CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Trend Micro TippingPoint Threat Protection System (TPS) v6.5

Maintenance Report Number: CCEVS-VR-VID11488-2026

Date of Activity: June 2, 2026

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [NDcPP]

Trend Micro TippingPoint Threat Protection System (TPS) v6.5 Impact Analysis Report, Version 1.1, June 2, 2026

Trend Micro TippingPoint Threat Protection System (TPS) v6.4 Security Target, Version 1.2, April 07, 2025

Common Criteria Evaluated Configuration Guide (CCECG) for TPS v6.4 Trend Micro TippingPoint Threat Protection System, Document Version 1.2, April 2025

Trend Micro™ TippingPoint™ Threat Protection System Release Notes Version 6.5.0

Affected Evidence:

Trend Micro TippingPoint Threat Protection System (TPS) v6.5 Security Target, Version 1.3, January 6, 2026

Common Criteria Evaluated Configuration Guide (CCECG) for TPS v6.5 Trend Micro TippingPoint Threat Protection System, Document Version 1.3, January, 2026

Updated Developer Evidence:

This assurance maintenance request is to update the TOE hardware and virtual appliances to include an additional device model and incorporate software updates and bug fixes since the previous Assurance Maintenance activity in June 2025. The developer has provided sufficient supporting rationale describing the impact of this change. The Security Target and Common Criteria Evaluated Configuration Guide were updated to identify the additional TOE hardware model and updated TOE version.

Description of ASE Changes:

Leidos submitted an Impact Analysis Report to CCEVS, on behalf of Trend Micro for approval to update the Trend Micro TippingPoint Threat Protection System TOE. The updates include:

- Introduction of the new TPS 5600TXE device model running TPS Software version 6.5 to the TOE product line.
- Updating the TOE's Threat Protection System (TPS) software from version 6.4 to version 6.5 to incorporate new/updated non-security relevant features and bug fixes.

As a result, the Security Target and Common Criteria Evaluated Configuration Guide documents were changed to reflect the new TOE hardware model and updated TPS software version.

Changes to TOE:

The TPS software was updated from v6.4 to v6.5 on all TOE hardware appliances, including the added TPS 5600TXE, and the vTPS virtual appliances. This update does not modify any of the third-party libraries or SFRs. The software updates included 1 new feature and 10 bug fixes/updates. The updates are summarized below.

- 1 new TOE device model, the TPS 5600TXE, expands the TXE-Series TPS devices. Existing TXE-Series functionality is unchanged. The TPS 5600TXE appliance is equivalent to the 8600TXE and 9200TXE appliances already included in the TOE boundary. The changed TOE consists of the following appliances running TPS software v6.5 (bold is new TOE device model):
    - TPS 1100TX
    - TPS 5500TX
    - **TPS 5600TXE**
    - TPS 8200TX
    - TPS 8400TX
    - TPS 8600TXE
    - TPS 9200TXE
    - vTPS.
- 1 new feature is related to stacking interconnect options. Stacking configurations are not included in the evaluated configuration and therefore does not affect the TOE.
- 10 bug fixes/updates are related to performance, boot process, storage/disk management, network monitoring, configuration/management, and upgrade/migration.

These changes either do not affect the security functionality of the TOE or are outside of the scope of the evaluated configuration.

Description of Documentation Changes:

1. Security Target – The Security Target has been updated to identify the new TOE device model and software version. No other changes were necessary to the Security Target as this change was minor and did not impact the ST.
2. Common Criteria Evaluated Configuration Guide – Common Criteria Evaluated Configuration Guide was updated to identify the new TOE device model and software version. No other changes were necessary to the Common Criteria Evaluated Configuration Guide as this change was minor and did not impact the ST.

Assurance Continuity Maintenance Report:

- Leidos submitted an Impact Analysis Report (V1.1), on behalf of Trend Micro to update the TOE TPS software from version 6.4 to 6.5.
- Updates consist of support for one new TOE device model in addition to software updates and bug fixes.
- There are no security relevant fixes, so no new certification is required.
- No development environment changes occurred that impacted the product.
- There were no changes that required the evaluators to do any additional testing.

Description of Regression Testing:

Vendor regression test results were produced and found consistent with the previous test results. Trend Micro performs extensive regression testing for every release including v6.5. Trend Micro conducts automation test suites and performs manual testing.

CAVP Analysis:

The Crypto Module included with Trend Micro TippingPoint Threat Protection System (TPS) is the same between versions 6.4 and 6.5. The cryptographic implementation remains the same for the Trend Micro TippingPoint Threat Protection System (TPS) v6.5 (A5111).

Vulnerability Assessment:

The public vulnerability search covers the period between the previous assurance maintenance search on 6/11/2025 and the updated search performed on 6/2/2026. The evaluator searched the following public vulnerability databases:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search) **Note:** the NVD implicitly performs a search of the CISA KEV as recent updates to the NVD indicate if there is CISA KEV data for the CVE.
- US-Cert (https://www.kb.cert.org/vuls/html/search)
- Tipping Point Zero Day Initiative (https://www.zerodayinitiative.com/advisories/published/)
- OpenSSL Vulnerabilities 3.0 (https://openssl-library.org/news/vulnerabilities-3.0/index.html)

with the following search terms:

- The list of software and hardware components that compose the TOE:
  - Processor:
    - Intel Pentium D1517
    - Intel Xeon D-1559
    - Intel Xeon E5-2648L v3
    - Intel Xeon Gold 5318N
    - Intel Xeon D-2753NT (new search term covering processor used in the 5600TXE device added in this assurance maintenance activity)
    - Broadwell microarchitecture
    - Haswell microarchitecture
    - Ice Lake microarchitecture
  - Software:
    - Linux 5.4
    - Yocto
    - Net-SNMP 5.8
    - OpenSSH 8.2
    - OpenSSL 3.0.9
- "Trend Micro", "TippingPoint", "TPS", and "Threat Protection System" as variations of the TOE name.

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. No vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the software minor version update.

Vendor Conclusion:

The specific changes made to the firmware version do not affect the security claims in the Trend Micro TippingPoint Threat Protection System (TPS) v6.5 Security Target, Version 1.3, January 6, 2026.

This update results in no changes to SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment and therefore is a **minor** change. The security target and the Common Criteria Evaluation Guidance Document have been updated to reflect the firmware version update.

As a part of the maintenance activity, support for an additional TOE appliance model, the 5600TXE, was introduced. The 5600TXE appliance is functionally equivalent to previously evaluated TOE models, as it executes the same TOE software and implements identical security functionality on the same microarchitecture (Ice Lake) as an evaluated model processors i.e., 8600TXE and 9200TXE. No changes to the TOE security architecture, security requirements, or assurance measures were required because of this addition.

Vendor regression test results were produced and found consistent with the previous test results. Trend Micro performs extensive regression testing for every release including v6.5. Trend Micro conducts automation test suites and performs manual testing.

The cryptographic implementation remains the same for the Trend Micro TippingPoint Threat Protection System (TPS) v6.5 (A5111).

Finally, the evaluation security team searched the public domain for any new potential vulnerabilities that may have been identified since the completion of the previous maintenance activity. The search did not identify any new potential vulnerability for the maintained TOE version.

Validation Team Conclusion:

The validation team reviewed the changes and concurred the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The Security Target and Common Criteria Evaluated Configuration Guide changed to add the new TOE device model and update the TOE TPS software version.

Based on this and other information from within the IAR document, the Validation Team agrees that the assurance impact of these changes is minor.