Virtual Threat Protection System Release Notes

Version v4.2.0

Release date: March 2017

This document contains release-specific information for the TippingPoint Virtual Threat Protection System (vTPS). The release notes describe changes and new features included in this release. This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint vTPS appliances 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:

- Dual-mode deployment has been disabled. A vTPS device can be deployed only in IPS mode.
- There is no longer a separate user disk for storage. The v4.2.0 vTPS release introduces a single-disk architecture with a user disk partition.
- For the v4.2.0 of vTPS, the general performance requirement changed from three cores to two cores. Enhanced performance changed from four cores to three cores.
- You can configure more vTPS parameters, including IPv6 information, hostname and location, DNS name, and console type.
- When configuring RADIUS groups, you can now set the Authentication Protocol.
- You have the flexibility to upgrade inspection throughput from 500Mpbs to 1Gpbs.
- X.509 certificates can now be imported in addition to CA certificates.
- RHEL version 6 of a KVM host is no longer supported.

In addition, the v4.2.0 vTPS release inherits features of TPS v4.2.0, including:

- The ability to collect a client's true IP address.
- The ability to identify the HTTP URI and hostname information associated with an event.
- Enhanced SNMP support

Release considerations

The following restrictions apply to this release.

Trial Mode

You can initially deploy your vTPS device in Trial Mode. However, this mode uses a limited number of filters and is not used for deployment, other than for exploration and experimentation. Before you deploy the vTPS in a full production environment, use the unique vTPS certificate that TippingPoint sends you to upgrade to Standard Mode. For more information, refer to the *Virtual Threat Protection System Deployment Guide*.

After you upgrade the device to Standard Mode, you must also upgrade your Digital Vaccine (DV) package. For more information, see the "Install a Digital Vaccine" section of the *Local Security Manager User Guide*.

Upgrade from TOS v4.0.1

A vTPS with TOS v4.0.1 or TOS v4.0.2 installed cannot be upgraded to TOS v4.2.0. Instead, you must redeploy the device.

IPv6 Support

During deployment, the vTPS supports only IPv4. After the vTPS has been installed, however, you can configure IPv6 from the console.

TOS v4.2.0 and Digital Vaccine

TOS v4.2.0 uses SIG-VTPS_4.0.0_8917 Digital Vaccine (DV) packages.

TOS v4.2.0 and the Security Management System

For a Security Management System (SMS) to manage a device with TOS v4.2.0 installed, the SMS must be running v4.5.0 or later. The SMS must be updated before you use it to manage devices with TOS v4.2.0 installed. Refer to the SMS Release Notes for information about updating the SMS.

Maximum transmission unit size

The maximum transmission unit (MTU) size for sending packets or frames is fixed at 1500 for all hypervisors.

Resolved issues

The following items, grouped by category, provide clarification or describe issues fixed in this release.

Description	Reference
Link Down Synchronization now functions in Breaker and Wire mode in a virtual environment.	108844
The vTPS now supports a fresh install. Previously, attempts to perform an emergency software installation would fail when the package could not be verified.	112239
SMS no longer fails to distribute a reputation filter to the vTPS.	112589

Known issues

This release contains the following known issues.

Description	Reference
After performing a Suspend and Resume operation in a KVM deployment, a HEALTH-ALERT error message is generated in the system log. **Workaround**: This error message does not affect Suspend and Resume functionality and can safely be ignored.	107144
After a Suspend and Resume operation in a KVM deployment, the vTPS system time can be out of sync with the KVM host time. **Workaround**: To sync the time with the KVM host, reboot the vTPS device.	107768
With a KVM deployment, packet loss generally occurs in the bridge. Consequently, the vTPS does not register the loss and does not generate an `HA Performance Protection threshold exceeded` error in the System logs according to your packet loss notification settings.	109282
A factory reset does not reset the initial deployment parameter values, such as IP address, username, and password. **Workaround**: To change these values, you must deploy a new vTPS.	111553
VLAN translation is not supported on vTPS although the option is available on the CLI and LSM.	116825
References to external user disk can be ignored in a log-file summary. The vTPS device uses a single-disk architecture.	116998
Use of the `fips-mode-enable` command sends the vTPS device into recovery mode after rebooting. **Workaround**: Do not use the `fips-mode-enable` command with vTPS devices.	116881

Description	Reference
vTPS devices do not support ECDHE cipher suites. These suites are disabled by default.	116337
A user whose account has been disabled can still log in with a configured SSH key pair. **Workaround**: After disabling the user's account, delete the user's SSH private key.	113853

Product support

Get support for your product 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

Edition: March 2017