ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Trend Micro TippingPoint Threat Protection System (TPS) v5.2

Maintenance Update of Trend Micro TippingPoint Threat Protection System (TPS) v5.2

Maintenance Report Number: CCEVS-VR-VID10949-2019

Date of Activity: 06 November 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Trend Micro TippingPoint Threat Protection System (TPS) v5.2 Impact Analysis Report, Version 1.0, 15 October 2019
- NDcPP - collaborative Protection Profile for Network Devices, Version 2.0E + Errata 20180314, March

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Trend Micro TippingPoint Threat Protection System (TPS) v5.2 Security Target, Version 1.0, October 15, 2019	Changes in the maintained ST are: • The ST was updated to include the 2 additional appliance models and to update the software version to 5.2. • All document references were also updated to reference updated administrative guidance and the new version/date of the ST.
Guidance: The following documents are impacted: • Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide • Trend Micro TippingPoint Threat Protection System	Changes in the guidance are: • All legacy guidance was updated to reference the update to software version 5.2. • New features were described in the updated guidance as necessary; e.g., the installation guidance now references the installation procedures for the 1100TX

Command Line Interface Reference • Trend Micro TippingPoint Threat Protection System Install Your 440T and 2200T Security Devices • Trend Micro TippingPoint Threat Protection System Install Your 8200TX and 8400TX Security Devices • Trend Micro TippingPoint Virtual Threat Protection System (vTPS) Deployment Guide • Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.2	and 5500TX devices. Separate installation guidance was not produced for these devices because their physical characteristics are the same as existing models. • The vTPS guide was changed from "deployment guide" to "user guide" but this was a semantic change and does not relate to the TOE. • Aside from mentioning the updated TOE software and new TOE hardware models, there are no security-relevant changes to the CCECG.models.
Test: Trend Micro TippingPoint Threat Protection System (TPS) v5.2 Common Criteria Supplemental Testing For Network Device collaborative PP Version 2.0 IAR	A new copy of the test plan was generated for version 5.2 of the TOE. The TOE's functional claims did not change so all tests are the same as those that were used for the original evaluation, but the new 1100TX and 5500TX hardware models were used for the testing to demonstrate the proper function of the TOE on these new models.
Entropy: Trend Micro Inc. Trend Micro TippingPoint Entropy Documentation, Version 1.1, November 4, 2019	The Entropy Documentation was updated to include the 1100TX and 5500TX appliances, including captures of the amount of entropy in the entropy pool when the OpenSSL Crypto Core library is first loaded, demonstrating there is sufficient entropy in the pool when the DRBG is first instantiated. These results supplement the results already documented for the 8200TX, 8400TX, 2200T, 440T, and vTPS appliances.

Assurance Continuity Maintenance Report:

Leidos, submitted an Impact Analysis Report (IAR), for the Trend Micro TippingPoint Threat Protection System, to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 06 November 2019. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target, a supplemental Test Report, and the Impact Analysis Report (IAR). The ST was updated, the IAR and Test Report were new.

The changes to the ST concerned the introduction of the two new platforms as well as update to the TOE and TOE document version numbers, and updating a table of NIST certs

Changes to TOE:

For this Assurance Continuity, the following TOE updates were released:

Changes in Version 5.1.1	**Impact**
SSL inspection connection resets and errors have been addressed in this release.	**Minor change:** This function was not in scope of the original TOE.
The show np gen stat command now displays Invalid and Bypassed Counters in packet statistics.	**Minor change:** This function was not in scope of the original TOE.
Bypass packets/sec, Bypass to Rx ratio, VLANTrans to Rx Ratio and VLANTrans Packets/Sec are now available from the show np tier-stats command.	**Minor change:** This function was not in scope of the original TOE.
The show vlan-translations command now displays hit counts.	**Minor change:** This function was not in scope of the original TOE.
The show NTP command now displays the current NTP configuration.	**Minor change:** This function was not in scope of the original TOE.
A segmentation fault causing the device to enter layer-2 fallback has been corrected.	**Minor change:** This function was not in scope of the original TOE.
SNMP traps are now sent from TX with SNMP enabled when a Critical FAN or PSU alert occurs with the device.	**Minor change:** This function was not in scope of the original TOE.
False positives on filter 7120 are avoided by better handling of TCP keep-alive packets that were mistaken for overlaps.	**Minor change:** This function was not in scope of the original TOE.
An issue causing irregular character strings to appear in the audit log	**Minor change:** This behavior was not observed during completion of the required evaluation activities.

records under certain circumstances has been addressed.	
After performing a snapshot restore operation a full reboot now occurs to reset port properties.	**Minor change:** This function was not in scope of the original TOE.
If a port is disabled on an IO module, and then the IO module is hot swapped, the port is reset to the enabled state and now correctly passes traffic.	**Minor change:** This function was not in scope of the original TOE.
Even if a device is managed by SMS, a user can now execute the debug np regex clear command from the CLI.	**Minor change:** This is not applicable to the TOE because the SMS device is excluded from the evaluated configuration.
Changes in Version 5.2.0	**Impact**
The TPS TX Series is expanded to include the 1100TX and 5500TX models. These models extend the existing 440T and 2200T TPS capabilities with I/O modular functionality and increased throughput.	**Minor change:** The TPS1100TX and 5500TX devices feature the same architecture as the 8200TX and 8400TX models, but with fewer number of I/O modules. The actual product functionality of these models is identical to those that were tested as part of the original evaluation of the TOE.
The 40 GbE Fiber Bypass I/O module is introduced. By using this bypass I/O module, users can deploy TX devices on a 40 GbE network without any concerns of breaking the network in the event of a device failure.	**Minor change: T**he ST, bypass modules were not considered part of the evaluated configuration. Therefore, the introduction of a new type of bypass module is similarly outside the scope of the TOE.
New QSFP+ transceivers enable nonadjacent TPS 8200TX or 8400TX devices to be stacked at greater distances with comparable throughput rates.	**Minor change:** This function was not in scope of the original TOE.
Support is now provided for fixed ethtype inspection bypass that addresses Link Aggregation Control Protocol issues.	**Minor change:** This function was not in scope of the original TOE.
For 8200TX and 8400TX devices, VXLAN inspection support is now INI-configurable for UDP ports 4789, 8472, and 48879.	**Minor change:** This function was not in scope of the original TOE.

TPS administrators can now use the SMS as a remote authentication server.	**Minor change:** This update is not applicable to the TOE because the use of the SMS device is excluded from the evaluated configuration.
Selective acknowledgement now improves profile distribution times across remote or otherwise burdened networks.	**Minor change:** This function was not in scope of the original TOE.
vTPS devices support an inspection capacity of 2 Gbps (license required) for both Normal mode and Performance Mode.	**Minor change:** This function relates to network throughput, which is not relevant to the claimed Protection Profile.
Users are now warned when their CLI session has been idle too long and that they will be forcibly disconnected.	**Minor change:** This function relates to FTA_SSL_EXT.1 and FTA_SSL.3 in the claimed PP, but because the PP does not require a notification prior to initiating the session termination, this function does not change any of the security claims made by the TOE.
When the state of a stacking port changes—inserted or removed, moved up or down—an entry is recorded in the system log.	**Minor change:** This function was not in scope of the original TOE.
The device no longer generates an unexpected unchunking sequence derived message.	**Minor change:** This function was not in scope of the original TOE.
A condition that caused segment ports to disappear after an attempt to install a KVM-deployed vTPS without the correct number of data ports has been repaired.	**Minor change:** This function was not in scope of the original TOE.
Issues that caused filters to trigger on inapplicable traffic have been resolved.	**Minor change:** This function was not in scope of the original TOE.
A discrepancy in the general stats no longer occurs when a filter blocks an ICMP fragmented packet.	**Minor change:** This function was not in scope of the original TOE.
Manual restart is no longer required when inspection ports configured for Link Down Sync (LDS) Wire mode become disabled after an LDS event.	**Minor change:** This function was not in scope of the original TOE.
A best effort mode issue that could result in increased latency and reduced throughput without packet loss no longer occurs.	**Minor change:** This function was not in scope of the original TOE.

The SMS would send the "Any IP Address" Host IP filter to the device if a user deleted all IP filters. This caused TPS devices to crash. The SMS no longer permits users to delete the named resource if any entities are using it.	**Minor change:** The use of SMS was excluded from the evaluation scope so this issue does not relate to the TOE.
The yellow stacking LED now works correctly on 8200TX and 8400TX devices.	**Minor change:** This function was not in scope of the original TOE
A condition that caused the Module Health LED to turn green prematurely has been repaired.	**Minor change:** This function was not in scope of the original TOE
New TCAM scripts and a new FPGA image are provided to address a TCAM issue that caused TPS devices to enter Layer-2 Fallback.	**Minor change:** This function was not in scope of the original TOE.
An invalid process control block pointer is prevented from occurring, which caused TX devices to fail.	**Minor change:** This function was not in scope of the original TOE.
New inner tunnel limits prevent a cross-packet inspection issue.	**Minor change:** This function was not in scope of the original TOE.
Can now verify that the device and NTP server times are synced using the show ntp command.	**Minor change:** NTP was not part of the evaluation scope so this issue does not relate to the TOE.
Hovering the mouse over a filter name in Block/Alert logs no longer displays a 501 filter loading error.	**Minor change:** This function was not in scope of the original TOE.

No functionality, as defined in the SFRs, was impacted, and none of the software updates affected the security functionality or the SFRs identified in the Security Target. In addition, while the addition of the two new appliances required the introduction of new processors (an *Intel Pentium D-1517* in the 1100TX and an *Intel Xeon D-1559* in the 5500TX, each with a *Broadwell microarchitecture*), they are both *Intel x86* processors that use an extended version of the *Haswell microarchitecture* instruction set used in the original evaluation. The new processors are equivalent in cryptographic functionality as demonstrated by CAVP testing.

All updates are, therefore, considered to be Minor Changes.

Regression Testing:

Regression testing was performed on the two new Tipping Point devices. The test cases verified that software updates had no security-relevant impact, that the two devices generated the correct results, and did not affect the security functionality defined in the Security Target. The TOE was received from the vendor and configured according to the guidance documents. Both new appliances were tested according to the Assurance Activities contained in the NDcPP. Testing took place at Leidos in Columbia MD, from 8/19-9/24/2019. The overall testing verdict was that Trend Micro TPS 5.2 passed.

The results of testing were contained in a supplemental Test Report. The report was reviewed and considered acceptable.

NIST CAVP Certificates:

CAVP certificate #C1262 was obtained for the 1100TX and 5500TX. Specific information about that certificate is contained in the Impact Analysis Report.

Vulnerability Analysis:

The evaluation team conducted a public search for vulnerabilities that might affect the TOE on October 4, 2019. The results were compared to the original vulnerability analysis document, dated November 30, 2018.

The Search Terms used included:

- "TippingPoint"
- "threat protection"
- "TCP"
- "SSH"
- "openssh"
- "openssl"
- "linux (kernel)"

All issues (e.g., CVEs) located were confirmed as not directly effecting the TOE.

In summary, no residual vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the updated version of the TOE.

Conclusion:

Since none of the updates to the TOE changed the functionality and the testing produced the correct results, the overall update to the TOE can be considered Minor. A new CAVP certificate was awarded and an updated Vulnerability search was done that found that no unremediated vulnerabilities existed.

Therefore, CCEVS agrees that the original assurance is maintained for the product.