. This DV version now includes Zero Day Initiative (ZDI) filters. For users upgrading from a TOS with DV version 3.2.0.xxxx, the DV automatically converts to the version 4.0.0.9811. For users upgrading from TOS v6.x with a DV build version that is higher than the version packaged with TOS v6.1.0, the higher DV version will be maintained.	New
TLS inspection is now supported on stacked TXE devices.	TIP-89512
A CLI input validation issue for user creation would create a user group instead of a user. This has been fixed.	TIP-92729 SEG-181247
Some TPS devices exhibited extremely slow SMB and HTTP file transfers. This issue has been fixed.	TIP-91235 SEG-169436
This release resolves an issue that required an SMS to use 2048-bit (2K) keys to communicate with a device. Although this issue is resolved, you can avoid future compatibility issues by upgrading your SMS Certificate Key to a 2K key.	TIP-102107

An issue has been fixed that caused warnings in the system log because of a discrepancy in packet count stats between the NIC and switch.	TIP-83277 SEG-170835
A file handle leak that risked system instability over time has been fixed.	TIP-94031
This release fixes a rare segmentation fault involving libdbus and syslog that could cause the device to go into Layer 2 Fallback mode.	TIP-85986 SEG-159644

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
TOS v6.1.0 does not support FIPS mode. If you are upgrading from TOS v5.5.5 with FIPS mode enabled, the upgrade to v6.1.0 will succeed but the device will incorrectly report that it is still in FIPS mode.	TIP-94157
Because of the internal network switch components, TXE devices cannot support auto-negotiation on 1-GbE fiber interfaces. To establish a link on 1-GbE fiber interfaces, you must set the link partner to 1 GbE with auto-negotiation disabled.	TIP-92585
An issue on TX-Series devices prevents auto-negotiation from working for 1 GbE SFP transceivers in 10 GbE SFP+ modules.	TIP-93209 SEG-183369
The bypass light on any TX device remains on regardless of the bypass condition.	TIP-94280
You can safely ignore any COROSYNC ALERT error message that sometimes displays after upgrading TX-Series TPS devices from TOS v5.5.5 to v6.1.0.	TIP-91378

You can safely ignore the following System log warning message: `SOAP Daemon: Fault returned to SMS 'Error getting noisy security policies from TOS'.`	TIP-91196 SEG-170389
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
A condition that causes the device to generate packet traces faster than the SMS can download them generates an error in the device's system log.	TIP-88844
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-107378

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.