



TippingPoint™ Intrusion Prevention System – Release Notes

Version 3.6.7

December 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.

Important: This TOS update only applies to IPS S Series (10, 110, and 330) 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](#) on page 1
- [Release considerations](#) on page 3
- [Installation](#) on page 3
- [Product support](#) on page 5

New and changed in this release

This release improves the overall security of the IPS security device and addresses the following issues:

Description	Reference
DV package installation issues	120751

Description	Reference
<p>When attempting to install a more current DV package, a Critical error was created in the System log because the /usr partition was almost full. In some cases, the installation would fail because there was not enough space available on the /usr partition.</p> <p>This TOS update allows you to install the most current DV package updates without error. To resolve this issue, the contents of the DV package are now stored in the /opt partition.</p> <p>Important: This TOS update is required to install DV package updates that are released on or after January 16, 2018.</p>	
<p>'show routes' command did not work</p> <p>The show routes CLI command displayed the following error message:</p> <pre>Routing display support not included</pre> <p>The show routes command now properly displays the contents of the routing tables.</p>	88527
<p>Scan/sweep filters would stop triggering</p> <p>Scan/sweep filters would stop triggering, even after other filters were disabled, and a reboot would only fix this issue temporarily. This issue was less likely to occur if the scan/sweep filters were set with a Block + Notify action set instead of a Permit + Notify action set. Scan/sweep filters now function properly.</p>	108666
<p>An snmpwalk of the TPT-POLICY MIB revealed a symbol error on instance 7</p> <p>The snmpwalk command revealed a symbol error on the TPT-POLICY MIB because instance 7 was not defined.</p> <p>There is no value associated with instance 7. To resolve this issue, the TPT-POLICY MIB has been updated to remove the instance.</p>	113170
<p>Common Vulnerabilities and Exposures (CVE)</p> <ul style="list-style-type: none"> • CVE-2016-2183 	116544

Release considerations

The following restrictions apply to this release.

TOS v3.6.7 and IPS devices

TOS v3.6.7 is available for the following TippingPoint devices.

Product name	HP part number
TippingPoint 10	JC184A
TippingPoint 110	JC186A
TippingPoint 330	JC187A

TOS v3.6.7 and Digital Vaccine (DV)

TOS v3.6.7 requires v3.2.x DV packages. DV v2.5.x is not supported.

This TOS release includes the DV 3.2.0.9046 package. The TOS v3.6.7 installation preserves the active DV package on the device when it is more current than the DV package included with this TOS release.

TOS v3.6.7 and the Security Management System (SMS)

To manage an IPS device that is running TOS v3.6.7, the SMS must be running v4.3.0 or later. Refer to the SMS release notes for information about updating the SMS.

Installation

This section provides TOS v3.6.7 installation instructions.

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

Before you install TOS v3.6.7, consider the following:

- Install TOS v3.6.7 on IPS S Series devices running TOS v3.1.4 or later.

Note: If, for some reason, you need to factory reset the IPS device, and your SMS is on v5.0.0 (or later), depending on the TOS version that was originally installed on the device, your upgrade path varies:

- A factory reset to TOS v2.5.x – Update the device to TOS v3.1.4 so that you can manage the device with the SMS. From the SMS, you can update the device to TOS v3.6.7. Keep in mind, SMS v4.6.0 (or earlier) is required to manage IPS devices that are running TOS v2.5.x.
- A factory reset to TOS v3.1.4 (or later) – Manage the device with the SMS. From the SMS, you can update the device to TOS v3.6.7.
- To ensure a successful TOS update, make sure that the following disk partitions have enough free space:
 - /usr – At least 20 MB of free disk space is recommended.

For information about how to increase the available space on the /usr partition, contact TippingPoint product support. See [Product support](#) on page 5.

- /opt – At least 150 MB of free disk space is recommended.

(Best Practice) Maximize the available space on the /opt partition by removing previous TOS versions and snapshots that are no longer required. You can remove previous TOS versions and snapshots 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>.

Tip: You can verify the available space on the /opt and /usr partitions by using the following methods:

- **From the CLI** – Use the `show health disk-space` command.
- **From the LSM** – Use **System Summary > Disk**.
- **From the SMS** – Use **Devices > Events > System Health**.
- The TOS installation preserves the active DV package on the device when it is more current than the DV package included with this TOS release.

Product support

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

Legal and notice information

© Copyright 2017 Trend Micro Incorporated. All rights reserved. TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. TippingPoint Reg. U.S. Pat. & Tm. Off. All other company and/or product names may be trademarks of their respective owners.

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 in any form or by any means, 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.

Edition: December 2017