National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Wickr Enterprise Server 1.30.0

Report Number:	**CCEVS-VR-VID11321-2023**
Dated:	**12 June 2023**
Version:	**1.0**

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Jerome Myers

Marybeth Panock

Mike Quintos

The Aerospace Corporation

Common Criteria Testing Laboratory

Allen Sant

Anthony Apted

Armin Najafabadi

Josh J. Marciante

Pascal Patin

Leidos Inc.

Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Wickr Enterprise Server 1.30.0 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in June 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the following document:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021

The TOE is Wickr Enterprise Server 1.30.0.

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 documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the Security Target. 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 Wickr Enterprise Server 1.30.0 Security Target, Version 1.0, 28 March 2023 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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 Product Compliant List (PCL).

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): the unique identification of the document 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
Evaluated Product	Wickr Enterprise Server 1.30.0
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Wickr Enterprise Server 1.30.0, evaluated on Ubuntu 18.04.
Protection Profile	Protection Profile for Application Software, Version 1.4, 7 October 2021
Security Target	Wickr Enterprise Server 1.30.0 Security Target, Version 1.0, 28 March 2023
Evaluation Technical Report	Evaluation Technical Report for Wickr Enterprise Server 1.30.0, Version 1.0, 25 May 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
Sponsor & Developer	Wickr LLC W 31st Street New York, NY 10001
Common Criteria Testing Lab (CCTL)	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	June 2023

Item	**Identifier**
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*Protection Profile for Application Software*, Version 1.4, 7 October 2021
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
Evaluation Personnel	Allen Sant, Leidos Inc Anthony Apted, Leidos Inc Armin Najafabadi, Leidos Inc Josh J. Marciante, Leidos Inc Pascal Patin, Leidos Inc
Validation Personnel	Jerome Myers: Senior Validator, The Aerospace Corporation Marybeth Panock: Lead Validator, The Aerospace Corporation Mike Quintos: ECR Team, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

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

Protection Profile for Application Software, Version 1.4, 7 October 2021

That information has not been reproduced here and the NDcPP22e 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 PP_APP_v1.4 as described for this TOE in the Security Target.

As stated, the ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent, or hostile, and administers the software in compliance with the applied enterprise security policy.

3.2 Clarification of Scope

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

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following document:
    - *Protection Profile for Application Software*, Version 1.4, 7 October 2021
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Wickr Enterprise Server 1.30.0 Security Target, Version 1.0, 28 March 2023. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this report.

4 Architectural Information

4.1 TOE Architecture

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

The TOE is a containerized software application that runs on Docker (runtime engine 20.10) with an Amazon Linux 2 container image, which in turn runs on Ubuntu 18.04.

The TOE architecture is depicted in the following figure. The TOE is indicated by the red box. The application runs in a containerized Docker format, which is indicated by the yellow box. The Docker infrastructure then runs on the Linux server platform.

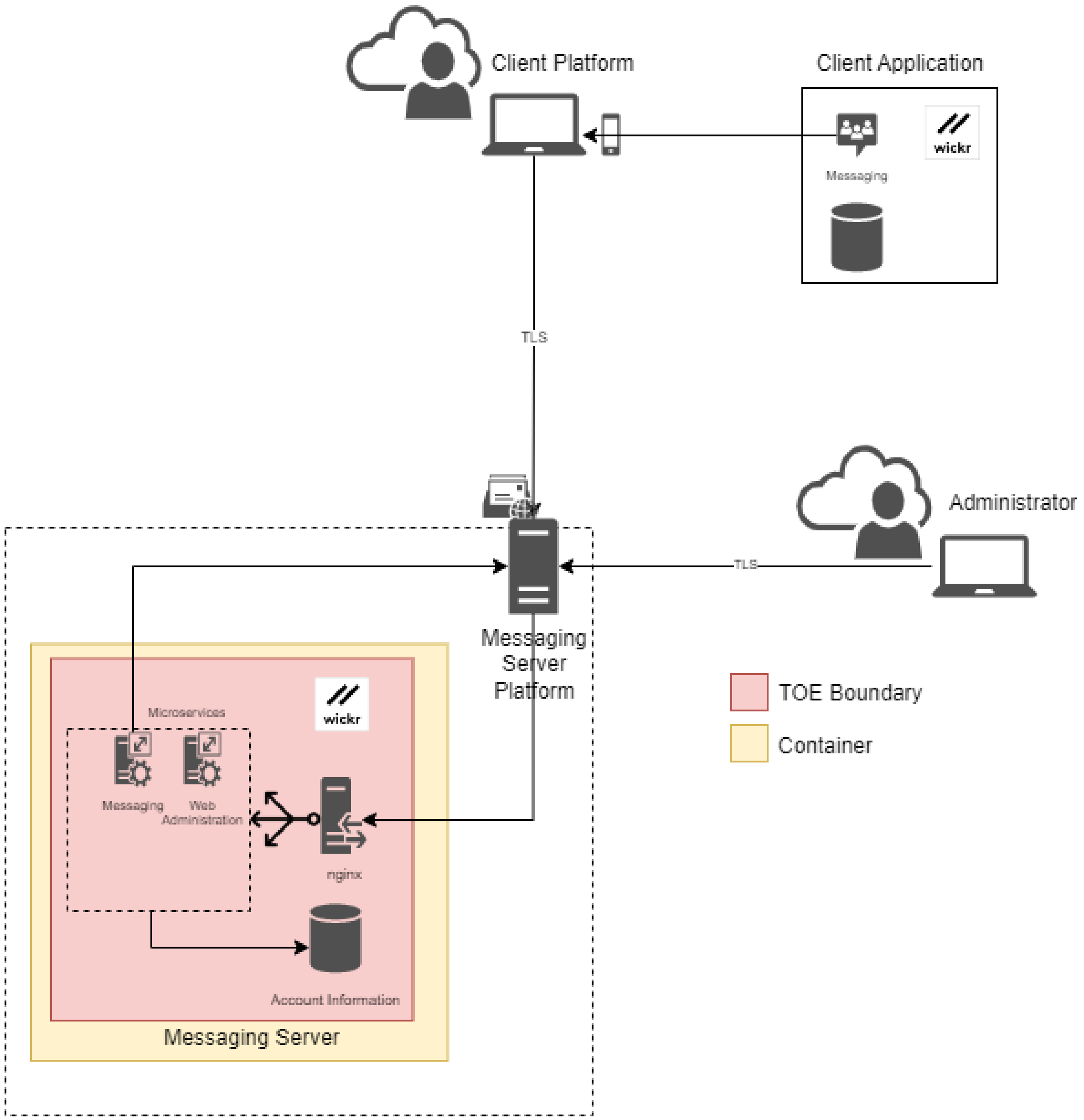


Figure 1: Wickr Architecture

In addition to the platform identified above, the TOE's operational environment includes the following:

- Remote Wickr Client instances that communicate through the TOE for client-to-client communication
- A workstation with a browser to access the TOE's administrator interface
- An update server (public download site).

4.2 Physical Boundaries

The TOE includes the Wickr Server in a base deployment that provides data messaging. The TOE includes an nginx service which functions as a reverse proxy for routing inbound network connections. This service is considered non-interfering with respect to security as it does not enforce any of the security functionality claimed by the TSF. The TOE runs on Linux platforms. For this evaluation, the TOE is evaluated on the following specific platform:

- Linux

o Intel Xeon E5-2620v3 (Haswell) processor

o Ubuntu 18.04 LTS 64-bit OS

In addition to the platforms identified above, the TOE's operational environment includes the following:

- Two or more remote Wickr Client instances to establish connections
- A workstation with a browser to access the TOE's administrator interface
- Docker is required to run the TOE
- Update server (public download site)

5 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

5.1 Cryptographic Support

The TOE uses NIST-validated cryptographic algorithms to secure messaging data in transit. The cryptographic functions are supplied by the host platform. Credential data is protected by a platform-provided mechanism.

5.2 User Data Protection

The TOE leverages platform functionality to secure sensitive data at rest. The TOE uses network resources provided by the underlying platform.

The TOE uses network connectivity to interact with Wickr Clients and for administrator sessions.

5.3 Security Management

The TOE provides management capability for environmental components via a web interface. Administrator accounts are defined locally. Wickr Server configuration data is stored locally but is not managed through the TOE.

5.4 Privacy

The TOE does not process any personally identifiable information (PII). No transmission of PII occurs that is not in direct response to user activity.

5.5 Protection of the TSF

The TOE includes measures to integrate securely with its Linux platform. The TOE does not perform explicit memory mapping, nor does it allocate any memory region with both write and execute permissions. Similarly, the TOE does not write user-modifiable data to directories that contain executable files. The TOE is compatible with its supported host OS platform when it is configured in a secure manner. The TOE includes C code compiled to enforce Address Space Layout Randomization (ASLR) and to protect against stack overflow, as well as interpreted code that enforces ASLR through its runtime environment and is not susceptible to stack-based buffer overflow attacks.

The TOE uses a well-defined set of platform APIs and third-party libraries.

The TOE provides the ability for a user to check its version. The TOE platform is used to apply updates. Updates are delivered as a container image. Updates to the TOE are digitally signed, and the signature is validated by the platform prior to installation. The TOE does not modify its own code. Removal of the application removes all executable code associated with the TOE.

5.6 Trusted Path/Channels

The TOE uses trusted paths to secure data in transit between itself and external entities using platform-provided mechanisms. The TOE uses platform provided TLS and HTTPS for service requests, data communication, and web administration.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Wickr Enterprise Server Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, 06 March 2023
- *Wickr Enterprise NIAP Version Installation and Maintenance*, Version 1.30.0
- *Wickr Enterprise Administrator Guide*, Version 426151b

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Wickr Enterprise Server Version 1.30.0 Common Criteria Test Report and Procedures*, Version 1.0, 14 April 2023.

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Wickr Enterprise Server 1.30.0*, Version 1.0, 19 May 2023

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specification:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021.

7.1 Developer Testing

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

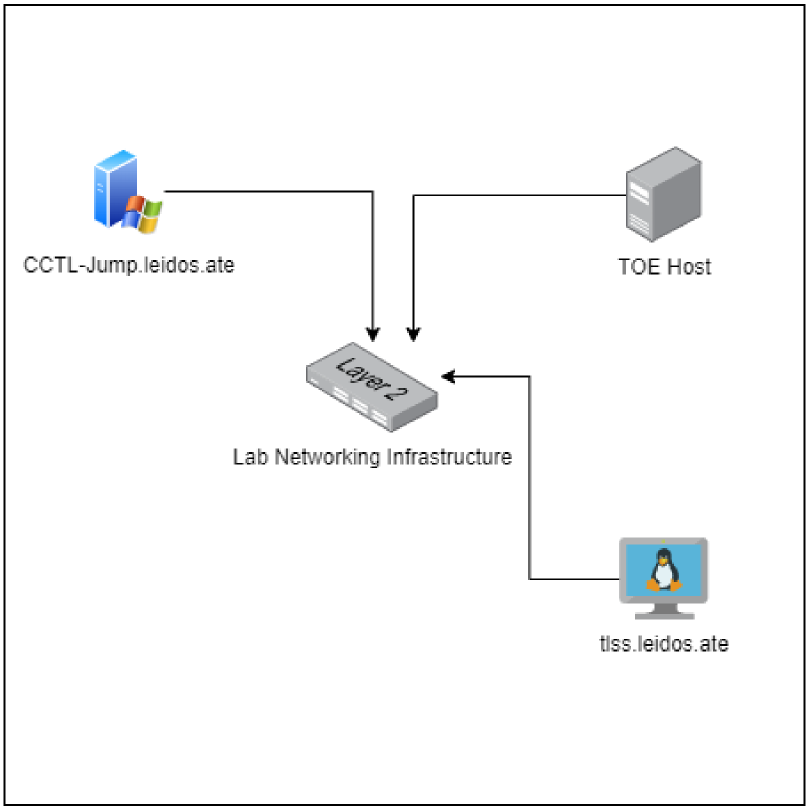
7.2 Evaluation Team Independent Testing

The evaluation team devised a test plan based on the test activities specified in the PP. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above.

The TOE was tested at Leidos's Columbia, MD location from March 2023 to June 2023. The procedures and results of this testing are available in the test report referenced above.

7.3 Test Configuration

This section identifies the devices used for testing the TOE and describes the test configuration. The test configuration is described below:



The following components were used to create the test configuration:

TOE Hardware (Physical)

- Dell PowerEdge R430
    - CPU: Intel Xeon E5
    - Operating System: Ubuntu 18.04
    - Storage: 500 GB HDD
    - Software: Docker 20.10 runtime (TOE runs on top of Docker using Amazon Linux 2 container for OpenSSL)

Lab Equipment

- Virtual machines
    - tlss.leidos.ate
        - Operating System: Ubuntu 18.04
        - Purpose: NMAP Scans, Packet Captures
- Physical machines
    - cctl-jump.leidos.ate
        - Operating System: Windows Server 2016
        - Purpose: Terminal Server to access test network from corporate network, Access to the TOE web interface.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the team test plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Application Software* were fulfilled.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is the Wickr Enterprise Server 1.30.0, evaluated on Ubuntu 18.04. The TOE runs on the platform OS as a containerized application in Docker (runtime engine 20.10) with an Amazon Linux 2 container image.

8.2 Excluded Functionality

Excluded Functionality	Description
Voice and Video Services (Conferencing Server)	The TOE includes the base text messaging server only.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Wickr Enterprise Server 1.30.0. The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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, revision 5 and CEM version 3.1, revision 5, and the specific evaluation activities specified in:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021.

The evaluation determined the TOE satisfies the conformance claims made in the Wickr Enterprise Server 1.30.0 Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the PP listed above.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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

The evaluation team performed each test activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the National Vulnerability Database (https://nvd.nist.gov/).

The evaluation team performed searches on 12 April 2023 and again on 22 May 2023, using the following search terms:

- “wickr”
- “encrypted service”
- “zero trust”
- “openssl 2.0.16”
- “amazon linux 2 openssl”
- The identity of each of the third-party libraries listed in Section A.2 of the ST.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. 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.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Wickr Enterprise Server Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, 06 March 2023. No versions of the TOE and software, either earlier or later were evaluated.

As specified in the ST and elsewhere in this report, the Wickr Server TOE is a containerized software application that runs on Ubuntu 18.04. The user should note that Ubuntu 18.04 reached End of Standard Support on May 31, 2023. To ensure that the security posture of the operational environment can be maintained, the Wickr vendor has specified that it is necessary for the organization deploying the TOE to have an Ubuntu Pro subscription, which includes Expanded Security Maintenance (ESM) for Ubuntu 18.04 until April 2028.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The Voice and Video Services (Conferencing Server) functionality is excluded from the evaluation. The TOE includes the base text messaging services only. This is specified in Section 8.2.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is *Wickr Enterprise Server 1.30.0 Security Target*, Version 1.0, 28 March 2023

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

14 Bibliography

The validation team used the following documents to produce this VR:

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

[2] 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 requirements, Version 3.1, Revision 5, April 2017.

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

[5] Protection Profile for Application Software, Version 1.4, 07 October 2021.

[6] Wickr Enterprise Server 1.30.0 Security Target, Version 1.0, 28 March 2023.

[7] Wickr Enterprise NIAP Version Installation and Maintenance, Version 1.30.0.

[8] Wickr Enterprise Administrator Guide, Version 426151b.

[9] Wickr Enterprise Server Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, 06 March 2023.

[10] Evaluation Technical Report for Wickr Enterprise Server 1.30.0, Version 1.0, 25 May 2023.

[11] Assurance Activities Report for Wickr Enterprise Server 1.30.0, Version 1.0, 19 May 2023.

[12] Wickr Enterprise Server Version 1.30.0 Common Criteria Test Report and Procedures, Version 1.1, 15 May 2023.