TippingPoint™ Threat Protection System – Release Notes

Version 5.0.1

Release date: January 2018

This document contains release-specific information for the TippingPoint Threat Protection System (TPS). The release notes describe new features and changes included in this release. This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint TPS and Virtual Threat Protection System (vTPS) security devices.

To ensure that you have the latest version of the release notes and other product documentation, download these documents from the Threat Management Center (TMC) at *https://tmc.tippingpoint.com*, or contact your TippingPoint representative.

This document contains the following important information:

New and changed in this release

The TOS v5.0.1 release is recommended for all TOS v5.0.0 and v4.2.0 customers.

This TOS release improves the overall security of the TPS and vTPS security devices, and resolves the following issues:

- **DV package installation issue**

  The TOS v5.0.0 installation incorrectly replaced the active DV package on the device with the DV package version that was included with the TOS v5.0.0 release. The TOS v5.0.1 installation now properly preserves the active DV package when it is more current than the DV package included with this TOS release. For information about the DV packages that are included with this TOS release, see *Release considerations* on page 9. This issue is not applicable to an unlicensed vTPS security device. (120775)

- **Device configuration not preserved (vTPS only)** When you upgraded a vTPS device from TOS v4.2.0 to TOS v5.0.0, any configuration changes to the device that you made after you upgraded to TOS v5.0.0 were lost when you rebooted the device. When you install TOS v5.0.1 on the vTPS device, your configuration changes are now properly preserved upon a reboot of the device. (120818)

- **Issue with excessive SNMP Get requests (or walks)**

  A TPS or vTPS device with TOS v4.2.0 or v5.0.0 can become unresponsive on excessive SNMPc Get requests (or walks) against standard MIBs, the TPT-HIGH-AVAIL MIB, or the TPT-RESOURCE MIB. The device now functions properly when querying TippingPoint MIBs.

  (Best Practice) In a production environment, do not perform excessive SNMP Get requests (or walks) against standard MIBs. (121003)

The TOS v5.0.1 release includes the same features that were introduced in TOS v5.0.0:

- *Introduction of the TPS TX Series* on page 3
- *Stacking* on page 4
- *SSL Inspection* on page 4
- *sFlow traffic sampling* on page 5
- *Configuration of TACACS+ remote authentication* on page 5
- *URL filtering capability for Reputation profiles* on page 5
- *Named IP address groups for Traffic Management filters* on page 5
- *Licensing enhancements* on page 5
- *Inspection bypass enhancements* on page 6
- *Provider Backbone Bridging (MAC-in-MAC) support* on page 6

Introduction of the TPS TX Series

The TPS TX Series is a powerful network security platform that offers comprehensive threat protection, performance scalability, and high availability:

- Flexible I/O module support – The 8200TX supports two I/O modules; the 8400TX supports four I/O modules.
  - The following **standard** I/O modules are supported for the 8200TX and 8400TX security devices and are hot-swappable:

Standard I/O module	Trend Micro part number
TippingPoint 6-Segment Gig-T	TPNN0059
TippingPoint 6-Segment GbE SFP	TPNN0068
TippingPoint 4-Segment 10 GbE SFP+	TPNN0060
TippingPoint 1-Segment 40 GbE QSFP+	TPNN0069

  - The following **bypass** I/O modules are supported for the 8200TX and 8400TX security devices and are hot-swappable:

Bypass I/O module	Trend Micro part number
TippingPoint 4-Segment Gig-T	TPNN0070
TippingPoint 2-Segment 1G Fiber SR	TPNN0071
TippingPoint 2-Segment 1G Fiber LR	TPNN0072
TippingPoint 2-Segment 10G Fiber SR	TPNN0073
TippingPoint 2-Segment 10G Fiber LR	TPNN0074

- Stacking support. See *Stacking* on page 4.
- SSL inspection support. See *SSL Inspection* on page 4.

Stacking

Stacking enables you to increase the overall inspection capacity of your TPS by grouping multiple TX Series devices and pooling their resources.

You can configure up to five TX Series devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). The devices in the stack can be all 8200TX or 8400TX TPS devices, or a mix of both 8400TX and 8200TX security devices. All devices in a stack should be licensed for the same inspection throughput.

In-line inspection capacity increases with each device that you add to the stack. For example, for each 8200TX or 8400TX added to a stack of devices, the inspection capacity increases according to the licensed inspection capacity of each device, up to a stacking maximum of 120 Gbps.

The following TippingPoint software is supported for stacking:

- **TippingPoint SMS v5.0.0, or later** - Centrally manages each stack of devices.
- **TippingPoint TPS v5.0.0, or later** - Must be installed on each security device.

Note: No additional licensing is required to implement stacking.

For complete information about stacking, see the *TX Series Stacking Deployment Guide* on the TMC.

SSL Inspection

Changes to SSL inspection include the following:

- **Device support for SSL inspection** – In addition to the 2200T, device support for SSL inspection extends to the TX Series (8200TX and 8400TX) and vTPS (performance image only, with RDRAND instruction recommended) security devices. For information about how to deploy the vTPS for SSL inspection, see the *vTPS Deployment Guide* on the TMC at *https://tmc.tippingpoint.com*.
- **Support for RC4 cipher suite removed** – SSL inspection no longer supports the RC4 cipher suite. If you configured an SSL server with RC4 cipher support, edit and save the server configuration to remove RC4. If no other ciphers were specified, the server configuration automatically adds the default ciphers.

sFlow® traffic sampling

Administrators can use sFlow® record emission to sample and analyze a random flow of traffic. This way, a baseline of typical application traffic can be established, and anomalous and malicious flows can be detected early. This feature cannot be enabled on vTPS devices.

TACACS+ remote authentication

A Terminal Access Controller Access-Control System Plus (TACACS+) server can be configured for central authentication of users. Because TACACS+ authenticates over TCP, it does not require transmission control the way RADIUS authentication does.

URL filtering capability for Reputation profiles

With URL filtering, users can achieve more granular reputation controls in their security profiles than with reputation filters based merely on domains or IP addresses. For example, instead of blocking everything at `www.mywebsite.com`, filtering can be configured to block only specific web pages like `www.mywebsite.com/malicious/stuff` but still allow access to `www.mywebsite.com/useful/information`. Configure URL filtering using the SMS GUI. For more information, see the *SMS User Guide* and the *URL Filtering Deployment and Best Practices Guide* on the TMC at *https://tmc.tippingpoint.com*.

Named IP address groups for Traffic Management filters

From the SMS, named IP address groups are now available for Traffic management filters on the TPS.

Licensing enhancements

Beginning with TOS v5.0.0, all TPS product licensing will be unbundled from the hardware and issued electronically. The license manager, available from the TMC by navigating to **My Account > License Manager**, allows you to easily control the certificates and licenses that you purchase for your TPS products. This licensing model enables you to attach and detach TPS speed and feature licenses. For more information, see the *License Manager User Guide* available from the license manager on the TMC at *https://tmc.tippingpoint.com*.

Inspection bypass enhancements

In addition to the default Bypass action, the following actions are available for inspection bypass:

- Block – Drops traffic.
- Ingress mirror – Sends a copy of the traffic to the mirror target Ethernet port prior to inspection.
- Egress mirror – Sends a copy of the traffic to the mirror target Ethernet port after inspection.
- Redirect – Interrupts the traffic and sends it to the target Ethernet port to prevent inspection.

Provider Backbone Bridging (MAC-in-MAC) support

The TippingPoint TX Series devices protect your MAC-in-MAC encapsulated traffic that follows the IEEE 802.1ah standard. Keep the following points in mind:

- The TPS TX Series device cannot inspect MAC-in-MAC traffic if the customer network uses the most significant four bits in the I-SID to form different MAC-in-MAC provider domains. Network protection is limited to the least significant 20 bits of the 24-bit service identifier (I-SID).
- You can verify the device recognizes MAC-in-MAC traffic by running the `debug np stats show npParseStatsInst` CLI command on the device or by taking a packet capture. When you configure the packet capture, specify a TCPDump expression that identifies the Backbone MAC address (B-MAC) or Backbone VLAN identifier (B-VID) of the traffic you want, or capture all packets for particular segment.

SNMP enhancements

Enhancements for SNMP include support for the following MIBs:

- TPT-TSE
- TPT-BAY
- TPT-NPSTATS
- TPT-SFLOW
- TPT-TRAFFIC – Rate limit objects

Increased VLANs for virtual segments

Beginning with TOS v5.0.0, the maximum VLAN IDs you can configure for a virtual segment has increased from 512 to 4094.

Configuration of TCP MSS for SYN-Proxy

TCP maximum segment size (MSS) is now INI-configurable for SYN-Proxy.

Note: Contact TAC to implement these INI changes. This also requires a device reboot.

Port agnostic HTTP Mode

HTTP mode enables all TCP ports to be treated as HTTP ports for inspection purposes. Beginning with TOS v5.0.0, this mode stops HTTP processing if it determines that a flow does not have HTTP traffic, thereby maintaining optimum performance.

Detailed device installation instructions are now on the TMC

Go to the TMC at *https://tmc.tippingpoint.com* for detailed installation instructions on TPS devices. Basic installation instructions are provided with the product shipment for the 440T, 2200T, 8200TX and 8400TX devices.

Secure system keystore

By default, the system keystore is always secure. The system master key protects the system keystore with encryption. The system keystore retains sensitive data, such as device certificates and private keys.

Important: To avoid system keystore issues when you rollback a TPS device to TOS v4.2.0, before you upgrade a TPS device to TOS v5.0.1, make sure that the master key is set to a passphrase that you specify. This issue is not applicable to vTPS devices running TOS v4.2.0 because vTPS devices on TOS v4.2.0 do not support the configuration of the system master key. For more information, see the *Local Security Manager User Guide*.

Snapshots no longer include contents of the system keystore

Snapshots taken in TOS v5.0.0 and later no longer include the contents of the system keystore. When you restore a snapshot to a different device, you should plan to also import any private key information from the device where the snapshot was taken.

Export a Tech Support Report from a TX Series device

In the SMS, you can collect diagnostic information from 8200TX and 8400TX devices by exporting a Tech Support Report (TSR). The TSR collects information from diagnostic commands and log files into a report that TippingPoint Technical Support can use to debug and troubleshoot the device.

Unlike a TSR created on the device by using the IPS Local Security Manager (LSM), the TSR exported by the SMS does not include snapshot information. However, you can create a snapshot from the SMS. For complete information about how you can export a TSR from the SMS, see the *Security Management System User Guide*.

Device support for packet captures

From the LSM and the SMS, you can now manually take a packet capture on a TPS device. For more information, see the *Local Security Manager User Guide* and the *Security Management System User Guide*, respectively. From the device CLI, use the `tcpdump` command to take a packet capture. For more information, see the *Command Line Interface Reference*.

MTU size increased

Jumbo frame support is enhanced on TPS devices to allow a maximum transmission unit (MTU) size of up to 9050 bytes. This includes the 14-byte Ethernet header, 9032 bytes of payload data, and the 4-byte Ethernet checksum. This feature is not supported on vTPS devices.

Release considerations

The following restrictions apply to this release.

TOS v5.0.1 and TPS devices

TOS v5.0.1 is available for the following TippingPoint devices.

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

TOS v5.0.1 and Digital Vaccine (DV)

The DV package that is installed on your device can vary based on the model of the device:

- All TPS hardware devices use the 3.2.0 series of DV packages. On a TPS device, the TOS v5.0.1 installation includes the SIG_3.2.0.9040 DV package.
- All vTPS devices use the 4.0.0 series of DV packages which do not include Zero Day Initiative (ZDI) filters. On a vTPS device, the TOS v5.0.1 installation includes the 4.0.0.1000 DV package which installs a limited number of security filters for testing and evaluation purposes.

  Important: The vTPS initially starts up in vTPS Trial Mode. Trial Mode is primarily exploratory and comes with a limited number of security filters in the Digital Vaccine (DV) package. In this mode, an SMS can manage only one vTPS at a time. Because Trial Mode has a fixed serial number and entitlement, you cannot use Trial Mode to perform TippingPoint Operating System (TOS) upgrades or distribute DVs. After you upgrade your device to Standard Mode, you can then install a full DV package.

For information about how you can update the DV package to the latest version, see the *Local Security Manager User Guide* or the *Security Management System User Guide*.

TOS v5.0.1 and the Security Management System (SMS)

SMS-managed devices with TOS v5.0.1 installed must be managed with SMS v5.0.0 or later. The SMS must be updated before you use it to manage devices with TOS v5.0.1 installed. Refer to the SMS release notes for information about updating the SMS.

Installation

This section provides TOS v5.0.1 installation instructions.

For detailed TPS device installation instructions, refer to the *Install your security device* quick start document on the TMC. For installation information about the vTPS security device, download the *Virtual Threat Protection System Deployment Guide* from the TMC at *https://tmc.tippingpoint.com*.

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

Before you install TOS v5.0.1, consider the following:

- Install TOS v5.0.1 on TPS and vTPS devices running TOS v4.2.0 or v5.0.0.
- When you upgrade a TPS device from TOS v4.2.0, after the upgrade completes, the flow of traffic is temporarily interrupted:
    - TPS 440T – approximately 20-30 ms interruption
    - TPS 2200T – up to 200 ms interruption

  To avoid experiencing the same interruption whenever the operating system is rebooted, perform a **full reboot** of the device by running the `reboot full` command from the device CLI. This issue is not applicable to vTPS devices. (117822)
- On vTPS devices, the flow of traffic is interrupted during a TOS upgrade and during a reboot of the device.
- To avoid system keystore issues when you rollback a TPS device to TOS v4.2.0, before you upgrade a TPS device to TOS v5.0.1, make sure that the master key is set to a passphrase that you specify. This issue is not applicable to vTPS devices running TOS v4.2.0 because vTPS devices on TOS v4.2.0 do not support the configuration of the system master key.
  After you upgrade from TOS v4.2.0, in order to rollback, 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 upgrade from TOS v4.2.0, 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 at *https://tmc.tippingpoint.com*. If you install TOS v5.0.1 without a recent license package, the device reverts to its unlicensed throughput.
- Maximize the space on your device by removing old TOS versions and packet traces. This ensures a successful installation and allows for a TOS rollback, if necessary. You can remove previous TOS versions by using the SMS, the LSM, or the CLI. For complete information, refer to your product documentation located on the TMC at *https://tmc.tippingpoint.com*.

After you install TOS v5.0.1, keep in mind the following:

- The TOS v5.0.1 installation preserves the active DV package on the device when it is more current than the DV package included with this TOS release. For information about the DV packages that are included with this TOS release, see *Release considerations* on page 9.
- 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 v5.0.1, 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 device 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 device, 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 Support to open a case and provide a detailed summary of the issue.

  d. Send the TSR file as an email attachment to your corresponding Support agent.

Resolved issues from the previous release

The TOS v5.0.1 release includes the following resolved issues that were originally addressed in TOS v5.0.0.

Description	Reference
Time changes and NTP synchronization When the device time was changed to a value that differs from the current time by more than 1000 seconds, the NTP service stopped, and the device no longer synchronized the time with the environment. If the NTP service did stop, the following critical log message appeared: `Large clock discrepancy detected (> 1000s), NTP service stopping. Check clock and restart NTP service.` The device now properly synchronizes time changes with the NTP service.	103644
Issues removing and importing device certificates in PKCS12 format You can now delete certificates that were imported in PKCS12 format without issue.	112174
Device events for SSL inspection did not display the name of the segment In the SMS, the device events for SSL inspection (*`device_name`* **> Events > SSL Sessions**) now properly display the actual segment name.	113102
When you unmanage a device that is configured to persist private keys on the SMS, the LSM incorrectly allowed you to import private keys If a managed device is configured to persist its private keys on the SMS, and you unmanage the device, the LSM no longer allows you to import a private key into the device keystore as part of a PKCS12 certificate.	113285
The Rx Packets/Sec SNMP tier statistics were incorrectly reduced by a factor of 1,000 During a TPT-NPSTATS-MIB query, the correct values for the `npstatsTiersRxPktsPerSec [Rx Packets/Sec]` and `npstatsTiersMaxPktsPerSec (Rx Packets/Sec)` tier statistics are now returned.	116508
Disk usage health issue with show health CLI command	116561

Description	Reference
The `show health` CLI command now properly indicates when disk usage health is critical.	

Known issues

The TOS v5.0.1 release includes the following known issues that were originally identified in TOS v5.0.0.

Description	Reference
Missing interface information in IPS logs The ipsBlock log incorrectly shows the incoming interface for a DDoS attack as `unknown`.	104275
Jumbo frames are not supported on vTPS Use a TPS device to monitor jumbo frames. The TPS supports a maximum transmission unit (MTU) size of up to 9050 bytes. This includes the 14-byte Ethernet header, 9032 bytes of payload data, and the 4-byte Ethernet checksum.	105776
Do not create a snapshot and a TSR with a snapshot at the same time If you need to create both a snapshot and a TSR that includes a snapshot, create them separately. If you attempt to create a snapshot and a TSR with a snapshot at the same time, XMSD errors are written to the System log.	107539, 112664
Configuring a Reputation profile from the LSM or the CLI does not work properly. **Workaround:** Use the SMS to configure a Reputation profile.	108632, 112859
Performance statistics for inspection bypass rules become reset When you disable or modify an inspection bypass rule from the SMS, the performance statistics for the rule, such as packet hit count, are reset. **Workaround:** To preserve the statistics for an inspection bypass rule, create a new rule.	109022
SSL traffic limitations over the TPS When SSL Inspection is enabled, the same SSL traffic (source/destination IP address and port) cannot traverse the TPS twice.	111096, 111531
IDS mode considerations	111159, 108569

Description	Reference
Intrusion Detection System (IDS) mode, configured from the CLI, requires a reboot for the change to take effect. Also, changing IDS Mode does not change Performance Protection mode. For best results, when enabling IDS Mode, change Performance Protection to "Always" mode.	
Incorrect system log entry for non-encrypted traffic on an SSL port When SSL inspection is configured, the system log incorrectly indicates that non-encrypted traffic flows on an SSL port are decrypted with an unknown protocol and cipher. The TPS device drops non-encrypted traffic flows that match a server tuple (destination port and destination IP address) in the SSL profile due to the lack of an SSL handshake.	111718
Inaccurate SYN flood information in DDoS block log The DDoS block log incorrectly shows SYN floods on all segments rather than the actual segments where the SYN floods occurred.	111859
Issue with the show interface statistics command on the vTPS On the vTPS, the `show interface statistics` command displays incorrect packet counts for incoming unicast, multicast, and broadcast packets. **Note:** The total received packet counter, `RX Total Packets`, displays the correct total.	115028
Removing a device from a stack If you remove a device from a stack, you can repurpose it for use in another stack or as a standalone device. To repurpose a device, you must use the `debug factory-reset` command. This restores the device to its original settings.	116325
Restoring a stacked device snapshot to standalone device If you restore a stacked device snapshot to a standalone device, the device state will be invalid. **Workaround:** Use the `reboot full` command to put the device back into a valid state.	116397
Non-encrypted traffic when SSL is configured	117048

Description	Reference
- The TPS drops non-encrypted traffic flows that match a configured SSL server tuple (destination port and destination IP address) in the SSL profile but send cleartext traffic before starting an SSL handshake (as some protocols allow via *STARTTLS*). - The TPS device will drop non-encrypted traffic flows that match a configured SSL server tuple (destination port and destination IP address) in the SSL profile due to the lack of the SSL handshake.	
vTPS on ESX 6.0 requires latest Update 3 (U3) When you deploy the vTPS on the vSphere Hypervisor (ESXi 6.0), always install the latest Update 3 (U3) to prevent IPv6 packet drops.	118038
When a link is down, the LSM and the CLI display incorrect port configuration When a link is down, the LSM and the `show interface` CLI command incorrectly indicate that the port configuration is 10 Mbps at half-duplex.	118216
All filter categories in the Default security profile are disabled when you manage a device with the SMS When you manage a TPS or vTPS device 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 device, 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.	118990
RDRAND recommended configuration for vTPS with SSL inspection For users with an SSL license who are deploying the Performance image, Intel Xeon CPUs based on Ivy Bridge or newer (for example, E5-2697v2 and E5-2683v3) are recommended for their support of hardware random number generation (RDRAND instruction). In order for the VM to incorporate the CPU features, additional hypervisor configuration might be necessary: - For VMWare, adjust the EVC mode to `Ivy Bridge` or newer as necessary. For more information, see the *VMWare Knowledge Base*. - For Red Hat, set the guest CPU to `host-passthrough`, `Haswell`, or newer. For more information, see the *Red Hat Enterprise Linux 7 Virtualization Deployment and Administration Guide*.	119429, 120345
Do not use DES privacy protocol with SNMPv3	119942

Description	Reference
When you configure NMS, do not configure SNMPv3 with DES privacy protocol. SNMPv3 traps and informs with DES privacy protocol do not work properly.	
Issue with changing the LDS configuration from Breaker mode to Wire mode after a link goes down With a segment in Breaker mode, after Link Down Synchronization (LDS), if you want to change the segment mode from Breaker mode to Wire mode, the segment remains in Hub mode. **Workaround:** Put the segment in Wire mode, and then manually restart both member ports. Or, restart the device to reset the segment LDS mode.	120081
Issue with inspection bypass rules on 40 GbE I/O modules On TPS TX Series devices, inspection bypass rules do not work with 40 GbE I/O modules. **Workaround:** There is no workaround for this issue. To avoid this issue, do not configure inspection bypass rules on a 40 GbE I/O module.	120459
Incorrect Bypass LED status during boot-up and reboot on 8200TX and 8400TX devices While a TX Series device completes its boot sequence, the Bypass LED status is incorrect. **Workaround:** On TPS 8200TX and 8400TX devices, disregard the status of the Bypass LED while the device completes its boot sequence. A TX Series device correctly stays in Intrinsic High Availability (Intrinsic HA) Layer-2 Fallback (L2FB) mode until its boot sequence completes. If INHA L2FB was enabled before the device rebooted, L2FB mode does not persist after the boot sequence completes.	120183
Status and Alert LED states are incorrect after TOS update on TPS 440T and 2200T devices On TPS 440T and TPS 2200T devices with TOS v4.2.0, when you install TOS v5.0.1, the Status and Alert LEDs incorrectly display an Amber status. **Workaround:** On TPS 440T and 2200T devices, when you update the TOS from v4.2.0 to v5.0.1, disregard the Status and Alert LED status information. You can access information about device health by using the SMS or the LSM.	120302

Description	Reference
Profile distribution issue with Reputation filters to a vTPS device When you distribute a profile with Reputation filters to a vTPS device, and the default Reputation filter settings have been updated to include the Reputation Enforcement option, the profile distribution may timeout. As a result, on a reboot of the vTPS (normal image), the device may enter the recovery console, where a factory reset is required to recover the device. On a timeout, the vTPS (normal image and performance image) creates following error in the System log: `Install failed: Error installing IPDB package from TOS: Timeout` The Reputation Enforcement option, **Also apply filter actions to HTTP requests with matching DNS names**, is not supported on the vTPS. **Workaround:** To resolve this issue, disable DNS enforcement in the Reputation filter settings and then redistribute the inspection profile. To verify the Reputation filter settings for an inspection profile, from the SMS, click **Profiles > Inspection Profiles >** *profile name* **> Reputation / Geo**, then click **Edit Settings**. Under Reputation Enforcement options, make sure the checkbox is not selected.	120395
TLS connection issues with SSL v3.0 When you configure an SSL server with SSL v3.0 and TLS v1.1 or TLS v1.2, SSL inspection cannot establish a TLS connection unless all TLS protocols are configured. If you need to configure SSL v3.0 with TLS, always configure all TLS protocols, including TLS v1.0, TLS v1.1, and TLS v1.2.	120412
Issue with inspection bypass rules on a 40 GbE I/O module On a TPS TX Series device, inspection bypass rules do not correctly match incoming traffic on a 40 GbE I/O module. **Workaround:** There is no workaround for this issue.	120459

Product support

Information for you to contact product support is available on the TMC at *https://tmc.tippingpoint.com*.

Legal and notice information

Trend Micro Incorporated makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro Incorporated shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro Incorporated products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro Incorporated shall not be liable for technical or editorial errors or omissions contained herein.

Edition: January 2018