Trend Micro™ TippingPoint™ Threat Protection System Release Notes

Version 6.1.1

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

Important notes

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

- If you are upgrading from an earlier, nonsequential TOS, refer to the release notes of any interim releases for additional enhancements.
- All TPS devices must be running a minimum of v5.5.5 before installing this version. Learn more.
- All devices running TPS TOS v6.1.1 use Digital Vaccine (DV) v4.0.0.9811. For users upgrading from a TOS with DV version 3.2.0.xxxx, the DV automatically converts to 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 v6.1.1, the higher DV version will be maintained.
- Use SMS v6.1.0 and later to manage a TPS device with this release. SMS v6.1.0 upgrades are only supported from an SMS installed with SMS v5.4.1 or later. Attempts to upgrade from an older release will return an error. If the error message is blank, check the SMS system log for the complete message.

Release Contents

Description	Reference
This release repairs a memory leak found in functions used within the internal network switch.	TIP-107948 PCT-13071
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
This release enhances SSH by removing weak algorithms. The improved SSH configuration replaces the existing one when you upgrade the device to TOS v6.1.1. You can use the CLI to add and remove any supported algorithms.	TIP-107705
The bypass light on a TX device no longer remains on regardless of the bypass condition.	TIP-94280 TIP-90596 TIP-109786 SEG-189492

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

Product support

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