Intrusion Prevention System Release Notes

Version 3.8.4

August 2016

This document contains release-specific information for the TippingPoint Intrusion Prevention System (IPS) TippingPoint Operating System (TOS). 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 IPS devices and associated 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

This release includes the following new features:

- The command `conf t host lsm disable` was added to the Command Line Interface (CLI). This command disables the LSM without disabling http or https.
- NTP and IPv6 auto-config mode can now be enabled at the same time.
- Several issues have been fixed. Descriptions for these fixed issues are described in the section *Resolved issues* on page 3.

Release restrictions

The following restrictions apply to this release.

TOS v3.8.4 and IPS devices

TOS v3.8.4 is available for the following TippingPoint devices.

Product name	HPE part number	Trend Micro part number
TippingPoint 660N	JC019A	TPNN0020
TippingPoint 1400N	JC020A	TPNN0023
TippingPoint 2500N	JC021A	N/A
TippingPoint 5100N	JC022A	N/A
TippingPoint 6100N	JC577A	N/A
TippingPoint S2600 NX	JC874A	TPNN0026
TippingPoint S5200 NX	JC824A	TPNN0029
TippingPoint S6200 NX	JC873A	TPNN0031
TippingPoint S7100 NX	JC644A	TPNN0034
TippingPoint S7500 NX	JC872A	TPNN0037

TOS v3.8.4 and Digital Vaccine (DV)

TOS v3.8.4 uses v3.2.0 DV packages.

TOS v3.8.4 and the Security Management Systems (SMS)

SMS-managed devices with TOS v3.8.4 installed must be managed with SMS v4.2.0 or later. The SMS must be updated before you use it to manage devices with TOS v3.8.4 installed. Refer to the SMS release notes for information about updating the SMS.

TOS v3.8.4 and NTP

The following restriction applies to N-series devices only: Enabling NTP and then switching to SNTP causes the SNTP feature to fail. After switching from the NTP feature to SNTP or the Manual/Internal Clock, reboot the device for the change to take effect. (107814)

Installation

All devices must be running a minimum of TOS v3.6.4 before they can be upgraded to TOS v3.8.4.

Before upgrading your device to the latest TOS, maximize the space on your device by removing old TOS versions and packet traces. This ensures a successful upgrade and allows for a TOS rollback, if necessary.

You can remove previous TOS versions using the SMS, the LSM, or the CLI. For complete information, refer to the corresponding documentation on the TMC, *https://tmc.tippingpoint.com/TMC/*.

Resolved issues

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

Description	Reference
When the Remote System Log action set was used, the port numbers that displayed in the syslog server were different than what displayed on the SMS.	106761
When inspecting traffic, filter 16261 incorrectly triggered packet inspection, which affected the device performance.	109252
A memory allocation issue caused the device to fail. This occurred when too many filters were enabled by category while both DV and Malware/Aux DV filters were installed. It is now possible to enable all filters in all categories, though this is not recommended as a best practice.	112128
Link Aggregation Control Protocol (LACP) packets were dropped when there was too much traffic on the device.	112635

Description	Reference
When the IPS was under extreme load conditions, the preservation of state could be lost. This caused the IPS engine to be bypassed for certain crafted evasion techniques. **Note:** See Product Bulletin #1061 for more information.	112904
When a packet was lost during high-bandwidth transfers that required software analysis, the engine put the flow of traffic into a state where it inspected every packet in the software for over a minute. This slowed down data transfer.	113002
An issue introduced in TOS v3.8.3 caused the IPS engine to incorrectly and silently drop traffic. This was more noticeable with UDP. **Note:** If you resolved this issue with an inspection bypass or a traffic management filter set to **Trust**, you can remove this workaround after you upgrade to TOS v3.8.4.	114012

Known issues

This release contains the following known issues.

Description	Reference
Slow LED blinking of an empty module slot during reboot When a module slot is empty, its LED blinks at a slower rate (every 3 – 4 seconds) than normal during a system reboot. **Note:** Do not leave slots empty for an extended period of time. Insertion of a blank module or I/O module ensures that the device is correctly cooled.	86301
RADIUS authentication issues • Certificate Notification — The LSM does not give an indication when no certificates are present on the device.	95399

Description	Reference
• Microsoft Windows servers and EAP-MD5 authentication — Certain versions of the Microsoft Windows server do not accept EAP-MD5 authentication. For information on enabling this authentication, refer to the Microsoft Knowledge Base: *http://support.microsoft.com/kb/922574/en-us*	
Remote authentication system-level settings and user access The system-level setting determines the protocol that is used to authenticate all remote users for remote servers (**System > Remote Servers** on the LSM). Even though a user can be configured with a specific remote authentication protocol (RADIUS or TACACS+), the system-level setting for remote servers will be used during authentication with the remote servers.	101704

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

Intrusion Prevention System Release Notes

Edition: August 2016

Publication Part Number: 5998-1406