National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Trned Micro, Inc.

Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6

Report Number: CCEVS-VR-VID11083-2020
Dated: July 6, 2020
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant
Patrick Mallett, PhD
Lisa Mitchell
The MITRE Corporation

Ken Elliott
Meredith Hennan
Aerospace Corporation

Common Criteria Testing Laboratory

Justin Bettencourt
Raymond Smoley
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation Team of the evaluation of Trend Micro Virtual Mobile Infrastructure (TMVMI), version 6 solution provided by Trend Micro, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in July 2020. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the Protection Profile for Application Software, Version 1.3, 01 March 2019 (ASPP13) with Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 (PKGTLS11).

The Target of Evaluation (TOE) is the Trend Micro Virtual Mobile Infrastructure (TMVMI), version 6.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The Validation Team monitored the activities of the Evaluation Team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation Team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation Team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6 (ASPP13) Security Target, Version 0.4, 06/29/2020 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing

laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6 (Specific models identified in Section 3.1)
PP	Protection Profile for Application Software, Version 1.3 (PP_APP_V1.3) with Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 (PKGTLS11)
ST	Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6 (ASPP13) Security Target, Version 0.4, 06/29/2020
Evaluation Technical Report	Evaluation Technical Report for Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6, Version 0.2 June 29, 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	SK Infosec, Inc.
Developer	Trend Micro, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is the Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6.

The TOE is the Virtual Mobile Infrastructure Client application for Android and iOS platforms. The TOE is a thin client providing access to a Trend Micro Virtual Mobile Infrastructure (VMI) server from a mobile device.

3.1 TOE Evaluated Platforms

The TOE was tested on the following mobile devices.

Device Name	Processor	Operating System
Samsung Galaxy S10	Qualcomm Snapdragon 855 (SDM855)	Android 9.0
Apple iPhone 7	Apple A10	Apple iOS 13.1

Table 1 - Tested Devices

The TOE runs on a Samsung Galaxy S10, Note 10, S9, Note 9, S8, and Note 8 devices running Android 9. The TOE also runs on Apple iOS 13.1 on iPhone devices including iPhone X, 8, 7, and 6. The same application runs on all Android devices and the same application runs on all iPhone devices. The S10 was used for Android testing and iPhone 7 was used for iOS testing. All other devices are claimed as equivalent.

Device Name	Processor	Operating System
Samsung Devices		
Galaxy S10+	Qualcomm Snapdragon 855 (SDM855)	Android 9.0
Galaxy S10	Qualcomm Snapdragon 855 (SDM855)	Android 9.0
Galaxy Note10	Qualcomm Snapdragon 855 (SDM855)	Android 9.0
Galaxy Note10+	Qualcomm Snapdragon 855 (SDM855)	Android 9.0
Galaxy Note10+ 5G	Qualcomm Snapdragon 855 (SDM855)	Android 9.0
Galaxy S9+	Qualcomm Snapdragon 845 (SDM845)	Android 9.0
Galaxy S9	Qualcomm Snapdragon 845 (SDM845)	Android 9.0
Galaxy Note 9	Qualcomm Snapdragon 845 (SDM845)	Android 9.0
Galaxy S8+	Qualcomm Snapdragon 835 (SDM845)	Android 9.0
Galaxy S8	Qualcomm Snapdragon 835 (SDM845)	Android 9.0
Galaxy Note 8	Qualcomm Snapdragon 835 (SDM845)	Android 9.0
Apple Devices		
iPhone XS	Apple A12 Bionic	iOS 13.1
iPhone XS Max	Apple A12 Bionic	iOS 13.1
iPhone XR	Apple A12 Bionic	iOS 13.1
iPhone X	Apple A11	iOS 13.1
iPhone 8 Plus	Apple A11	iOS 13.1
iPhone 8	Apple A11	iOS 13.1
iPhone 7 Plus	Apple A10	iOS 13.1
iPhone 7	Apple A10	iOS 13.1
iPhone 6 Plus	Apple A9	iOS 13.1
iPhone 6	Apple A9	iOS 13.1

Table 2 - Equivalent Devices

3.2 TOE Architecture

A VMI client is a service that hosts independent workspaces for every user. A user workspace is based on the Android operating system, which is accessible via the VMI mobile client application installed on an Android or iOS mobile device. Using the VMI client application, users can access the same mobile environment that includes all their applications and data from any location, without being tied to a single mobile device. The VMI client presents only the interface offered by the VMI server and ensures that communication with the server utilizes secured protocols.

The TOE when executed, connects to the specified Trend Micro Virtual Mobile Infrastructure (VMI) server, authenticating the server's certificate received while negotiating the HTTPS or TLS session. The TOE is responsible only for protecting data-in-transit between the physical mobile device and the VMI server.

3.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the device on which the TOE resides.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted path/channels

4.1 Cryptographic support

The VMI client utilizes platform APIs to provide secure network communication using HTTPS. The client also uses its own cryptography to establish trusted TLS channels to transmit data to the VMI Server.

4.2 User data protection

The VMI client informs a user of hardware and software resources the TOE accesses. It uses the platform’s permission mechanism to get a user’s approval for access. The user initiates a secure network connection to the VMI server using the TOE. In general, sensitive data resides on the VMI server and not the VMI Client, although the client does store encrypt credentials.

4.3 Identification and authentication

The VMI client performs certificate validation checking for TLS connections. Both Android and iOS applications support OCSP stapling when performing validity checks.

4.4 Security management

The VMI client does not include any predefined or default credentials, and utilize the platform recommended storage process for configuration options

4.5 Privacy

The VMI client does not collect any PII and does not transmit any PII over a network.

4.6 Protection of the TSF

The VMI client relies on the physical boundary of the evaluated platform as well as the Android and iOS operating system for the protection of the TOE's application components. All compiled VMI client code is designed to utilize compiler provided anti-exploitation capabilities. The VMI client application is available through the Google Play store and the Apple store.

4.7 Trusted path/channels

The VMI client utilizes platform API to establish HTTPS connections to a VMI server. The client also uses OpenSSL to establish TLS connections to a VMI server.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Application Software, Version 1.3 (ASPP13) with Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 (PKGTLS11)

That information has not been reproduced here and the ASPP13/PKGTLS11 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP13/PKGTLS11 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the ASPP13/PKGTLS11 and performed by the Evaluation Team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.

7 Documentation

The following document was available with the TOE for evaluation:

- Trend Micro Virtual Mobile Infrastructure (TMVMI) User's Guide, Version 0.3, 06/29/2020

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 0.2, June 29, 2020 (DTR), as summarized in the evaluation Assurance Activity Report.

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The Evaluation Team verified the product according a Common Criteria Certification document and ran the tests specified in the ASPP13/PKGTLS11 including the tests associated with optional requirements. The AAR, in sections 1.1 and 3.4.1, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

9 Evaluated Configuration

See Section 3.1.

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Trend Micro Virtual Mobile Infrastructure (TMVMI) TOE to be Part 2 extended, and to meet the SARs contained in the ASPP13/PKGTLS11.

10.1 Evaluation of the Security Target (ASE)

The Evaluation Team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Trend Micro Virtual Mobile Infrastructure (TMVMI) products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the Evaluation Team, and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

10.2 Evaluation of the Development (ADV)

The Evaluation Team applied each ADV CEM work unit. The Evaluation Team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the Evaluation Team performed the assurance activities specified in the ASPP13/PKGTLS11 related to the examination of the information contained in the TSS.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

10.3 Evaluation of the Guidance Documents (AGD)

The Evaluation Team applied each AGD CEM work unit. The Evaluation Team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation Team ensured the adequacy of the administrator guidance in

describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation Team applied each ALC CEM work unit. The Evaluation Team found that the TOE was identified.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each ATE CEM work unit. The Evaluation Team ran the set of tests specified by the assurance activities in the ASPP13/PKGTLS11 and recorded the results in a Test Report, summarized in the AAR.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

10.6 Vulnerability Assessment Activity (VAN)

The Evaluation Team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 6/25/2020 with the following search terms: "Trend Micro", "VMI", "SKInfosec", "Trend Micro VMI", "openSSL", "AFNetworking", "ASIHTTPRequest", "Libegal", "Libjpeg", "LibOpenGLRender", "FMDB", "G726", "EGOImageLoading", "MBProgressHUD", "SFHFKeychainUtils", "Reachability", "SBJson", "SPLockScreen", "TheSidebarController", "JSBadgeView", "Skia", "x264-152", "ffmpeg", "com.google.code.gson", "org.samba.jcifs", "fr.avianey.com.viewpagerindicator", "com.github.anzaizai:EasySwipeMenuLayout". No residual vulnerabilities exist in the TOE.

Additionally, the evaluator used Windows Defender Security to scan the TOE for viruses, ensuring to check that definitions were current first. In each application variant no issues were identified.

The validators reviewed the work of the Evaluation Team, and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the

evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

10.7 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's testing also demonstrated the accuracy of the claims in the ST.

The Validation Team's assessment of the evidence provided by the Evaluation Team is that it demonstrates that the Evaluation Team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the CC Guide document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6 (ASPP13) Security Target, Version 0.4, 06/29/2020.*

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is

complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Protection Profile for Application Software, Version 1.3, 01 March 2019 (ASPP13) with Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 (PKGTLS11).

[5] Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6 (ASPP13) Security Target, Version 0.4, 06/29/2020 (ST).

[6] Assurance Activity Report (ASPP13/PKGTLS11) for Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6, Version 0.2, June 29, 2020 (AAR).

[7] Detailed Test Report for Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 0.2, June 29, 2020 (DTR).

[8] Evaluation Technical Report for Trend Micro Virtual Mobile Infrastructure (TMVMI), Version 6, Version 0.2, June 29, 2020 (ETR).