MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

# M022 Assurance Maintenance Report Trend Micro TippingPoint Security Management System v6.4.0

File name: ISCB-5-RPT-M022-AMR-v1
Version: v1
Date of document: 17 June 2025
Document classification: PUBLIC


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

# M022 Assurance Maintenance Report

# Trend Micro TippingPoint Security Management System v6.4.0

17 June 2025

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:*** | M022 Assurance Maintenance Report |
| ***DOCUMENT REFERENCE:*** | ISCB-5-RPT-M022-AMR-v1 |
| ***ISSUE:*** | v1 |
| ***DATE:*** | 17 June 2025 |
| ***DISTRIBUTION:*** | UNCONTROLLED COPY - FOR UNLIMITED 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 | 10 June 2025 | All | Initial draft |
| v1 | 17 June 2025 | All | Final version |

# Table of Contents

# 1 Introduction

1 The TOE is Trend Micro TippingPoint Security Management System (SMS), v6.4.0. The TOE is a server-based solution that can act as the control center for managing large-scale deployments of TippingPoint Threat Protection System (TPS) and Intrusion Prevention System (IPS) products. It is also able to communicate threat data with TippingPoint Deep Discovery products. A single SMS can manage multiple TippingPoint devices—the maximum number depends on usage, network, and other environmental conditions.

2 The TOE is available as a rack-mountable hardware appliance or as a software-based product (vSMS) that operates in a virtual environment.

3 The core functionality provided by the TOE is the ability to create multiple filter profiles that are distributed to specific devices. Devices can be organized into groups or security zones to facilitate distribution and updating of security profiles, rather than doing this individually for each device. Administrators can also use the TOE to keep managed devices updated with the latest TippingPoint Operating System (TOS) software and Digital Vaccine (DV) packages.

4 The main components of the TOE are:

- SMS Server—provisioned as a rack-mountable appliance or as a virtual server (vSMS)
- SMS Client—a Java-based application for Windows, Linux or Mac workstations.

5 The TOE provides centralized control for managing large-scale deployments of the following TippingPoint products:

- TippingPoint NX Series Next-Generation Intrusion Prevention System (IPS)—uses a combination of technologies, including deep packet inspection, threat reputation, and advanced malware analysis, on a flow-by-flow basis to detect and prevent attacks on the network.
- TippingPoint Threat Protection System (TPS)—a network security platform that offers comprehensive threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks.

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

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** | M022 |
| **Project Identifier** | C133 |
| **Evaluation Scheme** | Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme |
| **Impact Analysis Report** | Trend Micro TippingPoint Security Management System (SMS) v6.4.0 Impact Analysis Report (IAR), Version 1.1 22 May 2025 |
| **New TOE** | Trend Micro TippingPoint Security Management System (SMS) v6.4.0 |
| **Certified TOE** | Trend Micro TippingPoint Security Management System (SMS) v6.2.0 |
| **New Security Target** | Trend Micro TippingPoint Security Management System (SMS) v6.4.0 Security Target, Version 1.2 05 June 2025 |
| **Evaluation Level** | EAL2 |
| **Evaluation Technical Report (ETR)** | Evaluation Technical Report – TippingPoint Security Management System (SMS) v6.2.0, V1.0 02 April 2024 |
| **Criteria** | Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5<br>Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, April 2017, Version 3.1, Revision 5<br>Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, April 2017, Version 3.1, Revision 5<br>Assurance Continuity: CCRA Requirements version 3.1, Feb 2024 |
| **Methodology** | Common Evaluation Methodology for Information Technology Security Evaluation, April 2017, Version 3.1 Revision 5 |
| **Common Criteria Conformance** | CC Part 2 Conformant<br>CC Part 3 Conformant<br>Package conformant to EAL2 |
| **Protection Profile Conformance** | None |
| **Sponsor** | Leidos Inc. |

| | |
|---|---|
| | 6841 Benjamin Franklin Drive Columbia, MD 21046, United States of America |
| **Developer** | Trend Micro Inc<br>11305 Alterra Parkway, Austin, Texas 78758, USA |
| **Evaluation Facility** | Securelytics SEF<br>A-17-01 & A-19-06, Tower A,<br>ATRIA SOFO Suites, Jalan SS 22/23,<br>Damansara Utama, 47400 Petaling Jaya,<br>Selangor, Malaysia. |

# 2 Description of Changes

10 Trend Micro has issued a new release which is Trend Micro TippingPoint Security Management System (SMS) v6.4.0. There were a series of minor updates to the Trend Micro TippingPoint Security Management System (SMS) since its certification version 6.2.0 on 03 May 2024 and Assurance Maintenance for Trend Micro TippingPoint Security Management System (SMS) v6.3.0 on 27 Nov 2024 (Ref[11].

## 2.1 Changes to the product associated with the certified TOE

11 The following features have been added in Trend Micro TippingPoint Security Management System (SMS) v6.4.0. 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 Security Management System (SMS) v6.4.0 | • This release introduces the next generation of SMS appliances, the Dell PowerEdge R660 SMS H5 and H5 XL rack servers, for greater available storage.<br>• This release adds support for TLS 1.3, delivering enhanced security, faster performance, and a streamlined protocol for improved reliability and efficiency.<br>• The following host key algorithms are no longer supported for SSH access to the SMS:<br>i. ecdsa-sha2-nistp256<br>ii. ecdsa-sha2-nistp384<br>iii. ecdsa-sha2-nistp521<br>• The SMS no longer uses the following ports; 10042, 10043, 1098, 1099, 4444<br>• In addition to x86 (Intel) processors, the SMS client can now also use ARM (Apple Silicon) processors.<br>• Filter exceptions no longer permit invalid IP ranges to be entered.<br>• This release removes the 'diffie-hellmangroup14- sha1' SSH key algorithm.<br>• This release fixes an issue where Scheduled Reports erroneously displayed as empty. | The updates do not affect the Security Functional Requirements of the TOE | CB consider it as **Minor** |

| Version | Description of Changes | Rationale | Impact |
|---|---|---|---|
| | • An issue that prevented profile distribution with the 'failed to build url' error has been resolved. | | |
| | • This release support for a new type of Reputation filtering enables users to alert and/or block malicious files according to their hash values. User can add as many as 35,000 SHA-1 or SHA-256 file hashes of any type to the Reputation Database. In this release, file hash is applied to http (or https when decrypting) get requests, for all files except the following; HTML, Audio or video, Font and Files larger than 50 MB.<br>When the 'Suspicious Object Sync'connectivity setting to Trend Vision One is enabled, the SMS can now pull SHA-1/SHA-256 file hashes from Trend Vision One into the SMS reputation database, along with IPv4/IPv6 addresses, Domain name entries, and URLs. File Hash Reputation does not support an action set with a 'Rate Limit' flow control. For those entries, you can change the action set to one with a different flow control type orremove file hashes from the entry criteria.<br>• This release introduces Let's Encrypt (LE) CA for ACME certificate requests, enabling automated TLS certificate renewal. The customer no longer has to manually request TLS certificates and keys from a protected web server for the initial TLS configuration and then again every time these assets expire. Automation includes:<br>i. Certificate Issuance. Automatically obtain a new certificate when needed.<br>ii. Validation. Verify domain ownership without manual intervention.<br>iii. Installation. Install and configure the CAsigned certificate for | The updates do not affect the Security Functional Requirements of the TOE as it has been reflected to be out of scope | CB consider it as **Minor** |

| Version | Description of Changes | Rationale | Impact |
|---|---|---|---|
| | transparent inspection of encrypted web traffic.<br>• Server name indication (SNI) filtering has been added to the Domain Suspicious Objects database. The TLS handshake inspection this provides enables the customer to filter servers by FQDN instead of wildcarded URLs, while sustaining the ability to inspect encrypted traffic without having to decrypt. In addition, Domain reputation filtering has been enhanced to support wildcards, allowing filtering by country code or top-level domains.<br>• The Digital Vaccine (DV) has a new deployment setting, which uses the same filters that are enabled in the Default deployment mode, but with a 'Permit+Notify' posture instead of 'Block'. Certain traffic normalization filters that detect malformed IP packets must remain configured to 'Block'. For any filters that have a recommended configuration of 'Block', you must manually override the default setting and set them to 'Block' yourself prior to distribution of the new DV that contains the Evaluation deployment mode. If the DV with the new Evaluation mode is deployed without this manual override, any profile that uses the new Evaluation deployment mode will have its existing default 'Block' filters modified to 'Permit+Notify' after the profile is distributed to the device.<br>• A new 'punycode' parameter has been added to the 'repEntries/query?dns' SMS API call. This parameter causes the output from a DNS query to show punycode-encoded domain names instead of Unicode domain names.<br>• This release fixes an issue that prevented users from accessing the SMS web management console after a reboot.<br>• From the SMS Web interface, download the MacOS SMS client installer specifically designed for ARM-based | | |

| Version | Description of Changes | Rationale | Impact |
|---|---|---|---|
| | CPUs and begin the upgrade process. Upgrades from previous client version to v6.4.0 on MacOS 15 and later will fail because of a known issue with the Rosetta 2 emulator.<br>• To improve scale and resilience, packet traces generated when a filter is matched can now be included as part of the syslog message output from SMS to a SIEM/collector. This can improve scale and helps avoid challenges related to matching pcap files with security events.<br>• An audit log spamming condition that caused the TPS disk to show as full has been repaired.<br>• This release fixes a status display issue for 8600TXE fans and power supplies.<br>• The KVM console readout no longer continuously shows disconnects and reconnects of the keyboard and mouse after an upgrade.<br>• When exporting a device configuration from SMS, the file no longer stores SNMP passwords in plain text.<br>• This release fixes incorrect file permissions on the 'smsportfwd' file that could cause a loss of access to the SMS Web interface.<br>• When you disable SMS High Availability with the intention of using the SMSs independently, if Trend Vision One integration has been used, the passive SMS must be factory reset. Do not disconnect from Trend Vision One prior to the factory reset.<br>• An issue that caused 'SOAP Daemon: Fault returned to SMS 'Error getting noisy security policies from TOS'' to repeatedly display in the system log has been fixed.<br>• Two SMS Web Server vulnerabilities, 'No Same site attribute: JSESSIONID and Slowloris Denial of service vulnerability', | | |

| Version | Description of Changes | Rationale | Impact |
|---|---|---|---|
| | are addressed by an upgrade to the Java environment (Wildfly) in this release.<br>• This release fixes an SMS Java Version Disclosure vulnerability through an upgrade to the Java environment (Wildfly).<br>• This release fixes an issue where multiple versions of snapshots were all marked as "Allow Restore."<br>• The help screen for the ThreatDV URL Lookup now displays correctly.<br>• Users no longer have to remove all leading or trailing spaces in their filter names (including Traffic Management, Advanced DDoS, Reputation, and SSL inbound/outbound filters) during an upgrade.<br>• Both HA nodes require an SMS certificate key size of 2048 bits before HA is configured.<br>• An issue was fixed on historical port graphs that caused the y-axis port speed labels to sometimes display incorrectly.<br>• Enhancements in this release prevent data duplication for events in the remote syslog that could occur under rare conditions:<br>i. New preference setting for events. A new system preference setting, 'Retrieve New Events/Logs Only', restricts the SMS to examining only recent entries from a device when the last fetched event is indeterminate, or the device is newly managed. This is enabled by default.<br>ii. Event transmission control. To further reduce data duplication and to ensure the relevance and efficiency of data transmission, the system now restricts transmitting remote syslog server events to those generated within the last 24 hours. | | |

| Version | Description of Changes | Rationale | Impact |
|---|---|---|---|
| | • Attempts to connect to the passive SMS in an HA configuration now automatically get redirected to the active SMS. | | |

# 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:**<br>Trend Micro TippingPoint Security Management System v6.4.0 Version 1.2 June 05, 2025 | Changes in the ST are:<br>• Front Page - The ST version and document date have been updated<br>• Front Page - TOE reference has been updated to reflect the change in TOE version from the developer<br>• Section 1 and Section 2 – TOE Description has been updated to reflect the change in TOE version from the developer<br>• Section 1.1 – Additional hardware appliances have been added; TippingPoint Security Management System H5 Appliance (TPNN0431) and TippingPoint Security Management System H5 XL Appliance (TPNN0432)<br>• Section 2.3.1 – Specifications for additional hardware appliances have been included for SMS H5 and SMS H5 XL<br>• Section 2.5 has been updated to the latest documents<br>• Section 6.4 - TLS v1.3 and TLS v1.3 cipher suites (TLS_AES_256_GCM_SHA384 and TLS_AES_128_GCM_SHA256) have been added<br>• Section 6.6 - TLS v1.3 and TLS v1.3 cipher suites (TLS_AES_256_GCM_SHA384 | 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** |

| Evidence Identification | Description of Changes | Rationale | Impact |
|---|---|---|---|
| | and TLS_AES_128_GCM_SHA256) have been added | | |
| **Design Documentation:**<br><br>Trend Micro TippingPoint Security Management System v6.4.0 Design Documentation Version 1.2 June 05, 2025 | Changes in the Design document are:<br>• Front Page - The Design Documentation version and date have been updated<br>• Section 1 - TOE reference has been updated to reflect the change in TOE version from the developer<br>• Section 1 - Additional hardware appliances have been added; TippingPoint Security Management System H5 Appliance (TPNN0431) and TippingPoint Security Management System H5 XL Appliance (TPNN0432)<br>• Section 2.3.1.3.83 - TLS v1.3 has been added<br>• Section 2.4 - Additional hardware appliances have been added; SMS H5 appliance; and SMS H5 XL appliance<br>• Section 3.2.1 - Additional hardware appliances have been added; SMS H5 appliance; and SMS H5 XL appliance<br>• Section 3.3 – TLS v1.3 and TLS v1.3 cipher suites (TLS_AES_256_GCM_SHA384 and TLS_AES_128_GCM_SHA256) have been added<br>• Sections 5.1 and Section 5.2 – References have been updated to include the latest document version and date | 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 |
|---|---|---|---|
| **Configuration Management Documentation:**<br>Trend Micro TippingPoint Security Management System v6.4.0 Configuration Management Documentation Version 1.4 June 05, 2025 | Changes in the Configuration Management document are:<br>• Front Page - The Configuration Management Documentation version and date have been updated<br>• Section 1 and Section 2 - TOE reference has been updated to reflect the change in TOE version from the developer<br>• Section 1.2 Additional hardware appliances have been added; TippingPoint Security Management System H5 Appliance (TPNN0431) and TippingPoint Security Management System H5 XL Appliance (TPNN0432)<br>• Section 2.1 Additional hardware appliances have been added; TippingPoint Security Management System H4 XL Appliance (TPNN0335), TippingPoint Security Management System H5 Appliance (TPNN0431), TippingPoint Security Management System H5 XL Appliance (TPNN0432)<br>• Section 3 – TOE Configuration List have been updated to include the latest document version and date | 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** |
| **Delivery Procedures Documentation:**<br>Trend Micro TippingPoint Security Management System Delivery Procedure Version 1.2 February 26, 2025 | Changes made to the Delivery Procedures are:<br>• Front Page - The Delivery Procedures version and date have been updated<br>• Section 1 - TOE reference has been updated to reflect the change in TOE version from the developer<br>• Section 1 - Additional hardware appliances have | 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 |
|---|---|---|---|
| | been added; TippingPoint Security Management System H4 XL Appliance (TPNN0335), TippingPoint Security Management System H5 Appliance (TPNN0431), TippingPoint Security Management System H5 XL Appliance (TPNN0432) | | |
| **User guidance documentation:**<br><br>Trend Micro TippingPoint Security Management System (SMS) Command Line Interface Reference December 2024 | The CLI user guidance has been updated to Trend Micro TippingPoint Security Management System (SMS) Command Line Interface Reference, December 2024. | 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:**<br><br>Trend Micro TippingPoint Security Management System (SMS) User Guide December 2024 | The TOE user guide has been updated to Trend Micro TippingPoint Security Management System (SMS) User Guide, December 2024. TLS v1.3 and TLS v1.3 cipher suites (TLS_AES_256_GCM_SHA384 and TLS_AES_128_GCM_SHA256) have been added | 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 this version of the product.

# Annex A References

[1] Trend Micro TippingPoint Security Management System (SMS) v6.4.0 Impact Analysis Report Version 1.1, 22 May 2025

[2] Trend Micro TippingPoint Security Management System (SMS) v6.4.0 Security Target, Version 1.2, 05 June 2025

[3] Evaluation Technical Report – Trend Micro TippingPoint Security Management System (SMS) v6.2.0, V1.0, 02 April 2024

[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 3.1, Revision 5, April 2017.

[7] Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

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

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

[10] Verification Test Plan Report Version 1.0, 07 May 2025

[11] M021 Maintenance Report Version 1, 21 November 2024

--- END OF DOCUMENT ---