Intrusion Prevention System Release Notes

Version 3.9.2

August 2017

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 who install, configure, and maintain 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 addresses the following issues:

- 117916 – INHA Layer-2 Fallback issue during a reputation update
- 118547 – INHA Layer-2 Fallback issue with particular RFC822 traffic
- 118022 – NTP incorrectly adjusted the system time
- 118875 – System log issue with Adaptive Filter Configuration (AFC)

For more information, see *Resolved issues* on page 4.

Release restrictions

The following restrictions apply to this release.

TOS v3.9.2 and IPS devices

TOS v3.9.2 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 v3.9.2 and DV packages

TOS v3.9.2 includes the Digital Vaccine (DV) 3.2.0.8983 package. After you install this TOS release, you should update the DV package to the latest version. For more information, see your product documentation on the TMC.

TOS v3.9.2 and the SMS

Use SMS v4.5.0 and later to manage a device with TOS v3.9.2 installed. When you plan your upgrade, you should install SMS v4.5.0 or later and then install TOS v3.9.2 on your managed devices.

⚠Warning! When SMS v4.4.0 (or earlier) is installed, do not install TOS v3.9.2 on your managed device.

For information about how to install a newer version of the SMS, see the *SMS Release Notes* on the TMC.

Supported transceivers and cables for TippingPoint I/O modules

The NX Series devices support the following I/O modules and bypass I/O modules for fiber and copper components.

⚠Warning! The use of other vendor devices could be detrimental to proper operation of the TippingPoint system.

Table 1. Supported transceivers for I/O modules

I/O module & part number	Transceiver part number	Transceiver name
6-Segment GbE SFP (TPNN0068)	TPNN0054	TippingPoint X126 1G SFP RJ45 Transceivers (Copper and Fiber)
4-Segment 10GbE SFP+ (TPNN0060)	TPNN0057 TPNN0058 TPNN0054	TippingPoint S136 10G SFP+ LC SR Transceiver TippingPoint S136 10G SFP+ LC LR Transceiver TippingPoint X126 1G SFP RJ45 Transceivers (Copper and Fiber)
1-Segment 40 GbE QSFP+ (TPNN0069)	TPNN0067	TippingPoint S146 40G QSFP+ SR4 850nm Transceiver

Table 2. Supported module cable

I/O module part number	Cable part number	Cable name
TPNN0069*	TPNN0212	TippingPoint 40G QSFP+ Active Optical Cable (AOC)

*When you use this I/O module with the listed cable, then transceiver TPNN0067 is not required. The transceiver is attached to the cable.

Installation

You can install TOS v3.9.2 only on devices with TOS v3.8.4 or later already installed.

Before you upgrade your device to the latest TOS, maximize the space on your device by removing outdated TOS versions and packet traces that are no longer required. This ensures a successful upgrade and allows for a TOS rollback, if necessary.

You can remove previous TOS versions by using the SMS, the LSM, or the command line interface (CLI). For complete information, refer to your product documentation on the TMC at *https://tmc.tippingpoint.com*.

Resolved issues

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

Description	Reference
INHA Layer-2 Fallback issue during a reputation update The device may have entered Layer-2 Fallback unexpectedly during a reputation update. This was due to a multi-processor timing issue during a reputation update that has been resolved in this release.	117916
INHA Layer-2 Fallback issue with particular RFC822 traffic The TOS v3.9.2 release corrects a problem that was introduced in TOS v3.9.1 where the device unexpectedly entered L2FB mode while inspecting particular RFC822 traffic. This issue also created `DP Watchdog` errors in the system log. The device now inspects RFC822 traffic properly.	118547

Description	Reference
NTP incorrectly adjusted the system time NTP incorrectly adjusted the system time and generated a lot of warning messages in the audit log. NTP now adjusts the system time properly.	118022
System log issue with Adaptive Filter Configuration (AFC) Under extreme load conditions, if adaptive filtering was unable to generate an event message for a defective filter, the system log may have incorrectly generated a lot of UDM warnings. The system log now properly creates warning messages for defective filters.	118875

Known issues

This release contains the following known issues.

Description	Reference
Do not connect to a NTP server by using the server hostname When your device is configured to connect to a NTP server by using the server hostname, when you reboot the device, the device no longer connects to the NTP server. To avoid this issue, always establish a NTP server connection by using the IPv4/IPv6 address of the NTP server.	118020
Issue with establishing an SSH session to the IPS security device When you establish an SSH session to the IPS security device by using OpenSSH version 7.2 (and later), the SSH client displays the following error: `Connection to ip_address port 22: DH GEX group out of range` By default, newer versions of OpenSSH no longer connect to the IPS security device because of an increase in the minimum number of bits that are required for the key exchange.	116548, 120500

Description	Reference
Workaround: To avoid this issue, update the key exchange algorithms on the SSH client computer to allow `diffie-hellman-group1-sha1` for compatibility with the IPS security device. For example, run the following command: `ssh -o KexAlgorithms=diffie-hellman-group1-sha1 <device_ip_address>`	
LSM connection issue with Microsoft Edge and Microsoft Internet Explorer The LSM may not connect to a TippingPoint IPS security device when using Microsoft Edge or Microsoft Internet Explorer. To resolve this issue, use the `conf t server tls` command to enable TLS v1.0 on the IPS security device or use the Mozilla Firefox browser. For more information, see the *IPS Command Line Interface Reference*.	117878

Product support

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

Legal and notice information

Edition: August 2017