CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Trend Micro TippingPoint Threat Protection System (TPS) v6.4

Maintenance Report Number: CCEVS-VR-VID11488-2025

Date of Activity: June 11, 2025

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) v6.4 Impact Analysis Report, Version 1.2, June 11, 2025

Trend Micro TippingPoint Threat Protection System (TPS) v6.4 Security Target, Version 1.2, April 7, 2025

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

Affected Evidence:

Trend Micro TippingPoint Threat Protection System (TPS) v6.3 Security Target, Version 1.0, September 23, 2024

Common Criteria Evaluated Configuration Guide (CCECG) for TPS v6.3 Trend Micro TippingPoint Threat Protection System, Document Version 1.0, September 2024

Updated Developer Evidence:

This assurance maintenance request is to update the TOE hardware and virtual appliances to incorporate software updates and bug fixes. 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 new 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 TOE's Threat Protection System (TPS) software was updated from version 6.3 to version 6.4 to incorporate new/updated features and bug fixes. As a result, the Security Target and Common Criteria Evaluated Configuration Guide documents were changed to reflect the updated TPS software version.

Changes to TOE:

The TPS software was updated from v6.3 to v6.4 on the TOE hardware appliances and the vTPS virtual appliances. None of the hardware appliances running the updated TPS software v6.4 were changed or modified. This update does not modify any of the third-party libraries or SFRs. The updates included 3 new and 2 updated non-security relevant features and 13 bug fixes. The updates are summarized below.

- 3 new features are related to reputation filtering, traffic inspection, and performance.
- 2 updated features are related to port configuration and license utilization.
- 13 bug fixes are related to the reliability of power, networking functionality/availability, multi-threaded processing, compatibility, and boot process.

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 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 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 (V1.2), on behalf of Trend Micro to update the TOE TPS software from version 6.3 to 6.4.
- Updates consist of 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 v6.4. Trend Micro conducts automation test suites and also performs manual testing. The Trend Micro regression testing verified the correct functionality of all of the hardware appliances and the vTPS virtual appliances.

CAVP Analysis:

The Crypto Module included with Trend Micro TippingPoint Threat Protection System (TPS) is the same between versions 6.3 and 6.4. The CAVP certificates remains applicable in the Trend Micro TippingPoint Threat Protection System (TPS) v6.4 (A5111).

Vulnerability Assessment:

The public vulnerability search covers the period between the original evaluation search on 12/4/2024 and the updated search performed on 6/11/25. The evaluator searched the following public vulnerability databases:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- 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:

- Intel Pentium D1517
- Intel Xeon D-1559
- Intel Xeon E5-2648L v3
- Intel Xeon Gold 5318N
- Broadwell microarchitecture
- Haswell microarchitecture
- Ice Lake microarchitecture
- Linux 5.4
- Yocto
- Net-SNMP 5.8
- OpenSSH 8.2
- OpenSSL 3.0.9
- “Trend Micro”
- “TippingPoint”
- “TPS”
- “Threat Protection System”

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 software version do not affect the security claims in the Trend Micro TippingPoint Threat Protection System (TPS) v6.4 Security Target, Version 1.2, April 7, 2025.

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 are updated to reflect the software version update.

Vendor regression test results were produced and found consistent with the previous test results. Trend Micro performs extensive regression testing for every release including v6.4. Trend Micro conducts automation test suites and also performed manual testing.

The cryptographic implementation remains the same for the Trend Micro TippingPoint Threat Protection System (TPS) v6.4 (A5111). The cryptographic module is unmodified and is applicable to the updated TOE.

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 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.