TippingPoint

Intrusion Prevention System Release Notes

Version 3.6.5

September 2015

This document contains release-specific information for the Intrusion Prevention System (IPS) TippingPoint Operating System (TOS). The release notes describe new features and changes included in this TOS release. This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining HP TippingPoint IPS devices and associated devices.

Important: TOS V. 3.6.5 only supports the S10, S110, and S330 devices.

This document contains the following important information about the TOS V. 3.6.5 release:

Release restrictions

The following restrictions apply to this release.

TOS V. 3.6.5 and IPS devices

TOS V. 3.6.5 is available for the following TippingPoint devices.

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

TOS V. 3.6.5 and Digital Vaccine (DV)

TOS V. 3.6.5 requires V. 3.2.x DV packages. DV 2.5.x is not supported.

TOS V. 3.6.5 and the Security Management Systems (SMS)

SMS-managed devices with TOS V. 3.6.5 installed must be managed with SMS V. 4.1.0 or later. The SMS must be updated before you use it to manage devices with TOS V. 3.6.5 installed. Refer to the SMS release notes for information about updating the SMS.

Upgrading TOS

All devices must be running a minimum of TOS V. 3.6.1 before they can be upgraded to TOS V. 3.6.5.

Important: Before upgrading your device to the latest TOS, maximize the space on your device by removing old TOS versions, snapshots, and packet traces as well as performing a filter reset. This ensures a successful upgrade and allows for a TOS rollback, if necessary.

You can remove previous TOS versions using the SMS, the Local Security Manager (LSM), or the Command Line Interface (CLI). For complete information, refer to the product documentation on the HP TippingPoint Threat Management Center (TMC), https://tmc.tippingpoint.com/TMC/.

What's new in TOS V. 3.6.5

This release includes the following new features:

- The Tech Support Report (TSR) now contains a list of filters currently disabled by Adaptive Filter Configuration (AFC).
- The hostname is now displayed prior to the login screen in the IPS CLI.

This release also fixes several traffic, Reputation, Layer-2 Fallback, and administrative issues described in Resolved issues on page 2.

Resolved issues

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

Traffic passing and filter issues

The following traffic and filter issues were resolved in this release.

Description	Reference
The device stopped passing traffic on segment 1 after an upgrade to a previous release.	101305
The device would not pass traffic in wire mode on segments 3 or 4 if auto-negotiation was disabled.	100175

Description	Reference
Multiple filters fired with a Major severity in the event logs, but when the individual filter information was checked, the filter severity was stated as Critical.	104262
When a Reputation DV delta package was distributed to the device, filters that had been disabled by AFC were automatically re-enabled.	106046

Reputation issues

The following Reputation issue is resolved in this release.

Description	Reference
The device did not consistently block IPv4/IPv6 Reputation or user-defined entries.	105677
The device did not consistently block IPv4/IPv6 GEO based filters.	102452
IPv4/IPv6 Reputation events were inconsistent when using a Permit + Notify action set.	103487
The device did not follow reputation filter precedence if the IPv4/IPv6 traffic matched multiple filters. For instance, precedence would not be followed if the source IP matched one filter and the destination IP matched a different filter. If one of the filters had a blocking action set, then that filter took precedence, even if it was below a reputation filter with a permit action set.	101417
An error occurred while updating the hit cache. The severity of the issued log message was modified from `ERR` to `WARN`. Additional information is included in the log message.	106517

Layer-2 Fallback issues

Some devices could go into Layer-2 Fallback (L2FB) under rare circumstances.

Description	Reference
A process during SMS distribution was improved to keep the IPS from falling into L2FB because of a suspended task and a threshold failure.	106034
The device went into L2FB because of a race condition in the Threat Suppression Engine (TSE) while processing regular expressions.	106042

Administrative and allocative issues

The following system administrative fixes or improvements are included in this release.

Description	Reference

This issue specifically affected users located in the southern hemisphere. The device did not support southern hemisphere Daylight Savings Time calculations.
Solution: Two optional parameters were added to the `conf t timezone` command: `-beginDST` and `-endDST`. These parameters must be specified as a pair.
`conf t clock timezone`
`<zone>  Timezone. Type 'show timezones' for valid values.`
`-beginDST  Date & hour DST begins (mmddhh)`
`-endDST  Date & hour DST ends (mmddhh)`
Note: These values remain in effect until they are deleted. If these values are deleted, the internal default values (appropriate for the northern hemisphere) are used. To delete the user-defined starting and ending dates, use the `conf t timezone` command without specifying the optional parameters.
	106028

The following CVEs have been addressed in this release: • CVE-2015-0208 • CVE-2015-0209 • CVE-2015-0287 • CVE-2015-0288 • CVE-2015-0289 • CVE-2015-0293	106103 (CVE-2015-0208) 106047
After deleting a TOS rollback version, the entire TOS installation list became empty and would not allow you to remove any of the other TOS rollback versions.	106030
The TSR did not contain enough information about quarantines. The TSR now contains both the quarantine log and the list of devices currently quarantined at the time the TSR was generated.	96015
The management port of the IPS still responded to pings after the device was halted.	106031

Support information

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

Note: Have the following information about your product available:

- Serial number and/or software version for your product
- System logs or event logs if available for your product

Online support

Go to the HP TippingPoint Threat Management Center (TMC) at:

http://tmc.tippingpoint.com

Phone support

North America: +1 866 681 8324

International: +1 512 681 8324

For a list of international toll-free contact numbers, go to http://tmc.tippingpoint.com, click the **Support** tab in the left navigation panel, select the **Support Contacts** option, and then click **View All**.

HP website

For the name of the nearest HP authorized reseller, see the Contact HP Worldwide website:

http://www.hp.com/country/us/en/wwcontact.html

Legal and notice information

Intrusion Prevention System Release Notes

Publication Part Number: 5998-1406