

# Trend Micro™ TippingPoint™ Threat Protection System Release Notes

Version 6.2.0

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, 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 v6.2.0. 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 v6.2.0 and later to manage a TPS device with this release.
- This release ships with Digital Vaccine (DV) version 4.0.0.9862. For users upgrading from a TOS with DV version 3.2.0.*xxxx*, the DV automatically converts to version 4.0.0.9862. For users upgrading from TOS v6.*x* with a DV build version that is higher than the version packaged with TOS v6.2.0, the higher DV version will be maintained.
- For information about third party and open source licenses, refer to the *Third-Party Licensing* document under the Documentation node on the <u>Threat Management Center (TMC)</u>.

**Important:** Users can continue to use the CLI interface to manage their v6.2.0 devices; however, the Local Security Manager (LSM) interface is no longer available.

### **Release contents**

Description	Reference
This release includes support for vTPS device deployments.	
<b>Note:</b> Beginning with TOS v6.2.0, a vTPS device can be run only in Performance mode, and the host CPU must support the AVX2 instruction set. For information on all other deployment requirements, refer to the <i>Virtual Threat Protection System (vTPS) User Guide</i> .	New
This release enhances SSH by removing weak algorithms. The improved SSH configuration replaces the existing one when you upgrade the device to TOS v6.2.0. You can use the CLI to add and remove any supported algorithms.	New
You can now import your own X509 certificates to SMS-managed TX and TXE devices without affecting management functionality or encountering compatibility issues. Import the X509 certificates using the new https-certificate CERTIFICATE-NAME command. Remove the certificate using the new delete https-certificate CERTIFICATE-NAME command.	New
Beginning with TOS v6.2.0, TPS devices support TLS inspection of traffic encrypted with ECDSA.	New
A file handle leak that risked system instability over time has been fixed.	TIP-94031
TPS devices no longer support the DES privacy protocol for SNMPv3 Users or SNMPv3 Trap Destinations. Update any users/trap destinations that use DES to use the AES privacy protocol instead. Otherwise, the device will ignore any users/trap destinations that are using DES, and a system log error will be generated for each invalid configuration item.	TIP-101939
An issue where a heavily configured device could fail to upgrade properly and cause a rollback has been fixed.	TIP-107012 PCT-9125
This release fixes a segmentation fault that could cause the device to go into Layer 2 Fallback mode.	TIP-107008 PCT-7265
An OpenSSH vulnerability (CVE-2023-48795) that enabled attackers to manipulate sequence numbers during the SSH handshake has been repaired in this release.	TIP-107615
TOS v6.2.0 now supports FIPS mode. An upgrade from TOS v5.5.5 with FIPS mode enabled will succeed without an incorrect FIPS mode status.	TIP-94157
The bypass light on a TX device no longer remains on regardless of the bypass condition.	TIP-94280 SEG-189492
An issue that prevented encryption mode in TRHA has been fixed.	TIP-104679 PCT-2907
This release includes updates that improve network stability.	TIP-102599
This release fixes a memory leak issue in switch code.	TIP-107948

A discrepancy that caused the output of "Show NP Tier Stats" in the Stack Segment Ports section to display the incorrect value for each device in the stack has been fixed.	TIP-105781 PCT-5752
An issue with the device CLI misreporting speed/duplex values in the management interface when auto-negotiation is disabled has been fixed.	PCT-2030

# 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:	TIP-119635
	PCT-23736
<ul> <li>Insert an IOM only while the TXE device is powered off.</li> </ul>	
<ul> <li>Whenever you insert an IOM while the TXE device is running, make sure the device goes through a complete power cycle afterwards.</li> </ul>	
• From the device CLI, enter reboot full after inserting an IOM into a running TXE device.	
The fans of a TXE device that has been upgraded from TOS v6.1.0 to v6.2.0 continuously run at their maximum level when you roll back to v6.1.0. After you upgrade the device to v6.2.0 again, the fans will operate properly.	TIP-107191
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.	TIP-92585
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.	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	TIP-107378
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.	

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 discrepancy occurs in the output of "Show NP Tier Stats" when there are stacked devices and a large number of packets bypassed. The value for Tier 1 Bypass Mbps is incorrect.	TIP-105781 PCT-5752

## **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.