MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

# C135 Certification Report

## Vidcall Version 8.2

File name: ISCB-5-RPT-C135-CR-V1
Version: V1
Date of document: 17 February 2025
Document classification : PUBLIC


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

# C135 Certification Report

## Vidcall Version 8.2

17 February 2025

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:*** | C135 Certification Report |
| ***DOCUMENT REFERENCE:*** | ISCB-5-RPT-C135-CR-V1 |
| ***ISSUE:*** | V1 |
| ***DATE:*** | 17 February 2025 |
| ***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. 200601006881 (726630-U)

*Printed in Malaysia*

# Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 7th March 2025, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at https://iscb.cybersecurity.my/index.php/certification/product-certification/mycc/ and the Common Criteria Recognition Arrangement (CCRA) Portal at http://www.commoncriteriaportal.org .

# Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# Document Change Log

| RELEASE | DATE | PAGES AFFECTED | REMARKS/CHANGE REFERENCE |
|---|---|---|---|
| d1 | 17 February 2025 | All | Initial draft |
| v1 | | All | |

# Executive Summary

The Target of Evaluation (TOE) is Vidcall Version 8.2. The TOE is a web and software application designed to facilitate virtual meetings, conferences, chat and messaging and collaborations while prioritizing the protection of sensitive information and the privacy of participants. The TOE enables individuals or groups to connect and interact in real-time, regardless of their physical locations. The TOE typically offers a range of features to make virtual meetings, chat and messaging are more effective and efficient, including video and audio conferencing, peer to peer call, screen sharing, meeting recording, watermark, file sharing and history.

The Vidcall Version 8.2 is designed with robust security features to safeguard sensitive information, maintain privacy, and to prevent unauthorized access or data breaches during online interactions. The security features implemented by the TOE are including Security Audit, Cryptographic Support, Identification and Authentication, and Secure Communication.

The scope of the evaluation is defined by the Security Target [6] which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL 2).

This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by CyberSecurity Malaysia SEF (CSM MySEF) and the evaluation was completed on 5 February 2025.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC website and the Common Criteria Recognition Arrangement (CCRA) website.

It is the responsibility of the user to ensure that Vidcall Version 8.2 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref **Error! Reference source not found.**) and this Certification Report prior to deciding whether to purchase the product.

# Table of Contents

# Index of Tables



# Index of Figures

# 1 Target of Evaluation

## 1.1 TOE Description

1 The TOE is a virtual meetings, conferences, chat and messaging and collaborations web and software application that provides security functionality such as Security Audit, Cryptographic Support Identification and Authentication and Secure Communication.

2 A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture as follows.

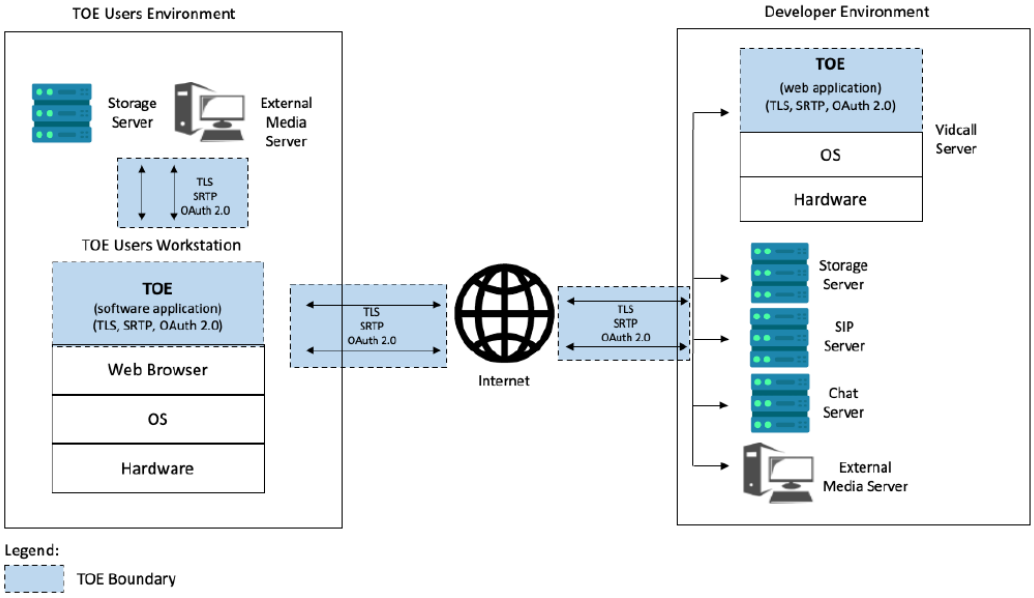


Figure 1: Example TOE Deployment

3 The TSF includes the following security functions:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Secure Communication

## 1.2 TOE Identification

4 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

| | |
|---|---|
| **Evaluation Scheme** | Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme |
| **Project Identifier** | C135 |
| **TOE Name** | Vidcall |
| **TOE Version** | Version 8.2 |
| **Security Target Title** | VidCall Version 8.2 Security Target |
| **Security Target Version** | 1.2 |
| **Security Target Date** | 31 December 2024 |
| **Assurance Level** | Evaluation Assurance Level 2 |
| **Criteria** | Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2]) |
| **Methodology** | Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3]) |
| **Protection Profile Conformance** | None |
| **Common Criteria Conformance** | CC Part 2 Conformant<br>CC Part 3 Conformant<br>Package conformant to EAL 2 |
| **Sponsor** | Advanced Product Design Sdn Bhd.<br>No.209, Jalan Impian Emas 22<br>Taman Impian Emas,<br>81300, Skudai, Johor |
| **Developer** | Advanced Product Design Sdn Bhd.<br>No.209, Jalan Impian Emas 22<br>Taman Impian Emas,<br>81300, Skudai, Johor |
| **Evaluation Facility** | CyberSecurity Malaysia MySEF (CSM MySEF) |

## 1.3 Security Policy

5 There is no organisational security policies defined regarding the use of TOE.

## 1.4 TOE Architecture

6 The TOE includes both physical and logical boundaries which are described in Section 1.6 of the Security Target (Ref [6]).

### 1.4.1 Logical Boundaries

7 The TOE consists of security functions provided by the TOE that are identified in the Security Target ([6]).

Table 2: VidCall Logical Boundaries

| | |
|---|---|
| Security Audit | The TOE generates audit records for security events such as TOE user's login and logout activities, reset password and reset password request. TOE users have the capability to view the audit logs |
| Cryptographic Support | The TOE implements encryption algorithms that utilize ECC (Prime256v1), AES256 CBC Mode, ECIES (Prime256v1), ECDSA (Prime256v1) and AES-256-CM-HMAC-SHA1-80. |
| Identification & Authentication | TOE users are required to identify and authenticate before to perform the TOE's operations stated in the Security Target section 6.4. |
| Secure Communication | The TOE can protect the user data from disclosure and modification by using TLS v1.2, OAuth 2.0 Bearer Tokens (RESTful APIs) and SRTP (AES-256-CM-HMAC-SHA1-80) as a secure communication |

### 1.4.2 Physical Boundaries

8 The TOE shown in Figure 1 consists of two parts: TOE web application and TOE software application. The TOE web application is used by the TOE users to perform TOE users' registration, change TOE user's password, enable two-factor (2FA) authentication. The TOE user accessed the TOE web application via a supported web browser.

9 While the TOE software application (installed on the TOE user's workstation) is used to perform TOE operation such as video conferencing, audio conferencing, audio/video

peer to peer call, screen sharing, chat and messaging, meeting recording, watermark, file sharing and history.

10 In order to perform the TOE operation, the TOE will need to communicate with several servers that are hosted locally in the developer environment which is located in Malaysia. There are five (5) servers involved but not in the scope of evaluation:

- **VidCall Server:** Web Server is a server to host the TOE web application and system management console. System management console is a web-based system used by the authorised user to manage the TOE users. Note that the system management console is out of the scope of evaluation.
- **External Media Server:** The Media Server is a PC that utilized an Intel GPU and is connected to the internet via an Ethernet cable, which is also known as Ethernet intel. The PC used for standby media server purposes is out of the scope of testing. This ready media server will act as a host if the TOE user who wants to host the meeting does not meet the media server requirement.
- **SIP Server:** a SIP server or SIP proxy processes session initiation protocol (SIP) requests. This server is the main element of an IP private branch exchange. SIP is an internet protocol used to initiate and receive voice and video communication by transmitting data packets across an internet connection. This enables the quick and easy transmission of SIP calling between two or more parties.
- **Chat Server**: A Chat server is a central application or system in a client-server architecture that manages and maintains real-time communication among multiple users connected over the internet. It facilitates message exchange and ensures that the chat data is delivered correctly to the intended recipients. Chat messages are end-to-end encrypted, and each message is digitally signed.
- **Storage Server**: The storage server is used to temporary store the files attached in the TOE (software application). When a user sends an attachment to another user, the TOE (software application) will upload the encrypted file to the storage server. The recipient will then download the encrypted file from the storage server. Data stored is encrypted for both chat messages and attachment and can only be accessed via successful log in to TOE (software application). As stated above, storage server is a temporary storage location for file attachment during chat and messaging and video conferencing. A storage server can be located inside or outside of developer environment or at TOE user designated location.

## 1.5 Clarification of Scope

11 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

12 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

13 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

## 1.6 Assumptions

14 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

Table 3: Assumptions for the TOE

| Assumption | Statements |
|---|---|
| A.AUTHORISE | The TOE user is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the developer |
| A.OPSYS | The operating systems supporting the TOE components protect against the unauthorised access, modification or deletion of the individual TOE components that they host. |
| A.UPDATE | The underlying platform on which the TOE operates will be regularly updated with the latest security patches and fixes to ensure data stored on the platform remains protected and secure. |
| A.FIREWALL | The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE. |

| Assumption | Statements |
|---|---|
| A.OS | The authorised user shall ensure the OS backend server have been hardened to counter the perceived threats. |
| A.TIMESTAMP | The platforms on which the TOE operate shall be able to provide reliable time stamps. |

## 1.7 Evaluated Configuration

15 The TOE is to be configured according to the Preparative Guidance.

16 The TOE is delivered as a software application installer that will be downloaded (https://1dataonline.com/download/vidcall_8.2.exe) and installed by the TOE user.

17 The TOE user must ensure the minimum hardware requirement of Vidcall media server is PC/Server with Intel GPU and the connection with Local area network by using LAN cable. A media server must be a PC/Server with Intel GPU that supports Intel Quick Sync Video and connected to Ethernet with reliable high-speed internet.

18 After the installation done, the TOE user needs to browse to the TOE web application (https://1dataonline.com/authentication/Register) to register for a new account. Upon registration, TOE users will receive a verification email in TOE user's email inbox.

19 User login: After the registration and email validation, the TOE users must wait till the authorised user activation before they are able to login via the TOE software application (vidcall_8.2.exe (Windows)) and TOE web application (https://1dataonline.com/authentication/Login).

## 1.8 Delivery Procedures

20 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

### 1.8.1 TOE Delivery

21 Once the new version of the TOE or key application component is released it is verified by the developers by checking the version of the TOE and checking the version with

the Release logs. Only after a successful verification will the TOE be accepted and be put onto production server for use.

i. ***User Registration:*** The TOE software application will be downloaded and installed by the TOE user. The TOE software application can be downloaded by the TOE user by visiting to https://1dataonline.com/home/homepage. On the homepage, simply click the "Download" button to download the installer necessary for installation. For new registration, TOE users need to browse to the TOE web application (https://1dataonline.com/authentication/Register) to register for a new account. They have to fill out all the required information such as Email, Display Name, Password and Retype Password and then click 'SIGN ME UP' to register. Upon registration, TOE users will receive a verification email in TOE user's email inbox.

ii. ***User login:*** After the registration and email validation, the TOE users have to wait till the authorised user activation before they are able to login via the TOE software application (vidcall_8.2.exe (Windows)) and TOE web application (https://1dataonline.com/authentication/Login).

22 If any issues occur, the TOE users can communicate via a phone call, email or meet face-to-face with the developer to resolve the issue via contact information provided below:

Advanced Product Design Sdn Bhd (737874-A)
No 209, Jalan Impian Emas 22,
Taman Impian Emas, 81300 Skudai, Johor, Malaysia.
Website: www.biocryptodisk.com
Email: marketing@biocryptodisk.com
Phone No: +607-550 4855 / +6012-7769949

# 2 Evaluation

23 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

## 2.1 Evaluation Analysis Activities

24 The evaluation activities involved a structured evaluation of the TOE, including the following components:

### 2.1.1 Life-cycle support

25 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

26 The evaluators confirmed that the configuration list includes TOE itself, the parts that comprise the TOE the evaluation evidence required by the SARs in the the Security Target (Ref [6]).

27 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

### 2.1.2 Development

**Architecture**

28 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

29 The security architecture description describes the security domains maintained by the TSF.

30 The initialisation process described in the security architecture description preserves security.

31 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

**Functional Specification**

32 The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

33 The evaluators also examined the presentation of the TSFI and determined that:

- It completely identifies all parameters associated with every TSFI; and
- It completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

34 The evaluators also confirmed that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

**TOE Design Specification**

35 The evaluators examined the TOE design (contained in [8]) and determined that the structure of the entire TOE is described in terms of subsystems.

36 The evaluators also determined that all subsystems of the TSF are identified.

37 The evaluators determined that interactions between the subsystems of the TSF were described.

38 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

39 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

40 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

41 The evaluators determined that all SFRs were covered by the TOE design and concluded that the TOE design was an accurate instantiation of all SFRs.

### 2.1.3 Guidance documents

42 The evaluators examined the operational user guidance determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

43 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

44 The evaluators examined the operational user guidance in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

45 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

46 The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

### 2.1.4 IT Product Testing

47 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by CyberSecurity Malaysia MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

48 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

49 At EAL 2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

50 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 4: Independent Functional Test

| TEST ID/SFR | DESCRIPTIONS | RESULTS |
|---|---|---|
| Test Group A – Identification and Authentication | | |
| A.1 – TOE User Login<br>FIA_UID.2<br>FIA_UAU.2<br>FIA_ATD.1 | To verify that each users to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of that user. | Passed. Result as expected. |
| A.2 – Two-Factor Authentication (2FA) Login<br>FIA_ATD.1<br>FIA_UID.2<br>FIA_UAU.2 | To verify that TOE maintains username, and 2FA authentication code belonging to individual users | Passed. Result as expected. |

| TEST ID/SFR | DESCRIPTIONS | RESULTS |
|---|---|---|
| | | |
| A.3 – Perform Authorised Function<br><br>FMT_SMF.1 | To verify the authorized user can perform their designated functions.<br>o [Sign Up New User].<br>o [Edit Display Name and Enable/Disable 2FA]<br>o [Change Picture]<br>o [Forgot Password]<br>o [Signing Out]<br>o [Sign Up New User]<br>o [Forgot Password]<br>o [Create New Meeting Room]<br>o [Edit Meeting Details]<br>o [Start a Meeting]<br>o [Join a Meeting]<br>o [Validate Features during a Meeting]<br>o [Deleting a Meeting and View Meeting History]<br>o [View Chat Messages]<br>o [Send Files Attachment using Chat function]<br>o [Sending Messages in Email format (Attach Files, Reply Email)]<br>o [Forward Chat Messages]<br>o [Search for Messages in Chat] | Passed. Result as expected. |

| TEST ID/SFR | DESCRIPTIONS | RESULTS |
|---|---|---|
| | o [Deleting a Message (Delete for Me, Delete for Everyone, Cancel)]<br>o [Reply Chat Messages]<br>o [Emoji]<br>o [Add Contact]<br>o [Add Group]<br>o [Calling, Chat and Delete Contact]<br>o [Receiving a Call]<br>o [Searching for Contact]<br>o [ Group Chat (View Group Chat, Create a New Group Chat, Edit Group Chat, Delete Group Chat)]<br>o [Change Profile Picture]<br>o [Mic and Speaker Testing]<br>o [Camera Testing]<br>o [File Upload]<br>o [Download Chat and Meeting History]<br>o [About (Update)]<br>o [Signing Out] | |
| A.4 – Password Policy<br>FIA_SOS.1 | To verify that TOE provides a mechanism to verify that secrets meet 8 characters in length, at least 1 uppercase letter, at least 1 number, and at least 1 special characters. | Passed. Result as expected. |

| TEST ID/SFR | DESCRIPTIONS | RESULTS |
|---|---|---|
| Test Group B – Secure Communication | | |
| B.1 – Encrypted Communication<br>FTP_TRP.1 | To verify the encrypted communication between TOE user and TOE. | Passed. Result as expected. |
| Test Group C – Cryptographic Support | | |
| C.1 – Generate Cryptographic Key<br>FCS_CKM.1 | To verify that TOE able to generate cryptographic key. | Passed. Result as expected. |
| C.2 – Distribute Cryptographic Key<br>FCS_CKM.2 | To verify that TOE able to distribute cryptographic key. | Passed. Result as expected. |
| C.3 – Key Zeroization<br>FCS_CKM.4 | To verify that TOE User able to delete keys from TOE (key zeroization). | Passed. Result as expected. |
| C.4 – Perform Cryptographic Operation<br>FCS_COP.1 | To verify that TOE correctly uses the specified cryptographic algorithm and key size during cryptographic operations. | Passed. Result as expected. |
| Test Group D – Security Audit | | |
| D.1 – Generate Audit Report<br>FAU_GEN.1 | To verify that TOE able to generate audit report. | Passed. Result as expected. |
| D.2 – Read Audit Report<br>FAU_SAR.1 | To verify that TOE user able to read all audit information from the audit records. | Passed. Result as expected. |

51 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration testing

52 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

53 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation

54 The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched:

a) www.google.com

b) www.yahoo.com

c) www.bing.com

d) www.cve.mitre.org

55 The penetration tests focused on:

a) Cryptographic Failures;

b) Injection;

c) Security Misconfiguration;

d) Identification and Authentication Failure;

e) Poor Error Handling;

f) Server-Side Request Forgery (SSRF);

g) Bypassing OS on the Underlying Platform;

h) Bypassing physical access to the developer environment;

i) Software and data integrity failure;

j) Insecure Communication;

k) Broken Authentication and Session Management;

l) Security Logging and Monitoring Failures; and

m) Bypassing TOE installed from non-trusted platform.

2.1.4.4 Residual Vulnerability

56 The evaluators have identified a residual vulnerability in the PHP version used by the TOE, which is version 7.4.7. The ECDSA key length of 256 bits is only supported by PHP version 7.4.7.

57 The residual vulnerability in PHP version 7.4.7 is a known vulnerability, listed below:

a) CVE-2022-37454: Integer Overflow or Wraparound

b) CVE-2024-4577: PHP-CGI OS Command Injection Vulnerability

c) CVE-2021-21708: Use After Free

58 These residual vulnerabilities would require more advanced skills or resources to exploit where it is beyond Basic attack potential.

2.1.4.5 Testing Results

59 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

# 3 Result of the Evaluation

60 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7], the Malaysian Common Criteria Certification Body certifies the evaluation of Vidcall Version 8.2 performed by CyberSecurity Malaysia MySEF.

61 CyberSecurity Malaysia MySEF found that Vidcall Version 8.2 upholds the claims made in the Security Target (Ref [6] and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

62 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

## 3.1 Assurance Level Information

63 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE to understand the security behaviours.

64 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

65 EAL 2 also provides assurance through use of a configuration management system and the secure delivery procedures.

## 3.2 Recommendation

66 These recommendations are outside the scope of SAMM accreditation.

67 The Malaysian Certification Body (MyCB) is strongly recommends that:

a) It is advisable for the users to test the entire TOE if there are updates, patches, or new features added to ensure that the current features are not jeopardized.

b) It is advisable for the users to test on different platforms, such as using laptop and desktop views, to ensure the user interface displayed correctly.

c) It is advisable for the users to conduct performance testing for the TOE to determine the maximum and minimum number of users that able to participate in a video conference effectively.

d) It is advisable for the TOE to provide notifications to users regarding meeting invitations and any changes to meeting details.

# Annex A References

## A.1 References

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

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

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

[4] MyCC Scheme Requirement (MYCC_REQ), v1b, CyberSecurity Malaysia, July 2023.

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

[6] Vidcall Version 8.2 Security Target, Version 1.2, 31 December 2024.

[7] CyberSecurity Malaysia MySEF E052, Evaluation Technical Report, Version 1.0, 5 February 2025.

[8] Vidcall Version 8.2 Design Documentation, Version 1.0, 31 December 2025.

## A.2 Terminology

### A.2.1 Acronyms

Table 5: List of Acronyms

| Acronym | Expanded Term |
|---|---|
| CB | Certification Body |
| CC | Common Criteria (ISO/IEC15408) |
| CEM | Common Evaluation Methodology (ISO/IEC 18045) |
| CCRA | Common Criteria Recognition Arrangement |
| IEC | International Electrotechnical Commission |
| ISO | International Organisation for Standardization |
| ISCB | Information Security Certification Body |
| MyCB | Malaysian Common Criteria Certification Body |
| MyCC | Malaysian Common Criteria Evaluation and Certification Scheme |
| MyCPR | MyCC Scheme Certified Products Register |
| MySEF | Malaysian Security Evaluation Facility |
| PP | Protection Profile |

| Acronym | Expanded Term |
|---|---|
| ST | Security Target |
| TOE | Target of Evaluation |

### A.2.2 Glossary of Terms

Table 6: Glossary of Terms

| Term | Definition and Source |
|---|---|
| CC International Interpretation | An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants. |
| Certificate | The official representation from the CB of the certification of a specific version of a product to the Common Criteria. |
| Certification Body | An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA |
| Consumer | The organisation that uses the certified product within their infrastructure. |
| Developer | The organisation that develops the product submitted for CC evaluation and certification. |
| Evaluation | The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC 17065 |
| Evaluation and Certification Scheme | The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA. |
| Interpretation | Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**. |
| Certifier | The certifier responsible for managing a specific certification task. |
| Evaluator | The evaluator responsible for managing the technical aspects of a specific evaluation task. |
| Maintenance Certificate | The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme. |

| Term | Definition and Source |
|---|---|
| National Interpretation | An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only. |
| Security Evaluation Facility | An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy |
| Sponsor | The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer. |

--- END OF DOCUMENT ---