Threat Protection System Release Notes

Version 5.0.2

This document contains release-specific information for the Trend Micro™ TippingPoint® Threat Protection System Family.

To ensure that you have the latest versions of the product documentation, download from the *TMC*.

This TOS release improves the overall reliability and performance of your TPS security devices, and is required for a TPS TX Series device to correctly inspect traffic with a 40 GbE I/O module. This release is recommended for all TPS and vTPS security devices.

Important: To enable the 40 GbE I/O module to work properly, install this TOS release immediately on your TPS 8400TX and 8200TX devices. The installation performs a **full reboot** of a TPS TX Series device which causes a network interruption on any network slots that are not configured with a bypass I/O module.

Release contents

The following items describe issues fixed in this release.

Description	Reference
This release addresses multiple issues that are related to the 40 GbE I/O module on the TPS 8400TX and 8200TX devices.	121581
A TPS or vTPS security device would enter Layer-2 Fallback when processing HTTP responses. This issue has been resolved and HTTP response processing now works properly.	121150

Release considerations

Consider the following points when applying this release.

TOS v5.0.2 and TPS devices

TOS v5.0.2 is available for the following TippingPoint devices.

Product name	Trend Micro part number
TippingPoint vTPS	n/a

Product name	Trend Micro part number
TippingPoint 440T	TPNN0002
TippingPoint 2200T	TPNN0005
TippingPoint 8200TX	TPNN0090
TippingPoint 8400TX	TPNN0091

TOS v5.0.2 and the Security Management System (SMS)

SMS v5.0.0 is required to manage TOS v5.0.2. SMS v5.0.0 with Patch 2 or later is strongly recommended to manage a TPS or vTPS that is running TOS v5.0.2. Update the SMS to the recommended version before you manage a device with TOS v5.0.2. See the SMS release notes for more information.

Installation

All devices must be running a minimum of TOS v4.2.0 before you can upgrade them to this TOS version. The TOS v5.0.2 release is cumulative and includes all of the issues that were resolved in TOS v5.0.1.

Important: You should plan your TOS installation during a scheduled maintenance window.

Before you install TOS v5.0.2, consider the following:

- Install TOS v5.0.2 on TPS and vTPS devices running TOS v4.2.0 or later.
- On a TPS 8400TX or 8200TX device only, the installation performs a **full reboot** during which time network traffic is interrupted on any network slots that are not configured with a bypass I/O module. It can take up to 20 minutes for the reboot to complete and for the device to return to normal operation.

  Important: A bypass I/O module is required to avoid interruption to the flow of traffic during a full reboot.
- When you upgrade a TPS 2200T or 440T device from TOS v4.2.0 to TOS v5.0.0 or later, the installation causes a small network interruption of approximately 200 ms.
- On a vTPS, the flow of traffic is interrupted during the TOS installation and during a reboot of the TOS.
- To avoid system keystore issues when you rollback a TPS device to TOS v4.2.0, before you install TOS v5.0.2, make sure that the master key is set to a passphrase that you specify. This issue is not applicable to vTPS devices that are running TOS v4.2.0 because vTPS devices on TOS v4.2.0 do not support the configuration of the system master key.
  To rollback to TOS v4.2.0 after you install TOS v5.0.2, the master key that secures the system keystore in the rollback image must match the master key on the device. If you do not set the master key before you install TOS v5.0.2, after you rollback, the keystore is inaccessible until you reset the keystore. For more information, see the *Local Security Manager User Guide*.
- Verify that a recent license package (October 2017 or later) is installed on the device and if necessary, download and install a new license package from the *TMC*. If you install TOS v5.0.2 without a recent license package, the device reverts to its unlicensed throughput.
- When you upgrade from TOS v4.2.0, the authentication settings on your TPS and vTPS devices are remapped. If the authentication security level on your device was set to Maximum, after you install TOS v5.0.0 or later, the security level is reset to Medium, which is the default security level. If necessary, update the security level to specify a higher security level. For more information, see the *Local Security Manager User Guide*.

The following guidelines provide important deployment information:

- **Initial setup** – After you power on, the setup wizard on the console port terminal runs through its initial checks and configurations.
- **Powering on after a system shutdown** – On the 440T TPS device only, after the device is shut down using the `halt` command, you must completely disconnect power—by unplugging the unit or by turning off the power switch on the back of the unit—*for at least 60 seconds* before attempting to power on the device again. For the 2200T and TX Series devices, power can be removed by holding down the front panel power button for 5 seconds, and restored by pressing the power button.
- **Traffic handling on initial setup** – The device blocks traffic until the device has completed the boot sequence. After the boot sequence completes, the device inspects traffic by using the Default inspection profile.

  Important: On TX Series devices, any bypass I/O modules remain in bypass mode until you remove them from bypass mode through the CLI, LSM, or SMS. Rebooting the TPS does not change the bypass mode of the bypass I/O module.

- **Device management** – You can manage your TPS device using the Security Management System (SMS), Local Security Manager (LSM), or the Command Line Interface (CLI).

  Important: When you manage a TPS or vTPS with the SMS, always distribute an inspection profile to all segments to begin protecting network traffic. By default, when you add a vTPS or TPS, all filter categories are disabled in the Default security profile. When a TPS or vTPS device is unmanaged or deleted, there is no change in the filters. For information about device management, see the *Security Management System User Guide*.

- **Virtual segments and IPS profiles** – Rather than edit the settings in the default IPS profile, we recommend that you preserve the default IPS profile. To apply your own IPS profile, create a copy of the default IPS profile and edit the virtual segments.
- **Idle timeout period** – By default, when there has been no LSM or CLI activity for 15 minutes, connection to the device times out. The idle timeout period was reduced from 60 minutes for improved security, and is configurable from the LSM (under **Authentication > Authentication Settings**) or from the CLI. From the `aaa` context, the `login cli-inactive-timeout` and `login lsm-inactive-timeout` commands configure the CLI and LSM timeout periods, respectively. For more information, see the *Threat Protection System Command Line Interface Reference*.
- **Sending Tech Support Reports via email** – If you encounter any issues, create a Tech Support Report (TSR) for each issue you wish to submit. To send a TSR by email, use the following steps:
  a. Create a TSR using the LSM (**Tools > Tech Support Report**). Or, from the CLI, use the `tech-support-report` command. If the TSR times out on the LSM, create a TSR from the CLI.
  b. Use the LSM to export the file to your local system.
  c. Contact *TAC* to open a case and provide a detailed summary of the issue.
  d. Send the TSR file as an email attachment to TAC.

Known issues

This release contains the following known issues.

Description	Reference
When deployed in a stack configuration with four or more TX Series devices, the stack master may be incorrectly placed into Intrinsic HA Layer-2 Fallback. For the latest information on this issue, contact *TAC*.	121741
Inspection Bypass rules do not perform the Egress Mirror action. Because Inspection Bypass rules do not perform the Egress Mirror action, Trend Micro recommends that you use the Ingress Mirror action.	121652

Product support

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