MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

4

M021 Maintenance Report

File name: ISCB-5-RPT-M021-AMR-v1
Version: v1
Date of document: 21 Nov 2024
Document classification: PUBLIC

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

M021 Maintenance Report

21 Nov 2024

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:	M021 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M021-AMR-v1
ISSUE:	v1
DATE:	21 Nov 2024

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. 201601006881 (726630-U)

Printed in Malaysia

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	15 Nov 2024	All	Initial draft
v1	21 Nov 2024	All	Final version

Table of Contents

1 Introduction

1 The Target of Evaluation (TOE) is Trend Micro TippingPoint Security Management System (SMS), v6.3.0. 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	M021
Project Identifier	C133
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	Trend Micro TippingPoint Security Management System (SMS) v6.3.0 Impact Analysis Report (IAR), Version 1.1 13 Nov 2024
New TOE	Trend Micro TippingPoint Security Management System (SMS) v6.3.0
Certified TOE	Trend Micro TippingPoint Security Management System (SMS) v6.2.0
New Security Target	Trend Micro TippingPoint Security Management System (SMS) v6.3.0 Security Target, Version 1.0 15 Oct 2024
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 Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, April 2017, Version 3.1, Revision 5 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, April 2017, Version 3.1, Revision 5 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 CC Part 3 Conformant 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 11305 Alterra Parkway, Austin, Texas 78758, USA
Evaluation Facility	Securelytics SEF A-17-01 & A-19-06, 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 Security Management System (SMS) v6.3.0. 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.

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) v6.3.0. 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) v6.3.0	• This release expands SMS management support to include the new TPS 8600TXE model. • Port 443 must remain open for downloading installer applications from a web browser. When port 443 is enabled, the client UI will use it for downloading updates and patches during login; if this port is disabled, the client UI will fall back to java message Service (JMS) ports. • A condition that caused RADIUS authentication to fail intermittently has been repaired. • Version 3 of the snmpwalk command now works correctly. • The error message has been improved when a device is managed using an expired password.	The updates do not affect the Security Functional Requirements of the TOE	CB consider it as **Minor**
	• This release adds the option to enable, configure, or disable daily device discovery, ensuring it doesn't interfere with other deployments. Daily discovery is now disabled by default. • The hostname can now be used to configure PCAP offload for SMB. • The SMS client's Certificate Signing Request editor now accepts multiple organization unit (OU) or department	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
	name values for the certificate's subject Distinguished Name (DN). There is no limit for the number of entries within the field's 4k space allowance. Enter one value per line. • The Performance Protection Graph no longer indicates that performance protection is turned on when it is not enabled on the device. • Performance issues affecting SMS profile distributions have been repaired. • Resetting RepDV after bringing an SMS back online no longer results in excessive incremental updates. • The New and Delete buttons now work as expected in the System Snapshots interface on the SMS client. • The way the SMS stores and encodes URI Metadata in the database has been enhanced for detection data monitoring that is encoded in other languages. • Fixed an open file handle leak for Trend Vision One TLS Telemetry. • Fixed an issue that prevented the geolocation of Ips in Events from displaying.		

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 Security Management System v6.3.0 Version 1.0 Oct 15, 2024	Changes in the ST are: • Front Page - The ST version and 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 2.3.1 – VMware vSphere Client version 6.7 has been removed as the operational environment supported for vSMS platform • Section 2.5 has been updated to the latest documents	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Design Documentation: Trend Micro TippingPoint Security Management System v6.3.0 Design Documentation Version 1.0 Oct 15, 2024	Changes in the Design document 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.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
	• Section 2.4 – VMware vSphere Client version 6.7 has been removed as the operational environment supported for vSMS platform • Sections 5.1 and Section 5.2 – References have been updated to include the latest document version and date		
Configuration Management Documentation Trend Micro TippingPoint Security Management System v6.3.0 Configuration Management Documentation Version 1.1 Oct 15, 2024	Changes in the Configuration Management document are: • Front Page - The Configuration Management Documentation version and date have been updated • Section 1 and Section 2 - TOE reference has been updated to reflect the change in TOE version from the developer • Section 3 – TOE Configuration List have been updated to include the latest document version and date	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Delivery Procedures Documentation Trend Micro TippingPoint Security Management System Delivery Procedure Version 1.1 Oct 15, 2024	Changes made to the Delivery Procedures are: • Front Page - The Delivery Procedures version and date have been updated • Section 1 - TOE reference has been updated to reflect the change in TOE version from the developer	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
Trend Micro TippingPoint Security Management System (SMS) Command Line Interface Reference April 2024.	The CLI user guidance has been updated to Trend Micro TippingPoint Security Management System (SMS) Command Line Interface Reference, April 2024.	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Trend Micro TippingPoint Security Management System (SMS) User Guide April 2024	The change expands the TOE capabilities to include support for managing the TPS 8600TXE model	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**

4 Result of Analysis

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

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

Annex A References

[1] Trend Micro TippingPoint Security Management System (SMS) v6.3.0 Impact Analysis Report Version 1.1, 13 Nov 2024

[2] Trend Micro TippingPoint Security Management System (SMS) v6.3.0 Security Target, Version 1.0, 15 Oct 2024

[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), v1b, July 2023.

[9] ISCB Evaluation Facility Manual (ISCB_EFM) v3, January 2023.

[10] Verification Test Plan Report Version 1.0, Oct 2024

--- END OF DOCUMENT ---