ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Trend Micro TippingPoint Threat Protection System (TPS) v5.5

Maintenance Update of Trend Micro TippingPoint Threat Protection System (TPS) v5.3

Maintenance Report Number: CCEVS-VR-VID11206-2023

Date of Activity: September 1, 2023

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) v5.5 Impact Analysis Report v1.0, 3 August 2023[IAR].
- collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020 [CPP_ND_V2.2E]

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: • Trend Micro TippingPoint Threat Protection System (TPS) v5.3 Security Target, version 1.0,1 Jan 2022	**Maintained Security Target:** Trend Micro TippingPoint Threat Protection System (TPS) v5.5 Security Target, version 1.0, July 14, 2023 Changes in the maintained ST are: • Updated identification of ST • Section 1.1 - Updated TOE software version and ST title. • Section 2 - Updated the TippingPoint Threat Protection System version number. • Section 2.1 - Updated the TippingPoint Threat Protection System version number.

	• Section 2.2.1 - Updated the TippingPoint Threat Protection System version number. • Section 2.3 – Identified the most current documentation for the current TippingPoint Threat Protection System v5.5.4
Common Criteria Guidance Documentation • Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide, September 2020 • Trend Micro TippingPoint Threat Protection System Command Line Interface Reference, November 2019 • Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide, June 2019Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide, October 2021 • Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.3, 1 January 2022.	**Maintained Common Criteria Guidance documentation:** • Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide, September 2020 • Trend Micro TippingPoint Threat Protection System Command Line Interface Reference, November 2021 • Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide, October 2021 • Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.5, 14 July 2023. Changes in the maintained Guidance are: • Updated identification of Guidance • Updated identification of References • Updated identification of TOE version

	• All the changes documented in this report corresponding to the updates to the TOE.

Assurance Continuity Maintenance Report:

Trend Micro, submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on August 3,2023. 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 maintained TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence consists of the Security Target, the CC Configuration Guide, guidance documentation and the Impact Analysis Report (IAR) . The ST and guidance documentation were updated, the IAR documented the changes from the previously maintained version of the TOE (Version 5.3) to the updated TOE(Version 5.5).

Changes to TOE:

For this Assurance Continuity, the version number of TOE changed from Version 5.3 to Version 5.5.

Software Enhancements

The following paragraphs list the new features introduced in version 5.4 that required minor software changes made to the TOE during the maintenance cycle. The developer reported the new features/changes to the product located in the table below:

TOS v5.4.0, TPS devices provide in-line, real-time threat protection for both inbound server SSL traffic and outbound client SSL traffic. **Impact: Minor** **Rationale:** The new feature does not affect any of the claimed security functionality.
TOS v5.4.0 includes support for the TLSv1.3 protocol and six new cipher suites, including TLSv1.3-specific ciphers. **Impact: Minor** **Rationale:** The new feature does not affect any of the claimed security functionality.
The debug congestion visibility command has been added so you can view how uninspected traffic correlates to any systems or applications that might have been having issues during the congestion period. **Impact: Minor** **Rationale:** This new view command improves the usability of the TOE without affecting security functionality.
A new ipsprefs option has been added to the display conf running command that enables device configuration information (except policy settings) to be displayed. **Impact: Minor** **Rationale:** This new view command improves the usability of the TOE without affecting security functionality.

Bug Fixes

There were several bug fixes that were addressed as part of release 5.3.1 through release 5.5.4. None of the bug fixes resulted in changes to the ST or the Common Criteria Evaluated Configuration Guide. Also, the changes made to the TOE as part of the bug fixes did not have any effect on the result of any Assurance Activities. The details of the bug fixes are documented in the proprietary IAR provided to the validation team.

Regression Testing:

In addition to the vendor performing vulnerability analysis, functional regression testing was also performed against the updated TOE to ensure the TOE functionality is maintained and that the source code is fit for use. This functional testing included verification that any newly introduced

feature does not affect the security functionality previously tested and verified. This testing ensured that the functionality claimed within the Security Target has not been impacted by any software changes made to the product between releases.

For instances when security related bugs or general defects were identified, the vendor performed specific testing on the updates to ensure that the identified behavior is no longer present within the TOE and the TOE operates as expected.

NIST CAVP Certificates:

No changes to the CAVP certificates from the previously evaluated version of the TOE.

Vulnerability Analysis:

A public search for new vulnerabilities that might affect the TOE since the evaluation was completed was performed. In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the firmware minor version update.

The vulnerability search was performed on the Trend Micro TPS product that is posted on the NIAP Product Compliant List web pages.

- CCEVS-VR-VID11206-2022- Trend Micro TippingPoint Threat Protection System TPS) v5.3. Certificate Date: 2022.02.02

The original search terms and results for the evaluation listed above have been provided below as well as the results of a new search performed on 7/5/2023.

An updated search was performed on 8/3/2023 going back through to the last time the search was run on 7/5/2023. The NVD CVE website keyword search option was disabled and therefore the search was performed using CPE with vendor, product, version. In cases where Product or Version were not available selections, "Any" was selected. No results were returned related to the components used in the TOE. Additionally, for searches under kb.cert.org – no new results were found.

Databases used for the searches:

- http://web.nvd.nist.gov/view/vuln/search
- http://www.kb.cert.org/vuls/html/search

These search criteria were applied as follows:

- The list of software and hardware components that compose the TOE:
  - Processor:
    - Intel Pentium D-1517
    - Intel Xeon D-1559
    - Intel Xeon E5-2648Lv3
    - Broadwell microarchitecture (search term "Broadwell")

        - Haswell microarchitecture (search term “haswell”)
    - Software:
        - Linux-4.14.76-yocto-standard (search terms: “Linux”, “Yocto”)
        - OpenSSL 1.0.2l-fips (search term “openssl”)
- “Trend Micro”, “TippingPoint”, “Threat Protection System”, and “TPS” as variations of the TOE name.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. 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. Therefore, CCEVS agrees that the original assurance is maintained for the product.