MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

M024 Assurance Maintenance Report Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0

File name: ISCB-5-RPT-M024-AMR-v1
Version: v1
Date of document: 16 April 2026
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

M024 Assurance Maintenance Report

Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0

16 April 2026

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor, Malaysia
Tel: +603 8800 7999 | Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	M024 Assurance Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M024-AMR-v1
ISSUE:	v1
DATE:	16 April 2026
DISTRIBUTION:	CONTROLLED COPY - FOR LIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor, Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 200601006881 (726630-U)

Printed in Malaysia

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	6 April 2026	All	Initial draft
v1	April 2026	All	Final version

Table of Contents

Document Authorisation ii

Copyright Statement iii

Document Change Log iv

Table of Contents v

1 Introduction 1

2 Description of Changes 4

2.1 Changes to the product associated with the certified TOE 4

3 Affected Developer Evidence 8

4 Result of Analysis 12

Annex A References 13

1 Introduction

1 The TOE is Trend Micro TippingPoint Threat Protection System (TPS), v6.5.0. The TOE is a network security platform that offers threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks.

2 The TPS version 6.5.0 appliances included in the evaluation are the physical devices TPS 1100TX, TPS 5500TX, TPS 8200TX, TPS 8400TX, TPS 5600TXE, TPS 8600TXE, TPS 9200TXE, and the virtual vTPS device. Each physical appliance includes an RJ-45 console port and a 1 GbE copper management port. The 8200TX, 5600TXE, 8400TX, and 8600TXE devices are high-end systems that are designed for network environments requiring up to 40 Gbps of inspection throughput. The 9200TXE device is for even higher-end environments requiring up to 100 Gbps of inspection throughput. The 1100TX and 5500TX devices support the same I/O modules as the 8200TX and 8400TX so these models can support the same capacity on a per-module basis, but they have fewer module slots for a reduced overall performance capacity. The 5600TXE, 8600TXE and 9200TXE have their own set of supported I/O modules for increased throughput. The concept of I/O modules is not applicable to the vTPS model which has two virtual data ports.

3 The vTPS model is a virtual appliance supported on VMware ESXi and KVM. Each virtual platform supports a virtual serial console and virtual Ethernet management port. Each virtual appliance provides 2 Gbps IPS inspection throughput with six vCPUs. Each vTPS supports one vNIC (VMware) or one bridge interface (KVM) for management

4 All models (hardware and virtual) provide the same security protections and support all the functionality specified in this ST.

5 The TOE uses NIST validated cryptographic algorithms and must be configured to operate in FIPS mode to ensure the use of the NIST validated cryptographic library.DD Inspector – a network appliance that monitors all ports and over 100 different network protocols to discover advanced threats and targeted attacks.

6 The TOE implements security functions such as security audit, cryptographic support, identification and authentication, security management, protection of the TSF, TOE access, trusted path/channels and intrusion prevention system.

7 MyCB has assessed the Impact Analysis Report (Ref [1]) according to the requirements outlined in the document Assurance Continuity: CCRA Requirements (Ref [4])

8 This is supported by the evaluator's verification test plan report (Ref [10]).

9 The purpose of this document is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner against the certified and updated version of the TOE as in Table 1 identification below.

Table 1 – Identification Information

Assurance Maintenance Identifier	M024
Project Identifier	C140
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0 Impact Analysis Report (IAR), Version 1.3 14 April 2026
New TOE	Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0
Certified TOE	Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0
New Security Target	Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0 Security Target, Version 1.2 01 April 2026
Evaluation Level	EAL2
Evaluation Technical Report (ETR)	Evaluation Technical Report – TippingPoint Security Threat Protection System (TPS) v6.4.0, V1.0, 19 May 2025
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC:2022, Revision 1, November 2022 Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, CC:2022, Revision 1, November 2022 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, CC:2022, Revision 1, November 2022 Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements, CC:2022 Revision 1, November 2022 Assurance Continuity: CCRA Requirements version 3.1, 29 February 2024
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CC:2022, Revision 1, November 2022

Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL2
Protection Profile Conformance	None
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive Columbia, MD 21046, USA
Developer	Trend Micro Inc 11305 Alterra Parkway, Austin, Texas 78758, USA
Evaluation Facility	Securelytics SEF A-17-01, Tower A, ATRIA SOFO Suites, Jalan SS 22/23, Damansara Utama, 47400 Petaling Jaya Selangor, Malaysia.

2 Description of Changes

10 Trend Micro has issued a new release which is Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0. There were a series of minor updates to the Trend Micro TippingPoint Threat Protection System (TPS) since its certification version 6.4.0 on 09 June 2025.

2.1 Changes to the product associated with the certified TOE

11 The following features have been added in Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0. The details changes have been documented in the Impact Analysis Report (IAR).

Table 2 – General changes/additions

Version	Description of Changes	Rationale	Impact
Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0	[New Feature] The TOE version has been updated to v6.5.0. This release expands TXE Series TPS devices to include the new TPS 5600TXE model.	The added device does not affect the Security Functional Requirements (SFRs) of the TOE. The new TPS 5600TXE appliance serves as a supporting hardware on which the TOE is provisioned, and as such, changes to the underlying hardware platform do not impact the TOE's security functionality or its compliance with the defined SFRs. The evaluator has performed verification testing to confirm that the SFRs continue to be met and function as intended on the new hardware platform.	Certification Body consider it as **Minor**
	[New Feature] The TOE version has been updated to v6.5.0. This release allows for additional stacking interconnect options for TXE devices. 200GbE QSFP-DD discrete transceivers with MPO16	The updates do not affect the SFRs of the TOE as it has been reflected to be out-of-scope.	Certification Body consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	cables can now be used to stack devices where the distance between devices is further than fixed Active-Optical-Cables allow. Lower bandwidth stacking interconnect options are also supported for lower-bandwidth stacking configurations, including discrete 100GbE QSFP28 transceivers with MPO12 cables, discrete 40GbE QSFP+ transceivers with MPO12 cables, and 40GbE QSFP+ Active-Optical-Cables. Refer to the updated Stacking User Guide document to compare stacking interconnect to configuration guidance.		
	[Bug Fix] The TOE version has been updated to v6.5.0. An issue was fixed that prevented upgrades from TOE OS v6.3.0 to v6.4.0. This issue only occurred in rare configurations with a very large numbers of domain reputation entries and rules.	The updates do not affect the SFRs of the TOE because they only correct a software upgrade defect and do not introduce changes to the TOE's security functionality.	Certification Body consider it as **Minor**
	/Bug Fix] The TOE version has been updated to v6.5.0. Users no longer have to delete the stack and re-create it to change resilience and SRD values when editing a stack name.	The fix does not impact the TOE's SFR, as it pertains solely to non-security administrative functionality.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0.	The fix does not affect the SFRs of the TOE as they address a non-security related storage	Certification Body consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	An issue that caused the TPS external disk to fill up prematurely with telemetry package files has been fixed.	management issue and do not alter the TOE's security functionality or security policy enforcement.	
	[Bug Fix] The TOE version has been updated to v6.5.0. A discrepancy has been fixed between SNMP data types that TPS devices respond with and what is defined in the MIB files.	The fix does not impact the TOE's SFRs. As it corrects a data type inconsistency in SNMP responses and does not alter the TOE's security functionality.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. The delete trust default-ca command has been fixed so that default CA certificates can be disabled for inbound SSL Inspection when building the certificate chain. Any default CA certificates that were previously disabled using the command will now be removed as expected.	The fix restores the intended operation of CA certificate management within the SSL inspection process. It does not alter the TOE's security boundary, cryptographic algorithms, trust model, or claimed SFR implementations, but ensures proper enforcement of existing security configuration controls.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. An issue with an internal device has been fixed. In rare occurrences, an internal device would not shutdown properly during a reboot, which caused the device to go into and remain in Layer-2 Fallback (L2FB) mode.	The fix improves system stability during reboot operations but does not alter the TOE's SFRs implementations.	Certification Body consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	[Bug Fix] The TOE version has been updated to v6.5.0. This release fixes an issue where the device went into L2FB when using HTTP2 inspection in a high-traffic environment.	The fix improves reliability of the HTTP2 inspection function under high load but dies not introduce new security functionality or change any claimed Security Functional Requirements (SFR) implementations.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. An issue where the show health interfaces and show health all commands did not display the correct number of unused ports has been fixed.	The fix does not impact the TOE's SFRs, as it corrects an administrative reporting display issue and does not alter the TOE's security functionality.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. An issue where abandoned file locks were handled incorrectly in Vision One TLS telemetry was fixed. This issue caused the following system log error message: SOAPDERROR: failed to lock ini file	The fix restores intended operational behavior of telemetry processing and does not affect the Security Functional Requirements (SFR) of the TOE.	Certification Body consider it as **Minor**
	[Bug Fix] The TOE version has been updated to v6.5.0. This release fixed a slow memory leak issue in the connection monitor daemon, which lead to layer 2 fallback.	The fix restores intended operational behavior under sustained runtime conditions. It does not introduce new security functionality or alters the Security Functional Requirements (SFR) of the TOE.	Certification Body consider it as **Minor**

3 Affected Developer Evidence

12 The affected developer evidence submitted for the assurance continuity required by the CCRA Assurance Continuity: CCRA Requirements Version 3.1 Feb 2024 (Ref [4]) are as below:

Table 3 – Affected Developer Evidence

Evidence Identification	Description of Changes	Rationale	Impact
Security Target: Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0 Security Target, v1.2, 01 April 2026.	The ST has been updated to Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0 Security Target, v1.2, 01 April 2026. The changes are: ·Front Page - The ST version and the document date have been updated · Front Page - TOE reference has been updated to reflect the change in TOE version from the developer. · Section 1 and Section 2 – TOE Description has been updated to reflect the change in TOE version from the developer. · Section 1.1 - The ST version and the document date have been updated · Section 1 and Section 2 – Additional hardware appliances device model has been added; TippingPoint 5600TXE (TPNN0424). · Section 2.3 - has been updated to the latest documents.	The changes or updates made do not affect the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**
Design Documentation: Trend Micro TippingPoint	The Design Documentation has been updated to Trend Micro TippingPoint Threat Protection System 6.5.0 Design Documentation, v1.2,	The changes or updates made do not impact the SFRs or the	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
Threat Protection System 6.5.0 Design Documentation, v1.2, 1 April 2026.	1 April 2026. The changes are: · Front Page - The Design Documentation version and date have been updated · Section 1 - TOE reference has been updated to reflect the change in TOE version from the developer. · Section 1 – Additional hardware appliance and software image have been added; Trend Micro TippingPoint 5600TXE (TPNN0424), Trend Micro TippingPoint vTPS (VMware) (vTPS_vmw_6.5.0.14731.zip) and Trend Micro TippingPoint vTPS (KVM) (vTPS_ kvm_6.5.0.14731.tar.gz) · Section 2 - TOE reference has been updated to reflect the change in TOE version from the developer. · Section 3.2.1 TippingPoint TPS Subsystem - Additional hardware appliance has been added; 5600TXE.	functionality included in the scope of the previous evaluation.	
Configuration Management Documentation: Trend Micro TippingPoint Threat Protection System 6.5.0 Configuration Management Documentation v1.2, 1 April 2026.	The Configuration Management documentation has been updated to Trend Micro TippingPoint Threat Protection System 6.5.0 Configuration Management Documentation, v1.2, 1 April 2026. The changes are: · Front Page - The Configuration Management Documentation version and date have been updated. · Section 1 and Section 2 - TOE reference has been updated to	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
	reflect the change in TOE version from the developer. · Section 1.2 - Additional hardware appliance has been added; TPS 5600TXE (TPNN0424). · Section 2.1 - Additional hardware appliance and software image have been added; Trend Micro TippingPoint 5600TXE (TPNN0424), Trend Micro TippingPoint vTPS (VMware) (vTPS_vmw_6.5.0.14731.zip), Trend Micro TippingPoint vTPS (KVM) (vTPS_ kvm_6.5.0.14731.tar.gz) and TPS 5600TXE. · Section 3 - TOE Configuration List have been updated to include the latest document version and date.		
Delivery Procedures Documentation: Trend Micro TippingPoint Threat Protection System Delivery Procedures, v1.1, 22 December 2025.	The Delivery Procedures has been updated to Trend Micro TippingPoint Threat Protection System 6.5.0 Delivery Procedures, v1.1, 22 December 2025. The changes are: · Front Page - The Delivery Procedures version and date have been updated. · Front Page & Section 1 – TOE reference has been updated to reflect the change in TOE version from the developer. · Section 1 - Additional hardware appliance has been added; TPS5600TXE (TPNN0424).	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
CCECG documentation: Trend Micro TippingPoint Threat Protection System Common Criteria Evaluated Configuration Guide (CCECG) for TPS v6.5.0, v1.2, 1 April 2026.	The Configuration Guide documentation has been updated to Trend Micro TippingPoint Threat Protection System Common Criteria Evaluated Configuration Guide (CCECG) for TPS 6.5.0, v1.2, 1 April 2026. The changes are: · Front Page - The Configuration Guide version and date have been updated. · Section 1 - TOE reference has been updated to reflect the change in TOE version from the developer. · Section 3 - Additional hardware appliance has been added; Trend Micro TippingPoint 5600TXE (TPNN0424).	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**
User guidance documentation: Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide v6.5.0, April 2024.	The TOE User Guide, v6.5.0, April 2024 has been reviewed, and no changes have been identified in the current version.	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**
Command Line Interface Reference documentation: Trend Micro TippingPoint Threat Protection System (TPS) Command Line Interface Reference, v6.5.0, December 2024	The CLI documentation v6.5.0, December 2024 has been reviewed, and no changes have been identified in the current version.	The changes or updates made do not impact the SFRs or the functionality included in the scope of the previous evaluation.	CB consider it as **Minor**

4 Result of Analysis

13 The outcome of the review determined that none of the modifications significantly affects the security mechanisms that implement the functional requirements defined in the Security Target (Ref [2]), in accordance with the Assurance Continuity Procedure (Ref [4]).

14 The nature of the changes leads to the conclusion that they are classified as MINOR changes. Therefore, based on the evidence provided, it is agreed that assurance is maintained for the certified version of the product.

Annex A References

[1] Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0 Impact Analysis Report (IAR) Version 1.3, 14 April 2026

[2] Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0 Security Target, Version 1.2, 01 April 2026

[3] Evaluation Technical Report – Trend Micro TippingPoint Threat Protection System (TPS) v6.4.0, V1.0, 19 May 2025

[4] Assurance Continuity: CCRA Requirements Version 3.1, Feb 2024

[5] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[6] Common Criteria for Information Technology Security Evaluation, Version 2022, Revision 1, November 2012.

[7] Common Methodology for Information Technology Security Evaluation, Version 2022, Revision 1, November 2012.

[8] MyCC Scheme Requirement (MyCC_REQ), v2, 24 April 2025.

[9] ISCB Evaluation Facility Manual (ISCB_EFM) v4, 24 April 2025.

[10] Trend Micro TippingPoint Threat Protection System (TPS) v6.5.0 Verification Test Plan Report (VTPR) Version 1.3, 14 April 2026

--- END OF DOCUMENT ---