Threat Protection System Release Notes

Version 5.3.0

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

Important notes

This release is supported on vTPS, 440T, 2200T, 1100TX, 5500TX, 8200TX, and 8400TX 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 v5.0.1 before installing this version. Learn more.
- Use SMS v5.3.0 and later to manage a TPS device with this release.

Release Contents

Description	Reference
You can use multiple certificates and keys for a single SSL server. Support for the Server Name Indication (SNI) protocol extension enables the server to safely host multiple TLS/SSL certificates (up to 1000 per device) for multiple sites under a single IP. When configuring SSL to accept multiple certificates and keys, ensure that you do not enable the SSLv3 protocol. The SSLv3 protocol is disabled by default.	New
New options are available in the CLI for managing core files: • To remove core files: `delete corefiles` • For including or excluding core files in a tech support report: `include corefiles | exclude corefiles`	New
The number of supported ciphers for SSL inspection has increased from 11 to 14. The following three cipher suites are now supported: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 To see the full list of supported cipher suites, navigate to **Profiles** > **Shared Settings** > **SSL Servers** > **New** in the SMS Client. The list of supported cipher suites automatically updates based on your protocol selections.	New
Improvements to SNMP include support for or enhancements to the following MIBs: • TPT-POLICY • TPT-HOST • TPT-LICENSE • TPT-MULTIDV	New
The LSM interface for configuring SSL has been removed. Use the SMS Client interface to configure SSL. SSL inspection active session information has been removed from both the LSM and SMS.	TIP-43661
System logs now indicate when a device is forced into a cold reboot.	TIP-31776
Data no longer stalls on long-lasting persistent connections with infrequent traffic going through SSL inspection.	TIP-34514
Enterprise Vulnerability Remediation (eVR) scans now support non-ASCII characters in filenames.	TIP-35729
Adding or deleting inspection bypass rules no longer causes the remaining rules to be reordered differently than the way they were listed in the original configuration.	TIP-30537

Improved error handling and added scrubbing functionality for internal SRAM memory. Improvements include the elimination of fault-initiated L2FB caused by FPGA error codes `0x80`/`0x40`/`0xC0`, although some extreme cases can still impact performance.	TIP-27930
Placing an inspection bypass rule with an ingress-mirror action first in the rule order no longer changes the behavior of subsequent rules.	TIP-36974
The documentation has been updated to clarify that users with Administrative privileges can view and clear the audit logs for TPS devices.	TIP-36496
RX and TX power readings have been added to the `debug np port diag` command. The readings are updated every few seconds for supported transceivers. **Note:** Use `debug` commands only when you are instructed to do so by TippingPoint product support.	TIP-36124
The TPS and SMS interfaces no longer permit hostnames to include periods (.). Hostnames can consist only of alpha-numeric characters and hyphens, and cannot exceed 63 characters or have a hyphen at the beginning or end.	TIP-44323
A condition that caused the TPS to slowly consume internal memory has been resolved.	TIP-44191

Known issues

Description	Reference
When you insert a 40 Gbps bypass module (BIOM) into a TX-Series TPS device that has not been upgraded to at least TOS v5.2.0, the module health status LED indicates that the module has experienced a fault (solid amber). To recover from this state: 1. Upgrade the device to TOS v5.2.0 or later. 2. After the upgrade, perform a full reboot of the device. 3. Disable bypass on all BIOMs by selecting the normal option: • SMS: From the Device menu, click the device and select **Device Configuration -> HA (High Availability) -> Zero Power HA**. • LSM: Select **System -> High Availability -> Zero-Power HA**. • CLI: `high-availability zero-power (bypass|normal) (slot|all)`	TIP-33655
Performing any kind of inspection, including SSL inspection, on VXLAN packets with a vlan tag in the outer (tunnel) header is not supported on 8200TX and 8400TX devices.	TIP-45595
For optimal performance of URL filtering and other memory intensive features running on a vTPS in Normal mode, configure 16 GB of RAM.	TIP-33876

When you create a snapshot using the LSM, the browser sometimes times out even though the snapshot creation eventually succeeds.	TIP-37112
System logs do not indicate when the state of a transceiver changes.	TIP-39167
SSL inspection no longer supports compression within TLS/SSL, nor periodic rekeying.	TIP-32066

Product support

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