Threat Protection System Release Notes

Version 4.1.2

October 2016

These release notes apply to:

- TippingPoint Threat Protection System (TPS) 440T and 2200T security devices
- TippingPoint Operating System (TOS) v4.1.2

This document contains release-specific information for the TippingPoint Operating System (TOS) supplied with the TPS and describes known issues that are currently being addressed. This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint TPS devices.

Note: TOS v4.1.2 is available for TippingPoint 440T and 2200T devices only, and cannot be installed on other TippingPoint platforms. See *Release restrictions* for more information.

This document contains the following important information about the TOS v4.1.2 release:

New and changed in this release

This maintenance release includes several fixed issues, described in *Resolved issues* on page 3.

Release restrictions

The following restrictions apply to this release of the TippingPoint Operating System (TOS).

TOS v4.1.2

TOS v4.1.2 is available for TippingPoint 440T and 2200T devices.

TOS v4.1.2 cannot be installed on any other TippingPoint platforms.

TOS v4.1.2 and Digital Vaccine

TOS v4.1.2 includes the SIG_3.2.0_8851 DV package.

TOS v4.1.2 and the SMS

SMS-managed devices with TOS v4.1.2 installed must be managed with SMS v4.4.0 or later. The SMS must be updated before you use it to manage devices with TOS v4.1.2 installed.

Installation

The following section highlights important deployment information and operational characteristics of the 440T and 2200T devices.

Note: 440T devices must be running a minimum of TOS v4.0.0 before they can be upgraded to TOS v4.1.2.

- **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 only, after the device is shut down using the `shutdown` 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. This is not applicable to the 2200T TPS.
- **Traffic handling on initial setup** – The device blocks traffic until the device has completed the boot sequence.
- **Device management** – You can manage your TPS using the Security Management System (SMS), Local Security Manager (LSM), or the Command Line Interface (CLI).
- **Virtual segments and IPS profiles** – To preserve the settings in the default IPS profile, create a copy of it for your own IPS profiles. This way, you can edit the virtual segments to apply your own IPS profile rather than edit the default IPS profile.
- **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 CLI. From the `aaa` context, the `login cli-inactive-timeout` and `login lsm-inactive-timeout` commands configure the CLI and LSM timeout periods, respectively. See the *Threat Protection System Command Line Interface Reference* for more information.

- **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 via 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

The following items provide clarification or describe issues fixed in this release.

Description	Reference
An issue that caused the management port on a 440T device to become unresponsive was resolved.	107000
Logged messages that were a **Warning** severity or lower were not sent as an SNMP trap. SNMP traps can now be sent for lower severity levels.	112524
When a notification contact was created locally and added to the **system.log**, the contact was incorrectly deleted after the SMS distributed a new profile.	112929

Known issues

This release contains the following known issues.

Description	Reference
Time changes and NTP synchronization When the device time is changed by a value greater than 1000 seconds, the NTP service stops, and the device no longer synchronizes the time with the environment. If the NTP service does stop, the following critical log message appears:	103644

Description	Reference
`Large clock discrepancy detected (> 1000s), NTP service stopping. Check clock and restart NTP service.` **Workaround:** Disable and re-enable the NTP service. This will cause the NTP server to synchronize with the time server(s) and may also change the time on the device. **Note:** When the device time is manually changed, NTP (if enabled) will eventually reset the time to be in sync with the time server(s).	
Link state and LDS mode If the link state is changed during the six-second link negotiation period, then the link down synchronization (LDS) mode might not be triggered. **Workaround:** To recover from this condition, restart the segment using the LSM or SMS.	103751
Incorrect address displayed in quarantine log When an IPv6 address is quarantined, the quarantine logs display the solicited node multicast address (ARP in IPv4) instead of the actual IPv6 address that is quarantined.	103981
Missing interface information in IPS logs The IPS log for the DDoS attack shows the interface information as `unknown`.	104275
440T shutdown On the 440T TPS only, after the device is shut down using the `shutdown` 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. This is not applicable to the 2200T TPS.	104878
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, first create one, then create the other. If you attempt to create a snapshot and a TSR with a snapshot at the same the time, XMSD errors are written to the System log.	107539, 112664
SSL issues with DDoS filters The SSL client fails to establish the SSL session intermittently when the IPS profile is configured with one or more DDoS filters.	108350

Description	Reference
Workaround: Do not use DDoS filters with the SSL inspection profile.	
Issue configuring a Reputation profile using the LSM and CLI Configuring a Reputation profile from the LSM or the CLI does not work properly. **Workaround:** Use the SMS to configure a Reputation profile.	108632
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
Software upgrade fails if interrupted The TPS does not support interrupted software upgrades. **Workaround:** Do not power off the device while it is performing a software upgrade. Apply software upgrades manually so that you can avoid running software upgrades when a loss of power is a concern. To view the status of a software upgrade, use the serial port.	109223
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 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. When enabling IDS Mode, change Performance Protection to "Always" mode for best results.	111159
ZPHA remains enabled after a reboot If you manually enable ZPHA bypass, for example, from the LSM by clicking **System > Settings > High availability > Zero-Power HA > Change > Bypass**, the TPS bypasses traffic properly. However, when you reboot the device, ZPHA is not disabled and the TPS incorrectly continues to bypass traffic.	111704

Description	Reference
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
DDos protection fails on SSL inspection ports If you have configured Advanced Distributed Denial of Service (DDoS) filters to protect against SYN floods, the TPS supports DDoS protection of the SSL server, but not on the ports where inspection of SSL traffic is performed. For example, suppose you have a server at 1.1.1.1 that responds to HTTP traffic on port 80 and HTTPS traffic on port 443. If you have configured SSL Inspection of the traffic on 1.1.1.1:443, and you have configured DDoS protection of 1.1.1.1, then you will get DDoS protection on 1.1.1.1:80, but not on 1.1.1.1:443.	111883
Inaccurate session count statistics The `debug np stats` command intermittently shows a large number for session count information. **Workaround:** When an active session is closed, the session count is decremented. If the session count was already set to `0` by the `clear` command, then the session count will incorrectly appear as a very large number.	111924
Issues removing and importing device certificates in PKCS12 format When you delete a device certificate that was imported in PKCS12 format, the associated CA certificate is not deleted. In addition, if you re-import the device certificate in PKCS12 format, a duplicate CA certificate is created. **Workaround:** When you delete a device certificate, use the CLI to manually delete the corresponding CA certificate. If necessary, delete any duplicate CA certificates.	112174
SSL inspection logs show Profile and Policy Information as Unknown When you delete an SSL inspection profile or policy, corresponding SSL connections continue to be inspected until the SSL connection closes, but the SSL inspection logs may incorrectly indicate that the SSL connections have an unknown profile or policy. **Workaround:** Disregard these entries. The device stops logging these connections after the SSL connections close.	112740

Description	Reference
When you unmanage a device that is configured to persist private keys on the SMS, the LSM incorrectly allows you to import private keys If a managed device is configured to persist its private keys on the SMS, when you unmanage the device, the device continues to persist private keys on the SMS. However, the LSM incorrectly allows you to import a private key into the device keystore as part of a PKCS12 certificate. **Workaround:** While the device is unmanaged and configured to persist private keys on the SMS, do not use the LSM to import PKCS12 certificates. If necessary, delete any private keys from the device keystore. As a workaround, re-manage the device and either use the SMS to import private keys or configure the device to persist private keys on the device keystore and then unmanage the device to import private keys. **Note:** When you unmanage a device, and the device is configured to persist its private keys on the SMS, the device continues to access its private keys from memory until you reboot the device.	113285

Contacting support

Contact the TippingPoint Technical Assistance Center (TAC) by using any of the following options.

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See *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.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro Incorporated. 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.

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 or registered trademarks of their respective owners. This document contains confidential information, trade secrets or both, which are the property of Trend Micro. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Trend Micro or one of its subsidiaries.

All other company and product names may be trademarks of their respective holders.

TippingPoint Threat Protection System Release Notes

Edition: October 2016

Publication Part Number: 5900-4152