MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

M011 Maintenance Report

File name: ISCB-5-RPT-M011-AMR-V1
Version: V1
Date of document: 4 November 2019
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

M011 Maintenance Report

4 November 2019

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:	M011 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M011-AMR-V1
ISSUE:	V1
DATE:	4 November 2019

PREPARED BY:

Nur Shazwani Mohd Zakaria M011 Lead Certifier, ISCB Department CyberSecurity Malaysia	Date

VERIFIED BY:

Amiroul Farhan Roslaini Senior Certifier, ISCB Department CyberSecurity Malaysia	Date
Hasnida bt Zainuddin Scheme Manager, ISCB Department CyberSecurity Malaysia	Date

APPROVED BY

Wan Shafiuddin Zainudin Head of ISCB/Scheme Head CyberSecurity Malaysia	Date

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	31 October 2019	All	Initial draft
V1	4 November 2019	1, 2, 5, 6, 8, 9 and 11	Finalise the draft based on Developer and Evaluator's review

Table of Contents

1 Introduction

1 The TOE is Trend Micro TippingPoint Security Management System (TippingPoint SMS) v5.2.0. 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. TippingPoint SMS can communicate threat data with TippingPoint Deep Discovery products.

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

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

3 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	M011
Project Identifier	C097
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	Trend Micro TippingPoint Security Management System v5.2.0 Impact Analysis Report
New TOE	Trend Micro TippingPoint Security Management System v5.2.0
Certified TOE	Trend Micro TippingPoint Security Management System v5.1.0
New Security Target	Trend Micro TippingPoint Security Management System Security Target, version 1.0, 7 October 2019
Evaluation Level	EAL2
Evaluation Technical Report (ETR)	Evaluation Technical Report – Trend Micro TippingPoint Security Management System V5.1.0 EAU000426.07-S046-ETR 1.0, 10 September 2018
Criteria	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 USA
Developer	Trend Micro Incorporated 11305 Alterra Parkway, Austin, Texas 78758 USA
Evaluation Facility	BAE Systems Applied Intelligence Malaysia - MySEF

2 Description of Changes

4 Trend Micro Incorporated has issued a new release of the Trend Micro TippingPoint Security Management System version 5.2.0. There were a series of minor updates to the Trend Micro TippingPoint Security Management System since its certification version 5.1.0 of 9 October 2018.

2.1 Changes to the product associated with the certified TOE

5 The following features have been added in Trend Micro TippingPoint Security Management System version 5.1.1 and version 5.2.0 as below:

Table 2 – General changes/additions

Version	Description of Changes	Rationale	Impact
Trend Micro TippingPoint Security Management System 5.1.1	• Import the Geo Locator Database from the TMC. • Distribution failures with a 'Too many open files' error no longer occur. • Inspection events now display correctly in the SMS interface. • The Device Group editor no longer supports removing devices in a stack. • A new syslog field is now available for **actionSetName**. • Restoring a filter to category settings now correctly removes the filter override. • An issue causing an SMS filesystem to become full and experience degraded performance has been corrected. • SMS no longer incorrectly names custom filters from the DV toolkit. • SMS is able to properly import and merge a profile that has reputation filters with mismatching tag categories. • Changes to Rep DV Country Tag Category will no longer generate system log error message. • SMS can save alterations to tables (such as resized column	The updates do not affect the Security Functional Requirements of the TOE.	CB consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	widths) within logs viewable from the SMS client. • Sending email on reputation feed download is turned off by default. • DV activation failures due to conflicts with URL forwarding have been addressed. • An issue causing irregular character strings to appear in the audit log records under certain circumstances has been addressed. • An issue with reports containing un-escaped special characters has been addressed. • Users are able to unlock advanced DDos filters from the SMS interface. • Device management performance improvements are included. • Traffic management filters with IPv6 entries that had source and destination of ANY IPv6, and a user-defined IPv6 of '::0/0', and migrated from 4.6 would have resulted in events on devices even though appropriate traffic management trust filters were configured for the IP address. This issue has been addressed. • Issues with profile overrides and exceptions have been addressed in this release. • Device hostname configuration now supports non-standard top-level domain names. • Restarting SMS while distributions are in queue no longer suspend the distributions. Restarting in-queue distributions after a restart are now successful. • Improved threadpool management and usage issues have been addressed. Login		

Version	Description of Changes	Rationale	Impact
	failures to the SMS client no longer occur, and port statistics no longer show as blank. • The requirement for Bugtraq ID and CVE ID to end with a comma for Qualys-CSV file imports has been removed. • When a stack is in a degraded state, it no longer shows a special icon or 'fallback'. The degraded state now shows only on the Summary tab. • Filter descriptions now display https links as active links.		
Trend Micro TippingPoint Security Management System 5.2.0	• Two types of APIs are available for use with the SMS. o The SMS Web API Guide describes HTTP APIs can be used to access multiple SMS features if users have HTTPS service to the SMS. o The SMS REST API online help describes RESTful APIs available to access SMS functionality. Users can access the API from the SMS web Management console. • Users can configure a TPS device to use the SMS as a remote authentication server. • Remote Authentication Dial-In User Server (RADIUS) is available to authenticate user login requests. • SMS configuration includes creating Splunk syslog format and configuring a syslog exporter to send events and messages to Splunk. • Users can schedule distributions for Auxiliary Digital Vaccines (ThreatDV). • Selective acknowledgement (SACK) improves profile distribution times across	• Release Notes describes the Web and REST APIs are available for use with the from the SMS Web Management console. • Section 2.1 of the ST states the Web Management console is excluded from the scope of evaluation, as are its associated HTTP and REST APIs. • Remote authentication feature using a TPS device is excluded from the scope of evaluation. • Remote authentication feature using RADIUS has already been covered in the	CB consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	remote or otherwise burdened networks. • This release supports NTLMv3 for the TMC proxy. • Users can easily reorder Traffic Management Filters. • The Licensing Details panel displays the license expiration date for each device managed on the SMS. • Users can import up to 100 user-defined tag categories on the SMS. • The SMS Web Management console displays the banner message, the previous login, and the number of days as the count period.	certified TOE v5.1.0. • The other changes and new features do not affect the Security Functional Requirements of the TOE.	

2.2 Changes to the SFRs claimed in the ST

6 Changes described below do not affect the claimed Security Functional Requirements (SFRs) in the ST Ref ([5]).

Table 3 – SFR changes/additions

SFR	Description of Changes	Rationale	Impact
FMT_MOF.1.1(2), FTA_TAB.1.1	The SMS Web Management console displays the banner message, the previous login and the number of days as the count period.	The enhanced functionality stated does not affect these SFRs as this feature is not in subject of evaluation.	CB consider it as **Minor**
FMT_MTD.1.1(1), FMT_SMF.1.1, FTP_ITC.1.3	User can monitor certain SMS data, such as action set logic, distribution history, and dashboards on the Trend Micro TippingPoint Splunk App. SMS configuration includes creating a Splunk syslog format and configuring a syslog exporter to send events and messages to Splunk.	The enhanced functionality stated does not affect this SFR as this feature is not in subject of evaluation.	CB consider it as **Minor**

SFR	Description of Changes	Rationale	Impact
FTA_TAB.1.1	The SMS Web Management console displays the banner message, the previous login, and the number of days as the count period.	The enhanced functionality stated does not affect this SFR as this feature is not in subject of evaluation.	CB consider it as **Minor**
FTP_ITC.1.3	New release supports NTLMv3 for the TMC proxy.	The enhanced functionality stated does not affect this SFR as this feature is not in subject of evaluation.	CB consider it as **Minor**

3 Affected Developer Evidence

7 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 4 – Affected Developer Evidence

Evidence	Description of Changes	Rationale	Impact
Trend Micro TippingPoint Security Management System Security Target, Version 1.0, 07 October 2019	• The document version and document date have been updated. • TOE reference throughout the document has been updated to reflect the change in TOE version from the developer. • Section 3.3 has been updated to note that TLS 1.2 is not supported if the TOE has been placed into its optional FIPS mode. • "TLS_RSA_WITH_3DES_CBC_SHA" cipher was changed to "TLS_ECDHE_RSA_WITH_AES_256 _GCM_SHA384". Also, the TOE supports this additional TLS ciphersuite: TLS_ECDHE_RSA_WITH_AES_256 _CBC_SHA384. • List of TOE documentation in Section 5 has been updated to reflect the latest versions of guidance documentation.	No changes have been made to the SFRs or functionality that was included in the scope of the original evaluation.	CB consider it as **Minor**
Trend Micro TippingPoint Security Management System Configuration Management Documentation, Version 1.0, 07 October 2019	• The document version and document date have been updated. • TOE reference throughout the document has been updated to reflect the change in TOE version from the developer. • TOE Configuration List in Section 3 has been updated to reflect the latest versions of evaluation documentation.	No changes have been made to the SFRs or functionality that was included in the scope of the original evaluation.	CB consider it as **Minor**
Trend Micro TippingPoint Security Management	• TOE reference has been updated to reflect latest version.	No changes have been made to the SFRs or	CB consider

Evidence	Description of Changes	Rationale	Impact
System (SMS) User Guide, 5.2.0, February 2019	• Document date has been updated. • Description and references for SMS Rest API has been added.	functionality that was included in the scope of the original evaluation.	it as **Minor**
Trend Micro TippingPoint Security Management System (SMS) Command Line Interface Reference, 5.2.0, April 2019	• TOE reference has been updated to reflect the latest version. • Document date has been updated.	No changes have been made to the SFRs or functionality that was included in the scope of the original evaluation.	CB consider it as **Minor**
Trend Micro TippingPoint Security Management System (SMS) Web API Guide, 5.2.0, April 2019	• TOE reference has been updated to reflect latest version. • Document date has been updated. • Description and references for SMS Rest API has been added.	No changes have been made to the SFRs or functionality that was included in the scope of the original evaluation.	CB consider it as **Minor**
Trend Micro TippingPoint Virtual Security Management System (vSMS) Getting Started Guide, 5.2.0, July 2019	• TOE reference has been updated to reflect latest version. • Document date has been updated.	No changes have been made to the SFRs or functionality that was included in the scope of the original evaluation.	CB consider it as **Minor**

4 Result of Analysis

8 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 [5]) as required in accordance of Assurance Continuity: CCRA Requirements version 2.1 (2012-06-01) June 2012 (Ref [11]).

9 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 Impact Analysis Report (IAR), A0005408-IAR, Version 1.0, 18 October 2019

[2] Trend Micro TippingPoint Security Management System Release Notes, Version 5.1.1

[3] Trend Micro TippingPoint Security Management System Release Notes, Version 5.2

[4] Trend Micro TippingPoint Security Management System Security Target, Version 1.0, 21 August 2018 – Version 5.1.0

[5] Trend Micro TippingPoint Security Management System Security Target, Version 1.0, 7 October 2019 – Version 5.2.0

[6] Trend Micro TippingPoint Security Management System Configuration Management Documentation, Version 1.0, 7 October 2019

[7] Trend Micro TippingPoint Security Management System (SMS) User Guide, 5.2.0, February 2019

[8] Trend Micro TippingPoint Security Management System (SMS) Command Line Interface Reference, 5.2.0, April 2019

[9] Trend Micro TippingPoint Security Management System (SMS) Web API Guide, 5.2.0, April 2019

[10] Trend Micro TippingPoint Virtual Security Management System (vSMS) Getting Started Guide, 5.2.0, July 2019

[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] ISCB Product Certification Schemes Policy (Product_SP), v1b, March 2018.

[16] ISCB Evaluation Facility Manual (ISCB_EFM), v1a, March 2018.

[17] Trend Micro TippingPoint Security Management System Configuration Management V5.1.0 Evaluation Technical Report, EAU000426-S046-ETR, Version 1.0, 10 September 2018.

--- END OF DOCUMENT ---