MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

M017 Maintenance Report

File name: ISCB-5-RPT-M017-AMR-v1
Version: v1
Date of document: 27 January 2022
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Best Brand Internet Security 2008 & 2009
MS ISO/IEC 17021: 2011 ISMS 02082013 CB 02
Status Company
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

M017 Maintenance Report

27 January 2022

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:	M017 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M017-AMR-v1
ISSUE:	v1
DATE:	27 January 2022
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. 726630-U

Printed in Malaysia

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	10 January 2022	All	Initial draft
v1	27 January 2022	All	Final version

Table of Contents

1 Introduction

1 The TOE is TippingPoint Security Management System (SMS), v5.5.0. It 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 core functionality provided by the TOE is the ability to create multiple filter profiles that are distributed to specific devices. Devices can be organised 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

3 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.

4 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 TOE as in Table 1 identification below.

Table 1 – Identification Information

Assurance Maintenance Identifier	M017
Project Identifier	C097
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	Trend Micro TippingPoint Security Management System v5.5.0 Impact Analysis Report
New TOE	Trend Micro TippingPoint Security Management System v5.5.0
Certified TOE	Trend Micro TippingPoint Security Management System v5.4.0
New Security Target	Trend Micro TippingPoint Security Management System v5.5.0 Security Target, Version 1.3, 16 November 2021
Evaluation Level	EAL2

Evaluation Technical Report (ETR)	Evaluation Technical Report - Trend Micro TippingPoint Security Management System V5.1.0, 10 September 2018 (EAU000426.07-S046-ETR 1.0)
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 2.1, June 2012
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, Maryland 21046, United States of America
Developer	Trend Micro Inc. 11305 Alterra Parkway, Austin, Texas 78758, United States of America
Evaluation Facility	BAE Systems Lab – MySEF Menara Binjai, Level 28, No. 2, Jalan Binjai, 50450 Wilayah Persekutuan Kuala Lumpur, Malaysia

2 Description of Changes

5 Trend Micro has issued a new release of the Trend Micro TippingPoint Security Management System v5.5.0 since its re-certification version 5.4.0 on February 2021.

2.1 Changes to the product associated with the certified TOE

6 The following features have been added in Trend Micro TippingPoint Security Management System v5.5.0 as below:

Table 2 – General changes/additions

Version	Description of Changes	Rationale	Impact
Trend Micro TippingPoint Security Management System 5.5.0	• Integration of the SMS server with Vision One. This integration leverages Vision One's superior threat detection technology to help protect the network from suspicious objects, including known malicious or potentially malicious domains, IP addresses, or URLs.	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**
	• Using the SMS web management console, it now can be used by RESTful APIs to access SMS functionality (Help > Tools and Resources > SMS REST API Online Help).	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**
	• New APIs functionality, which can now export all enabled and disabled filters and corresponding CVEs for a profile to audit and assess if appropriate security controls are in place. • New APIs functionality, user can now retrieve all user defined reputation entries.	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**
	• SMS administrators can now assign segments to groups when adding a new device and add descriptions to segments	The updates do not affect the Security Functional Requirements of	CB consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	and segment groups to capture the network configuration or describe the segments within the group. They can also provide extended descriptions up to 2048 characters for profiles to capture and audit profile changes.	the TOE, as segments and segment groups are device attributes and are already covered in the scope of security management roles in the previous evaluation. This does not require any changes to FMT_MTD.1 or FMT_SMF.1.	
	• When using nested device groups, SMS administrators now have full path visibility for a device and can use the left-hand navigation tree to locate a device.	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**
	• SMS now sends a notification when a device has not been associated with a license. User can also navigate to the Devices tab to identify those devices without a license and view the current utilization of licensed devices to determine those nearing the limit.	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**
	• A user with operator role capabilities can now view: - secondary NTP server settings on the Device summary page - read-only device configurable settings	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
	• A banner message is now displayed on an SMS that is configured for HA and is passive, indicating that console access is disabled.	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**
	• Additional SMBv3 support was added for exporting SMS backups, profiles, and reports. Reports now can be successfully exported to an SMB share containing subdirectories.	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**
	• The maximum number of active sessions for AD, RADIUS, and TACACS are now enforced. If the user reaches the maximum number of active sessions, the login will fail.	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**
	• Although the limit of 5 concurrent packet traces is enforced, new packet traces can now be started if no more than 4 packet traces are actively running. Previously, under certain conditions, when the total number of packet traces started since the device was booted reached 5, additional packet traces could not start until the device was rebooted, even if no packet traces were actively running.	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**
	• The SMS now uses Named IP addresses if a match is found	The updates do not affect the Security	CB consider

Version	Description of Changes	Rationale	Impact
	when configuring Host IP Filters, SNMP Settings, Remote Syslog, Servers, Time Settings, and sFlow. This does not occur for newly managed devices.	Functional Requirements of the TOE, as it has been reflected to be out-of-scope.	it as **Minor**
	• Device hostname is now included among the information that the SMS uploads to the TMC. This enables License Manager to identify devices by name.	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**

2.2 Changes to the SFRs claimed in the ST

7 The changes that have been made is not affecting the Security Functional Requirements (SFRs) in the ST (Ref [3]).

3 Affected Developer Evidence

8 The affected developer evidence submitted for the assurance continuity required by the CCRA Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012 (Ref [11]) are as below:

Table 3 – Affected Developer Evidence

Evidence	Description of Changes	Rationale	Impact
Trend Micro TippingPoint Security Management System v5.5.0 Security Target, version 1.3, 16 November 2021	• The ST version and document date have been updated. • TOE reference has been updated to reflect the change in TOE version from the developer. • Section 2 – TOE Description has been updated to reflect the change in TOE version from the developer. • Section 2.1 – Overview has been updated to add description of Service One and Vision Gateway, which is out of the scope of the evaluation. • Section 2.3.1 – TOE Components has been updated to include VMware vSphere Client 6.7 or 7.0.2 and VMware ESX/ESXi version 6.7 or 7.0.2 as the operational environment supported for vSMS platform. • Section 2.5 has been updated to the latest documents' versions and dates.	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 v5.5.0 Design Documentation, version 1.0, 28 October 2021	• The ST reference version and document date have been updated. • The design documentation version and date have been updated. • TOE reference has been updated to reflect the change	The changes/ update that have been made is not affecting to the SFRs or functionality that was included in	CB consider it as **Minor**

Evidence	Description of Changes	Rationale	Impact
	in TOE version from the developer. • Section 2.4 - Services Provided by Operational Environment has been updated to include VMware vSphere Client 6.7 or 7.0.2 and VMware ESX/ESXi version 6.7 or 7.0.2 as the operational environment supported for vSMS platform. • Section 2.4 - Services Provided by Operational Environment has been updated to update the minimum recommended system requirements for the vSMS platform. • Section 2.4 - Services Provided by Operational Environment has been updated to update information on the FIPS-mode, which is outside the scope of the evaluation. • Sections 5.1 – TOE Documentation and Section 5.2 – Other References have been updated to include the latest document version and date.	the scope of the previous evaluation.	
Trend Micro TippingPoint Security Management System v5.5.0 Configuration Management System, version 1.3, 16 November 2021.	• Change History has been updated to include latest version of the document. • The ST reference version and document date have been updated. • The configuration management documentation version and date have been updated. • 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 to the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence	Description of Changes	Rationale	Impact
	• Section 3 – TOE Configuration List have been updated to include the latest document version and date.		

4 Result of Analysis

9 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 [3]) as required in accordance of Assurance Continuity: CCRA Requirements version 2.1 (2012-06-01) June 2012 (Ref [11]).

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

Annex A References

[1] Trend Micro TippingPoint Security Management System v5.5.0 Impact Analysis Report (IAR), EAU001078-IAR, Version 1.0, 16 December 2021

[2] Security Management System Release Notes, Version 5.5.

[3] Trend Micro TippingPoint Security Management System v5.5.0 Security Target, Version 1.3, 16 November 2021

[4] Evaluation Technical Report - Trend Micro TippingPoint Security Management System V5.4.0, 10 September 2018 (EAU000426.07-S046-ETR 1.0)

[5] TippingPoint Virtual Security Management System (vSMS) User Guide, July 2021

[6] Trend Micro Tipping Point Security Management System v5.5 Design Documentation Version 1.0, 28 October 2021

[7] Trend Micro Tipping Point Security Management System Configuration Management Documentation Version 1.3, 16 November 2021

[8] TippingPoint Security Management System (SMS) Command Line Interface Reference, July 2021

[9] TippingPoint Identify Agent Deployment Guide, July 2020

[10] TippingPoint URL Reputation Filtering Deployment and Best Practices Guide, July 2021

[11] Assurance Continuity: CCRA Requirements Version 2.1 (2012-06-01) June 2012

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

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

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

[15] MyCC Scheme Requirement (MyCC_REQ), v1, December 2019.

[16] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2020.

--- END OF DOCUMENT ---