MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

M016 Maintenance Report

File name: ISCB-5-RPT-M016-AMR-v1
Version: v1
Date of document: 18 February 2021
Document classification: PUBLIC

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

M016 Maintenance Report

18 February 2021

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:	M016 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M016-AMR-v1
ISSUE:	v1
DATE:	18 February 2021
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 February 2021	All	Initial draft
V1	18 February 2021	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 3

2.1 Changes to the product associated with the certified TOE 3

2.2 Changes to the SFRs claimed in the ST 5

3 Affected Developer Evidence 6

4 Result of Analysis 8

Annex A References 9

1 Introduction

1 The TOE is TippingPoint Security Management System (SMS), v5.4.0. 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	M016
Project Identifier	C097
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	Trend Micro TippingPoint Security Management System v5.4.0 Impact Analysis Report
New TOE	Trend Micro TippingPoint Security Management System v5.4.0
Certified TOE	Trend Micro TippingPoint Security Management System v5.3.0
New Security Target	Trend Micro TippingPoint Security Management System v5.4.0 Security Target, Version 1.2, 07 December 2020
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
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 v5.4.0 since its certification version 5.3.0 on 30 April 2020.

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 v5.4.0 as below:

Table 2 – General changes/additions

Version	Description of Changes	Rationale	Impact
Trend Micro TippingPoint SMS v5.4.0	**New features / enhancement** • Added real-time threat protection for outbound client SSL (Secure Sockets Layer) traffic. • The vSMS now supports VMware vSphere 6.7 and 7.0 of VMware vSphere and ESX/ESXi. **Fixed issues:** • Performance enhancements to prevent SMS clients from being locked out after HA (High Availability) events. • Fixed the issue of the SMS Client where previously it does not show device system logs beyond seven (7) days. • Fixed the issue where the SMS was only adding its name to syslog records for certain types of events. It is now always adding its name properly. • Local scheduled backups no longer fail. • Users no longer have to restart the SMS before certificate changes go into effect when using an encrypted TCP (Transmission Control Protocol) syslog. • The vSMS VMWare image is now signed with a cert that expires in three years instead of in one year. • Restrictions for validating host names from the SMS device editor required that the host names matched what was on the device LSM (Linux Security Module) or CLI (Command Line Interface). This was corrected on the SMS so that fully qualified domain names could be entered into the host name field.	The updates do not affect the Security Functional Requirements of the TOE.	CB consider it as **Minor**

	• Fixed the issue where syntax problems in the CSV (Comma-separated values) file caused the maximum record size to be exceeded, which also caused the error message to not display correctly in the UI (User Interface). • Fixed the issue where repeated CPU (Central Processing Unit) halting caused by the kernel version that SMS v5.3 shipped with could cause the Vertica database to become corrupted. • Fixed the issue where previously running the WHOIS command sometimes yields no results in the SMS client. • Fixed the issue that caused URL (Uniform Resource Locator) normalisation errors on some devices during URL reputation filtering no longer occurs. • Fixed the issue where previously devices panel would sometimes fail to display the managed devices when clicked. Clicking on any other panel after this would freeze the interface. • Fixed the issue where previously the SMS Diagnostic files could inflate inordinately under rare conditions. • Some Reputation IP (Internet Protocol) exceptions updates were not being applied to the exceptions list after the profile was distributed. This issue has been corrected. • If a user without access to all groups on the SMS performed an action that would restart the RADIUS (Remote Authentication Dial-In User Service) login module on the SMS, the map of groups used in RADIUS group mapping would be re-created to contain **only the groups that user had permission to view**. The 5.4 release version ensures that if the RADIUS login module is restarted, the map will contain all groups on the SMS **regardless of user permissions**. • Corrected an issue that caused the syslog to display old events along with new ones, even though the deployment was configured to forward only new events. • Corrected an issue that caused the SMS to enable Auto-Negotiation on a TPS (Threat		

	Protection System) device after an upgrade.		

2.2 Changes to the SFRs claimed in the ST

7 The changes that have been made is not affecting Security Functional Requirements (SFRs) in the ST (Ref [4]).

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 [10]) are as below:

Table 3 – Affected Developer Evidence

Evidence	Description of Changes	Rationale	Impact
Trend Micro TippingPoint Security Management System v5.4.0 Security Target, Version 1.2, 07 December 2020	• The ST version and document date have been updated. • TOE reference has been updated to reflect the change in TOE version from the developer (v5.4.0). • Section 2.3.1 has been updated to include virtualisation support for VMware vSphere Client and VMware ESX/ESXi version 6.7 and 7.0. • Section 2.5 has been updated to the latest document version and date.	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**
TippingPoint Security Management System (SMS) User Guide, August 2020	• The TippingPoint SMS User Guide document for the TOE v5.4.0 has been updated to reflect the enhancements made in the new TOE version release. • The document date has been updated.	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**
TippingPoint Virtual Security Management System (vSMS) User Guide, December 2020	• The TippingPoint Virtual SMS User Guide document for the TOE v5.4.0 has been updated to reflect the enhancements made in the new TOE version release. • The document date has been updated. • Section "VMware vSphere environment" has been updated to include virtualisation support for VMware vSphere	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
	Client and VMware ESX/ESXi version 6.7 and 7.0.		
TippingPoint Security Management System (SMS) Web API Guide, October 2020	• The TippingPoint SMS Web API Guide document for the TOE v5.4.0 has been updated to reflect the enhancements made in the new TOE version release. • The document date has been updated.	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**
Trend Micro TippingPoint Security Management System v5.4 Design Documentation, Version 1.0, 21 December 2020	• The document date and version have been updated. • TOE reference has been updated to reflect the change in TOE version from the developer (v5.4.0). • Section 5.2 has been updated to include the latest ST reference (v1.2). • Section 2.4 has been updated to include virtualisation support for VMware vSphere Client and VMware ESX/ESXi version 6.7 and 7.0.	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**
Trend Micro TippingPoint Security Management System Configuration Management Documentation, Version 1.2, 21 December 2020	• The document date and version have been updated. • TOE reference has been updated to reflect the change in TOE version from the developer (v5.4.0). • Section 3 has been updated to include the latest SAR Evidences with their respective Version Number.	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**

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 [4]) as required in accordance of Assurance Continuity: CCRA Requirements version 2.1 (2012-06-01) June 2012 (Ref [10]).

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

Annex A References

[1] Trend Micro TippingPoint Security Management System v5.4.0 Impact Analysis Report (IAR), EAU000970-IAR, Version 1.0, 28 January 2021

[2] Security Management System Release Notes, Version 5.4.0, 2020

[3] Trend Micro TippingPoint Security Management System Security Target, Version 1.1, 18 March 2020

[4] Trend Micro TippingPoint Security Management System v5.4.0 Security Target, Version 1.2, 07 December 2020

[5] TippingPoint Security Management System (SMS) User Guide, Version 5.4, August 2020

[6] TippingPoint Virtual Security Management System (vSMS) User Guide, Version 5.4, December 2020

[7] TippingPoint Security Management System (SMS) Web API Guide, Version 5.4, October 2020

[8] Trend Micro TippingPoint Security Management System v5.4 Design Documentation, Version 1.0, 21 December 2020

[9] Trend Micro TippingPoint Security Management System Configuration Management Documentation, Version 1.2, 21 December 2020

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

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

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

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

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

[15] ISCB Evaluation Facility Manual (ISCB_EFM), v2, December 2019.

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

--- END OF DOCUMENT ---