Assurance Activities Report
for
Wickr Enterprise Server 1.30.0

Version 1.0
5 June 2023

Evaluated By:

Leidos Inc.
https://www.leidos.com/civil/commercial-cyber/product-compliance
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Wickr LLC
W 31st Street
New York, NY 10001

The TOE Evaluation was Sponsored by:
Wickr LLC
W 31st Street
New York, NY 10001

Evaluation Personnel:
Allen Sant
Anthony Apted
Armin Najafabadi
Josh J. Marciante
Pascal Patin

Common Criteria Version:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.

Common Evaluation Methodology Version:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Protection Profiles:

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

Revision History

Version	Date	Description
0.1	26 October 2022	Initial draft
1.0	5 June 2023	Final version for Check-out

Contents

1. Introduction

This document presents the results of performing assurance activities associated with the Wickr Enterprise Server 1.30.0 evaluation. This report contains sections documenting the performance of evaluation activities associated with each of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) as specified in the following document:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 [PP_APP_v1.4]

Note that, in accordance with NIAP Policy Letter #5, all cryptography in the TOE for which NIST provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components must be NIST validated. The CCTL will verify that the claimed NIST validation complies with the NIAP-approved PP requirements the TOE claims to satisfy. The CCTL verification of the NIST validation will constitute performance of the associated assurance activity. As such, Test assurance activities associated with functional requirements within the scope of Policy Letter #5 are performed by verification of the relevant CAVP certification and not through performance of any testing as specified in the claimed PP documents.

1.1 Technical Decisions

This subsection lists the Technical Decisions that have been issued by NIAP against [PP_APP_v1.4], along with rationale as to their applicability or otherwise to this evaluation.

TD0624 – Addition of DataStore for Storing and Setting Configuration Options

This TD has been applied to this evaluation.

TD0628 – Addition of Container Image to Package Format

This TD has been applied to this evaluation.

TD0650 – Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4

N/A – the TOE does not claim VPN client functionality.

TD0655 – Mutual authentication in FTP_DIT_EXT.1 for SW App

This TD has been applied to this evaluation.

TD0664 – Testing activity for FPT_TUD_EXT.2.2

This TD has been applied to this evaluation.

TD0669 – FIA_X509_EXT.1 Test 4 Interpretation

N/A – the TOE does not claim this SFR.

TD0709 – Number of elements for iterations of FCS_HTTPS_EXT.1

N/A – the TOE does not claim this SFR.

TD0717 – Format changes for PP_APP_V1.4

This TD has been applied to this evaluation.

TD0719 – ECD for PP APP V1.3 and 1.4

Not applicable; this TD updates the App PP to include a formal ECD which is needed for the PP itself to conform to CC Part 3. This does not change the ST or how the evaluation of the TOE is conducted.

1.2 References

[ST]	Wickr Enterprise Server Version 1.30.0 Security Target, Version 1.0, 28 March 2023
[CCECG]	Wickr Enterprise Server Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, 6 March 2023.
[Install]	Wickr Enterprise NIAP Version Installation and Maintenance, Version 1.30.0
[Admin]	Wickr Enterprise Administrator Guide, Version 426151b

1.3 SAR Evaluation

The following Security Assurance Requirements (SARs) were evaluated during the evaluation of the TOE:

SAR	Verdict
ASE_CCL.1	Pass
ASE_ECD.1	Pass
ASE_INT.1	Pass
ASE_OBJ.2	Pass
ASE_REQ.2	Pass
ASE_TSS.1	Pass
ADV_FSP.1	Pass
AGD_OPE.1	Pass
AGD_PRE.1	Pass
ALC_CMC.1	Pass
ALC_CMS.1	Pass
ALC_TSU_EXT.1	Pass
ATE_IND.1	Pass
AVA_VAN.1	Pass

The evaluation work units are listed in the proprietary ETR. The evaluators note per the PP evaluation activities that many of the SARs were successfully evaluated through completion of the associated evaluation activities presented in the claimed PP.

2. Security Functional Requirement Evaluation Activities

This section describes the evaluation activities associated with the SFRs defined in the ST and the results of those activities as performed by the evaluation team. The evaluation activities are derived from [PP_APP_v1.4]. NIAP Technical Decisions have been applied and are identified as appropriate.

2.1 Cryptographic Support (FCS)

2.1.1 Certificate Table

The TOE does not implement any cryptographic functionality. It relies on platform-provided cryptographic functionality in order to meet certain claimed SFRs.

In accordance with NIAP Policy Letter 5 and Policy 5 Addendum 3 Item 5 (Certificate Report Template), the table below provides the following information for each of the SFRs claimed for the TOE that rely on platform-provided cryptography:

- the SFR claimed for the TOE
- the platform-provided cryptographic functionality the TOE relies on to satisfy the claimed SFR
- the applicable CAVP algorithm list name(s) for the platform-provided cryptographic algorithms that implement the platform-provided cryptographic functionality
- the applicable NIST standards defining the algorithm implementation
- the applicable CAVP certificate number.

SFR	Platform-provided Function	CAVP Algorithms	NIST Standard	CAVP Certs
FCS_STO_EXT.1 PBKDEF2	Keyed-hash message authentication	HMAC-SHA2-256	FIPS PUB 180-4 FIPS PUB 198-1	#A3455
	Cryptographic hash	SHA2-256	FIPS PUB 180-4	#A3455
	Deterministic random bit generation	Counter DRBG (AES-256)	NIST SP 800-90A	#A3455
FTP_DIT_EXT.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Key Establishment	KAS-ECC-SSC	Sp800-56Ar3	#A3455
	Asymmetric key generation	ECDSA KeyGen (P-384)	FIPS186-4	#A3455
	Asymmetric key generation	ECDSA KeyVer (P-384)	FIPS186-4	#A3455
	Asymmetric Signature Generation	ECDSA SigGen (P-256, P-384)	FIPS186-4	#A3455
	Asymmetric Signature Verification	ECDSA SigVer (P-256, P-384)	FIPS186-4	#A3455
	Digital signature generation	RSA SigGen (4096)	FIPS186-4	#A3455

SFR	Platform-provided Function	CAVP Algorithms	NIST Standard	CAVP Certs
	Digital signature verification	RSA SigVer (4096)	FIPS186-4	#A3455
	Symmetric encryption	AES-GCM (128 bits, 256 bits)	NIST SP 800-38	#A3455
	Keyed-hash message authentication	HMAC-SHA2-256	FIPS PUB 180-4 FIPS PUB 198-1	#A3455
	Keyed-hash message authentication	HMAC-SHA2-384	FIPS PUB 180-4 FIPS PUB 198-1	#A3455
	Cryptographic hash	SHA2-256	FIPS PUB 180-4	#A3455
	Cryptographic hash	SHA2-384	FIPS PUB 180-4	#A3455
	Deterministic random bit generation	Counter DRBG (AES-256)	NIST SP 800-90A	#A3455

2.1.2 Cryptographic Asymmetric Key Generation (FCS_CKM_EXT.1)

2.1.2.1 TSS Evaluation Activity

The evaluator shall inspect the application and its developer documentation to determine if the application needs asymmetric key generation services. If not, the evaluator shall verify the "***generate no asymmetric cryptographic keys***" selection is present in the ST. Otherwise, the evaluation activities shall be performed as stated in the selection-based requirements.

The evaluator inspected the application and its documentation, comprising [Admin], [Install], and [CCECG], and determined the TOE does not need asymmetric key generation services. The TOE invokes platform-provided cryptography to secure data in transit. As such, the evaluator verified the ST selects "generate no asymmetric cryptographic keys" in FCS_CKM_EXT.1.

2.1.2.2 Guidance Evaluation Activity

None.

2.1.2.3 Test Evaluation Activity

None.

2.1.3 Random Bit Generation Services (FCS_RBG_EXT.1)

2.1.3.1 TSS Evaluation Activity

If ***use no DRBG functionality*** is selected, the evaluator shall inspect the application and its developer documentation and verify that the application needs no random bit generation services.

If ***implement DRBG functionality*** is selected, the evaluator shall ensure that additional FCS_RBG_EXT.2 elements are included in the ST.

If ***invoke platform-provided DRBG functionality*** is selected, the evaluator performs the following activities. The evaluator shall examine the TSS to confirm that it identifies all functions (as described by the SFRs included in the ST) that obtain random numbers from the platform RBG. The evaluator shall determine that for each of these functions, the TSS states which platform interface (API) is used to obtain the random numbers. The evaluator shall confirm that each of these interfaces corresponds to the acceptable interfaces listed for each platform below.

It should be noted that there is no expectation that the evaluators attempt to confirm that the APIs are being used "correctly" for the functions identified in the TSS; the activity is to list the used APIs and then do an existence check via decompilation.

In FCS_RBG_EXT.1, the ST author has selected ***use no DRBG functionality***. The evaluator examined the application and its documentation, comprising [Admin], [Install], and [CCECG], and confirmed the application does not need random bit generation services.

2.1.3.2 Guidance Evaluation Activity

None.

2.1.3.3 Test Evaluation Activity

If ***invoke platform-provided DRBG functionality*** is selected, the following tests shall be performed:

The evaluator shall decompile the application binary using a decompiler suitable for the application (TOE). The evaluator shall search the output of the decompiler to determine that, for each API listed in the TSS, that API appears in the output. If the representation of the API does not correspond directly to the strings in the following list, the evaluator shall provide a mapping from the decompiled text to its corresponding API, with a description of why the API text does not directly correspond to the decompiled text and justification that the decompiled text corresponds to the associated API.

Linux: The evaluator shall verify that the application collects random from `/dev/random` or `/dev/urandom`.

If invocation of platform-provided functionality is achieved in another way, the evaluator shall ensure the TSS describes how this is carried out, and how it is equivalent to the methods listed here (e.g. higher-level API invokes identical low-level API).

In FCS_RBG_EXT.1, the ST author has selected ***use no DRBG functionality***. Therefore, this activity is not applicable to the TOE.

2.1.4 Storage of Credentials (FCS_STO_EXT.1)

2.1.4.1 TSS Evaluation Activity

The evaluator shall check the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored.

Section 6.3 of [ST] ("User Data Protection"), Table 5 ("Sensitive Data") lists the following persistent credentials: User Credentials; and TLS Server Private Key.

Section 6.2 of [ST] ("Cryptographic Support") states the TOE stores the credential data in an encrypted volume using Linux Unified Key Setup (LUKS) with an encryption key derived using a password-based key derivation function (PBKDF2) provided by the platform.

2.1.4.2 Guidance Evaluation Activity

None.

2.1.4.3 Test Evaluation Activity

For all credentials for which the application implements functionality, the evaluator shall verify credentials are encrypted according to FCS_COP.1/SKC or conditioned according to FCS_CKM.1.1/AK and FCS_CKM.1/PBKDF.

The TOE relies on a platform-provided mechanism to securely store credential data at rest. Therefore, this activity is not applicable to the TOE.

For all credentials for which the application invokes platform-provided functionality, the evaluator shall perform the following actions which vary per platform.

Platforms: Linux… The evaluator shall verify that all keys are stored using Linux `keyrings`.

As advised by NIAP in response to a Technical Query submitted by the evaluation team, platform-provided PBKDF2 is an allowable storage mechanism to protect credentials. The TOE uses platform-provided PBKDF2 to derive an encryption key that is used by LUKS to encrypt the volume on which the TOE stores credentials (CAVP A3455).

2.2 User Data Protection (FDP)

2.2.1 Encryption of Sensitive Application Data (FDP_DAR_EXT.1)

2.2.1.1 TSS Evaluation Activity

The evaluator shall examine the TSS to ensure that it describes the sensitive data processed by the application. The evaluator shall then ensure that the following activities cover all of the sensitive data identified in the TSS.

Section 6.3 of [ST] (“User Data Protection”), Table 5 (“Sensitive Data”) lists the data considered to be sensitive by the TOE and how the data is protected at rest.

The sensitive data consists of User Credentials and TLS Server Private Key. Table 5 states the TOE does not transmit sensitive data to remote systems. The TOE stores the credential data in an encrypted volume using Linux Unified Key Setup (LUKS) with an encryption key derived using a password-based key derivation function (PBKDF2) provided by the platform.

If ***not store any sensitive data*** is selected, the evaluator shall inspect the TSS to ensure that it describes how sensitive data cannot be written to non-volatile memory. The evaluator shall also ensure that this is consistent with the filesystem test below.

The ST does not select “not store any sensitive data” in FDP_DAR_EXT.1. Therefore, this activity is not applicable.

2.2.1.2 Guidance Evaluation Activity

None.

2.2.1.3 Test Evaluation Activity

Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1.

The evaluator shall inventory the filesystem locations where the application may write data. The evaluator shall run the application and attempt to store sensitive data. The evaluator shall then inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted.

Section 6.3 of [ST] states the TOE protects all sensitive data in accordance with FCS_STO_EXT.1. As such, this Test activity is not applicable.

If ***leverage platform-provided functionality*** is selected, the evaluation activities will be performed as stated in the following requirements, which vary on a per-platform basis:

Platforms: Linux… The Linux platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption clear to the end user.

Although the ST does not select “leverage platform-provided functionality”, the TOE relies on a platform-provided mechanism to protect sensitive data in accordance with FCS_STO_EXT.1. Section “TOE Description”, sub-section “Evaluated Configuration” of [CCECG] states the administrator must configure volume encryption using LUKS for the volume on which the TOE is installed.

2.2.2 Access to Platform Resources (FDP_DEC_EXT.1)

2.2.2.1 FDP_DEC_EXT.1.1

2.2.2.1.1 TSS Evaluation Activity

None.

2.2.2.1.2 Guidance Evaluation Activity

The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to hardware resources. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required.

The statement of FDP_DEC_EXT.1.1 in Section 5.2.2 of [ST] (“User Data Protection (FDP)”) specifies the only hardware resource the TOE accesses is network connectivity.

Section “Network Administrator” of [Admin] makes it clear, through description of the Network Administrator roles and responsibilities, that the Server TOE accesses platform network resources in order to communicate with Wickr Clients.

2.2.2.1.3 Test Evaluation Activity

Platforms: Linux… The evaluator shall verify that either the application software or its documentation provides a list of the hardware resources it accesses.

The only platform resource that the TOE accesses is network connectivity. This is clearly documented in the ST and the TOE documentation. During testing the TOE did not make any attempts to access other resources.

2.2.2.2 FDP_DEC_EXT.1.2

2.2.2.2.1 TSS Evaluation Activity

None.

2.2.2.2.2 Guidance Evaluation Activity

The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to sensitive information repositories. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each sensitive information repository which it accesses, identify the justification as to why access is required.

Section "Network Administrator", sub-section "Event Logging" of [Admin] makes it clear, through description of the Network Administrator roles and responsibilities, that the Server TOE accesses platform system log resources in order to write application logs.

2.2.2.2.3 Test Evaluation Activity

Platforms: Linux… The evaluator shall verify that either the application software or its documentation provides a list of sensitive information repositories it accesses.

The only platform information repository the TOE accesses is the system log to write event logs. This is clearly documented in the ST and the administrative guides. During testing the TOE did not make any attempts to access other repositories.

2.2.3 Network Communications (FDP_NET_EXT.1)

2.2.3.1 TSS Evaluation Activity

None.

2.2.3.2 Guidance Evaluation Activity

None.

2.2.3.3 Test Evaluation Activity

The evaluator shall perform the following tests:

Test 1: The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are documented in the TSS or are user-initiated.

The evaluator captured the traffic to and from the TOE while it was in operation. The evaluator verified all of the traffic was associated with a TLS connection from the remote administrator.

Test 2: The evaluator shall run the application. After the application initializes, the evaluator shall run network port scans to verify that any ports opened by the application have been captured in the ST for the third selection and its assignment. This includes connection-based protocols (e.g. TCP, DCCP) as well as connectionless protocols (e.g. UDP).

The evaluator scanned the TOE for open ports with NMAP and verified that all opened ports were documented.

2.3 Security Management (FMT)

2.3.1 Secure by Default Configuration (FMT_CFG_EXT.1)

2.3.1.1 FMT_CFG_EXT.1.1

2.3.1.1.1 TSS Evaluation Activity

The evaluator shall check the TSS to determine if the application requires any type of credentials and if the application installs with default credentials.

Section 6.4 of [ST] (“Security Management”) states the TOE installs with a single default administrator account with a default password. The TOE requires the administrator to set a new password on first login. The administrator can configure additional user accounts.

2.3.1.1.2 Guidance Evaluation Activity

None.

2.3.1.1.3 Test Evaluation Activity

If the application uses any default credentials the evaluator shall run the following tests.

Test 1: The evaluator shall install and run the application without generating or loading new credentials and verify that only the minimal application functionality required to set new credentials is available.

The evaluator installed the TOE and verified that the default credentials provided access to the TOE and that the TOE required the evaluator to change the default credentials as the only initial action that could be taken.

Test 2: The evaluator shall attempt to clear all credentials and verify that only the minimal application functionality required to set new credentials is available.

The evaluator found no way to clear all credentials and reset the TOE to the default credentials.

Test 3: The evaluator shall run the application, establish new credentials and verify that the original default credentials no longer provide access to the application.

The evaluator verified that the TOE did not permit the default credentials to be used once the new credentials had been established.

2.3.1.2 FMT_CFG_EXT.1.2

2.3.1.2.1 TSS Evaluation Activity

None.

2.3.1.2.2 Guidance Evaluation Activity

None.

2.3.1.2.3 Test Evaluation Activity

The evaluator shall install and run the application. The evaluator shall inspect the filesystem of the platform (to the extent possible) for any files created by the application and ensure that their permissions are adequate to protect them. The method of doing so varies per platform.

Platforms: Linux... The evaluator shall run the command `find -L . -perm /002` inside the application's data directories to ensure that all files are not world-writable. The command should not print any files.

The evaluator found no world-writable files in the TOE's data directories.

2.3.2 Supported Configuration Mechanism (FMT_MEC_EXT.1)

2.3.2.1 TSS Evaluation Activity

The evaluator shall review the TSS to identify the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. At a minimum the TSS shall list settings related to any SFRs and any settings that are mandated in the operational guidance in response to an SFR.

Section 6.4 of [ST] ("Security Management") states the TOE stores configuration data related to the TOE's initial configuration in `/etc/replicated`. The ST further states the TOE uses this data for initial deployment and does not provide any interface for an administrator to manage it.

Conditional: If "***implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption***" is selected, the evaluator shall ensure that the TSS identifies those options, as well as indicates where the encrypted representation of these options is stored.

The ST does not make this selection.

2.3.2.2 Guidance Evaluation Activity

None.

2.3.2.3 Test Evaluation Activity

If "***invoke the mechanisms recommended by the platform vendor for storing and setting configuration options***" is chosen, the method of testing varies per platform as follows:

Modified in accordance with TD0624.

Platforms: Linux... The evaluator shall run the application while monitoring it with the utility `strace`. The evaluator shall make security-related changes to its configuration. The evaluator shall verify that `strace` logs corresponding changes to configuration files that reside in `/etc` (for system-specific configuration), in the user's home directory (for user-specific configuration), or `/var/lib/` (for configurations controlled by UI and not intended to be directly modified by an administrator).

The evaluator verified that configuration changes were stored appropriately in the correct container.

If "***implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption***" is selected, for all configuration options listed in the TSS as being stored and protected using encryption, the evaluator shall examine the contents of the configuration option storage (identified in the TSS) to determine that the options have been encrypted.

The ST does not make this selection.

2.3.3 Specification of Management Functions (FMT_SMF.1)

2.3.3.1 TSS Evaluation Activity

None.

2.3.3.2 Guidance Evaluation Activity

The evaluator shall verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.

The guidance documentation describes each of the management functions specified in [ST], as follows:

- Configure the Messaging proxy—described in Section 6.1 (“Messaging Proxies”) of [Install]
- Manage users:
  - Section “Super Administrator”, sub-section “Creating a Network Administrator” of [Admin] describes how the Super Administrator creates Network Administrators on the TOE
  - Section “Network Administrator”, sub-section “Client Configuration” describes how Network Administrators manage client Config Files that allow client users to connect to the Wickr Enterprise
  - Section “Security Groups” describes how Network Administrators manage users grouped into Security Groups.
- Configure certificates—Section “Software Download, Installation, Configuration”, sub-section “Initial Download/Installation/Configuration” of [CCECG] describes how administrators configure the TOE’s TLS server certificate
- Configure room management—described in Section “Network Administrator”, sub-section “Default Rooms” of [Admin]
- Configure event logging—described in Section “Network Administrator”, sub-section “Event Logging” of [Admin].

2.3.3.3 Test Evaluation Activity

The evaluator shall test the application's ability to provide the management functions by configuring the application and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.

The evaluator used the TOE’s interface to configure event logging, room management, certificates, the messaging proxy, and the users.

2.4 Privacy (FPR)

2.4.1 User Consent for Transmission of Personally Identifiable Information (FPR_ANO_EXT.1)

2.4.1.1 TSS Evaluation Activity

The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted.

Section 6.5 of [ST] (“Privacy”) states the TOE never transmits known PII over a network. Wickr Client users could request encrypted PII data may be passed through the TOE, but this data is never decrypted on the TOE.

2.4.1.2 Guidance Evaluation Activity

> None.

2.4.1.3 Test Evaluation Activity

> If ***require user approval before executing*** is selected, the evaluator shall run the application and exercise the functionality responsible for transmitting PII and verify that user approval is required before transmission of the PII.

The ST does not make this selection.

2.5 Protection of the TSF (FPT)

2.5.1 Anti-Exploitation Capabilities (FPT_AEX_EXT.1)

2.5.1.1 FPT_AEX_EXT.1.1

2.5.1.1.1 TSS Evaluation Activity

> The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled.

Section 6.6 of [ST] (“Protection of the TSF”) states the TOE is implemented in a combination of compiled (C) and interpreted (Node, Java) code. The C code is compiled with `-wl.dynamicbase` to enforce ASLR. The interpreted code is not subject to stack-based overflow attacks.

2.5.1.1.2 Guidance Evaluation Activity

> None.

2.5.1.1.3 Test Evaluation Activity

> The evaluator shall perform either a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address. The method of doing so varies per platform. For those platforms requiring the same application running on two different systems, the evaluator may alternatively use the same device. After collecting the first instance of mappings, the evaluator must uninstall the application, reboot the device, and reinstall the application to collect the second instance of mappings.
>
> **Platforms: Linux...** The evaluator shall run the same application on two different Linux systems. The evaluator shall then compare their memory maps using `pmap  -x  PID` to ensure the two different instances share no mapping locations.

PMAP showed that different instances of the TOE do not share memory mapping locations.

2.5.1.2 FPT_AEX_EXT.1.2

2.5.1.2.1 TSS Evaluation Activity

None.

2.5.1.2.2 Guidance Evaluation Activity

None.

2.5.1.2.3 Test Evaluation Activity

The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform.

Platforms: Linux... The evaluator shall perform static analysis on the application to verify that both

- `mmap` is never be invoked with both the `PROT_WRITE` and `PROT_EXEC` permissions, and
- `mprotect` is never invoked with the `PROT_EXEC` permission.

The evaluator examined the TOE's source code for all uses of mmap and mprotect and verified that the TOE never invoked with PROT_EXEC permissions.

2.5.1.3 FPT_AEX_EXT.1.3

2.5.1.3.1 TSS Evaluation Activity

None.

2.5.1.3.2 Guidance Evaluation Activity

None.

2.5.1.3.3 Test Evaluation Activity

The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests:

Platforms: Linux... The evaluator shall ensure that the application can successfully run on a system with either SELinux or AppArmor enabled and in enforce mode.

The evaluator verified that the TOE could run on a system with AppArmor enabled and enforcing.

2.5.1.4 FPT_AEX_EXT.1.4

2.5.1.4.1 TSS Evaluation Activity

None.

2.5.1.4.2 Guidance Evaluation Activity

None.

2.5.1.4.3 Test Evaluation Activity

The evaluator shall run the application and determine where it writes its files. For files where the user does not choose the destination, the evaluator shall check whether the destination directory contains executable files. This varies per platform:

Platforms: Linux… The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files.

The TOE does not write any user-modifiable files in the normal mode of operation. Per the TSS the only way to get the TOE to write a file to a directory with executable files is to directly and explicitly instruct the TOE to do so.

2.5.1.5 FPT_AEX_EXT.1.5

2.5.1.5.1 TSS Evaluation Activity

None.

2.5.1.5.2 Guidance Evaluation Activity

None.

2.5.1.5.3 Test Evaluation Activity

The evaluator will inspect every native executable included in the TOE to ensure that stack-based buffer overflow protection is present.

The TOE comprises interpreted code without any just-in-time compilation, so this activity is not applicable.

2.5.2 Use of Supported Services and APIs (FPT_API_EXT.1)

2.5.2.1 TSS Evaluation Activity

The evaluator shall verify that the TSS lists the platform APIs used in the application.

Section 6.6 of [ST] (“Protection of the TSF”) references Appendix A.1 of [ST] (“Platform APIs”) for the lists of platform APIs used by the TOE. The evaluator confirmed Appendix A.1 of [ST] lists platform APIs used by the TOE.

2.5.2.2 Guidance Evaluation Activity

None.

2.5.2.3 Test Evaluation Activity

The evaluator shall then compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported.

All APIs used by the TOE were shown to be properly documented and valid.

2.5.3 Use of Third Party Libraries (FPT_LIB_EXT.1)

2.5.3.1 TSS Evaluation Activity

None.

2.5.3.2 Guidance Evaluation Activity

None.

2.5.3.3 Test Evaluation Activity

The evaluator shall install the application and survey its installation directory for dynamic libraries. The evaluator shall verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.

The evaluator verified that all the libraries included with the TOE were consistent with those documented in the ST.

2.5.4 Software Identification and Versions (FPT_IDV_EXT.1)

2.5.4.1 TSS Evaluation Activity

If **"other version information"** is selected the evaluator shall verify that the TSS contains an explanation of the versioning methodology.

Section 5.2.5 of [ST] ("Protection of the TSF (FPT)") selects "other version information" in FPT_IDV_EXT.1.1 and completes the assignment with "major.minor.release". Section 6.6 of [ST] ("Protection of the TSF") states the TOE can display its current version in major.minor.release format.

2.5.4.2 Guidance Evaluation Activity

None.

2.5.4.3 Test Evaluation Activity

The evaluator shall install the application, then check for the existence of version information. If ***SWID tags*** is selected the evaluator shall check for a .swidtag file. The evaluator shall open the file and verify that is contains at least a SoftwareIdentity element and an Entity element.

As described in the ST, the TOE does not use SWID tags. The TOE is versioned using a major.minor.release versioning system. FPT_TUD_EXT.1.2 shows the TOE displays versioning information in that format.

2.5.5 Integrity for Installation and Update (FPT_TUD_EXT.1)

2.5.5.1 FPT_TUD_EXT.1.1

2.5.5.1.1 TSS Evaluation Activity

None.

2.5.5.1.2 Guidance Evaluation Activity

The evaluator shall check to ensure the guidance includes a description of how updates are performed.

Section 3.4 of [Install] ("Replicated Overview") states the evaluated configuration supports only the "Online Install" installation option, which makes use of the Replicated third-party service to install and manage software setup and deployment.

Section 7 of [Install] ("Software Updates") describes how the administrator updates a deployment of the TOE installed using the "Online Install" option.

2.5.5.1.3 Test Evaluation Activity

The evaluator shall check for an update using procedures described in either the application documentation or the platform documentation and verify that the application does not issue an error. If it is updated or if it reports that no update is available this requirement is considered to be met.

The TOE is capable of checking for an update itself. The evaluator observed that the check for update completed successfully and did not return an error.

2.5.5.2 FPT_TUD_EXT.1.2

2.5.5.2.1 TSS Evaluation Activity

None.

2.5.5.2.2 Guidance Evaluation Activity

The evaluator shall verify guidance includes a description of how to query the current version of the application.

Section "Software Download, Installation, Configuration" of [CCECG] describes how the administrator queries the current version of the TOE.

2.5.5.2.3 Test Evaluation Activity

The evaluator shall query the application for the current version of the software according to the operational user guidance. The evaluator shall then verify that the current version matches that of the documented and installed version.

The evaluator demonstrated that the TOE's user interface displays the version number using the major.minor.release format.

2.5.5.3 FPT_TUD_EXT.1.3

2.5.5.3.1 TSS Evaluation Activity

None.

2.5.5.3.2 Guidance Evaluation Activity

None.

2.5.5.3.3 Test Evaluation Activity

The evaluator shall verify that the application's executable files are not changed by the application.

Platforms: Apple iOS… The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).

For all other platforms, the evaluator shall perform the following test:

Test 1: The evaluator shall install the application and then locate all of its executable files. The evaluator shall then, for each file, save off either a hash of the file or a copy of the file itself. The evaluator shall then run the application and exercise all features of the application as described in the ST. The evaluator shall then compare each executable file with the either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical.

The evaluator obtained a hash of the TOE's executable files. After performing some testing activity, a second hash of these files was generated. It was found to be unchanged from the first.

2.5.5.4 FPT_TUD_EXT.1.4

2.5.5.4.1 TSS Evaluation Activity

The evaluator shall verify that the TSS identifies how updates to the application are signed by an authorized source. The definition of an authorized source must be contained in the TSS. The evaluator shall also ensure that the TSS (or the operational guidance) describes how candidate updates are obtained.

Section 6.6 of [ST] ("Protection of the TSF") states the vendor digitally signs TOE updates using a 4096-bit RSA key.

Section 6.6 of [ST] states the TOE platform provides the means to check for, verify and apply TOE updates. In addition, Section 7.0 of [Install] ("Software Updates") describes how the administrator obtains candidate updates.

2.5.5.4.2 Guidance Evaluation Activity

None.

2.5.5.4.3 Test Evaluation Activity

None.

2.5.5.5 FPT_TUD_EXT.1.5

2.5.5.5.1 TSS Evaluation Activity

The evaluator shall verify that the TSS identifies how the application is distributed. If "***with the platform***" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS. If "***as an additional package***" is selected the evaluator shall perform the tests in FPT_TUD_EXT.2.

Section 6.6 of [ST] states the TOE is distributed as a Docker container image. Refer to Section 2.5.6 for evaluation activities associated with FPT_TUD_EXT.2.

2.5.5.5.2 Guidance Evaluation Activity

None.

2.5.5.5.3 Test Evaluation Activity

None.

2.5.6 Integrity for Installation and Update (FPT_TUD_EXT.2)

2.5.6.1 FPT_TUD_EXT.2.1

2.5.6.1.1 TSS Evaluation Activity

None.

2.5.6.1.2 Guidance Evaluation Activity

None.

2.5.6.1.3 Test Evaluation Activity

Modified in accordance with TD0628.

If a container image is claimed the evaluator shall verify that application updates are distributed as container images. If the format of the platform-supported package manager is claimed, the evaluator shall verify that application updates are distributed in the format supported by the platform. This varies per platform:

Platforms: Linux… The evaluator shall ensure that the application is packaged in the format of the package management infrastructure of the chosen distribution. For example, applications running on Red Hat and Red Hat derivatives shall be packaged in RPM format. Applications running on Debian and Debian derivatives shall be packaged in DEB format.

The evaluator verified that the TOE is packaged in an appropriate format for container images.

2.5.6.2 FPT_TUD_EXT.2.2

2.5.6.2.1 TSS Evaluation Activity

None.

2.5.6.2.2 Guidance Evaluation Activity

None.

2.5.6.2.3 Test Evaluation Activity

Modified in accordance with TD0664.

All Other Platforms… The evaluator shall record the path of every file on the entire filesystem prior to installation of the application, and then install and run the application. Afterwards, the evaluator shall then uninstall the application, and compare the resulting filesystem to the initial record to verify that no files, other than configuration, output, and audit/log files, have been added to the filesystem.

The evaluator recorded the path of every file on the entire file system prior to installation of the TOE. The evaluator then installed and ran the TOE, after which the evaluator uninstalled the TOE. The evaluator again recorded the path of every file on the entire file system and verified that no files have been added to the file system, other than configuration, output, and audit/log files.

2.5.6.3 FPT_TUD_EXT.2.3

2.5.6.3.1 TSS Evaluation Activity

The evaluator shall verify that the TSS identifies how the application installation package is signed by an authorized source. The definition of an authorized source must be contained in the TSS.

Section 6.6 of [ST] ("Protection of the TSF") states the vendor digitally signs TOE installation packages (which are also used for TOE updates) using a 4096-bit RSA key.

2.5.6.3.2 Guidance Evaluation Activity

None.

2.5.6.3.3 Test Evaluation Activity

None.

2.6 Trusted Path/Channels (FTP)

2.6.1 Protection of Data in Transit (FTP_DIT_EXT.1)

2.6.1.1 TSS Evaluation Activity

For platform-provided functionality, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.

Section 5.2.6 of [ST] ("Trusted Path/Channels (FTP)") specifies the application shall invoke platform-provided functionality to encrypt all transmitted data with TLS and HTTPS. Section 6.7 of [ST] ("Trusted Path/Channels") states the TOE uses platform-provided TLS and HTTPS for service requests, data communication, and web administration.

The TOE uses nginx, which makes calls to the platform-provided OpenSSL library to implement trusted communications. Section 6.2 of [ST] ("Cryptographic Support"), Table 4 ("Cryptographic Functions") identifies the platform-provided OpenSSL library as Amazon Linux 2 OpenSSL Crypto Module.

2.6.1.2 Guidance Evaluation Activity

None.

2.6.1.3 Test Evaluation Activity

The evaluator shall perform the following tests:

Test 1: The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall verify from the packet capture that the traffic is encrypted with HTTPS, TLS, DTLS, SSH, or IPsec in accordance with the selection in the ST.

The evaluator observed the network traffic while accessing the TOE administrative interface and observed that the connection was protected with TLS.

Test 2: The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall review the packet capture and verify that no sensitive data is transmitted in the clear.

The evaluator observed that the TLS connection was encrypting the actual data transmitted between the two endpoints.

Test 3: The evaluator shall inspect the TSS to determine if user credentials are transmitted. If credentials are transmitted the evaluator shall set the credential to a known value. The evaluator shall capture packets from the application while causing credentials to be transmitted as described in the TSS. The evaluator shall perform a string search of the captured network packets and verify that the plaintext credential previously set by the evaluator is not found.

The TOE does not transmit user credentials; thus this test is Not Applicable.

3. Security Assurance Requirement Assurance Activities

3.1 Development (ADV)

3.1.1 Basic Functional Specification (ADV_FSP.1)

3.1.1.1 Assurance Activity

There are no specific assurance activities associated with these SARs, except ensuring the information is provided. The functional specification documentation is provided to support the evaluation activities described in Section 5.1, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.

The Assurance Activities identified above provided sufficient information to determine the appropriate content for the TSS section and to perform the assurance activities. Since these are directly associated with the SFRs, and are implicitly already done, no additional documentation or analysis is necessary.

3.2 Guidance Documents (AGD)

3.2.1 Operational User Guidance (AGD_OPE.1)

3.2.1.1 Assurance Activity

Some of the contents of the operational guidance will be verified by the assurance activities in Section 5.1 and evaluation of the TOE according to the [CEM]. The following additional information is also required. If cryptographic functions are provided by the TOE, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. The documentation must describe the process for verifying updates to the TOE by verifying a digital signature – this may be done by the TOE or the underlying platform. The evaluator shall verify that this process includes the following steps: Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature. The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.

The TOE does not implement cryptographic functions. Instead, it leverages platform-provided cryptography (specifically, the Amazon Linux 2 OpenSSL Crypto Module) for its cryptographic functionality.

The guidance provided by [Install] includes a description of how the administrator performs updates of the TOE. The description covers how to obtain the update and make it accessible to the TOE and how to initiate the update process. Refer to Section 7.0 (“Software Updates”) of [Install]. Applying the update downloads and stages new container images. When they are ready and have been validated, the platform restarts the necessary services with the new images in place. The administrator can discern the success or otherwise of an upgrade attempt by viewing the running TOE version displayed on the left hand column above the Sign Out button on each screen of the administrator GUI.

Section “Logical Boundaries” of [CCECG] describes the security functionality of the TOE that falls within the scope of evaluation, while section “Excluded from the Evaluation” lists specific TOE functionality not covered by the evaluation.

3.2.2 Preparative Procedures (AGD_PRE.1)

3.2.2.1 Assurance Activity

As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

The TOE in its evaluated configuration is supported on a single platform that is adequately addressed in the guidance documentation. Section “Physical Boundaries” of [CCECG] states the TOE consists of exactly one instance of Wickr Enterprise Server provided as a containerized software application evaluated on the following specific platform:

- Docker runtime engine v20.10.x
- Ubuntu 18.04
- Intel Xeon E5-2620v3 (Haswell) processor.

3.3 Tests (ATE)

3.3.1 Independent Testing – Conformance (ATE_IND.1)

3.3.1.1 Assurance Activity

The evaluator shall prepare a test plan and report documenting the testing aspects of the system, including any application crashes during testing. The evaluator shall determine the root cause of any application crashes and include that information in the report. The test plan covers all of the testing actions contained in the [CEM] and the body of this PP’s Assurance Activities.

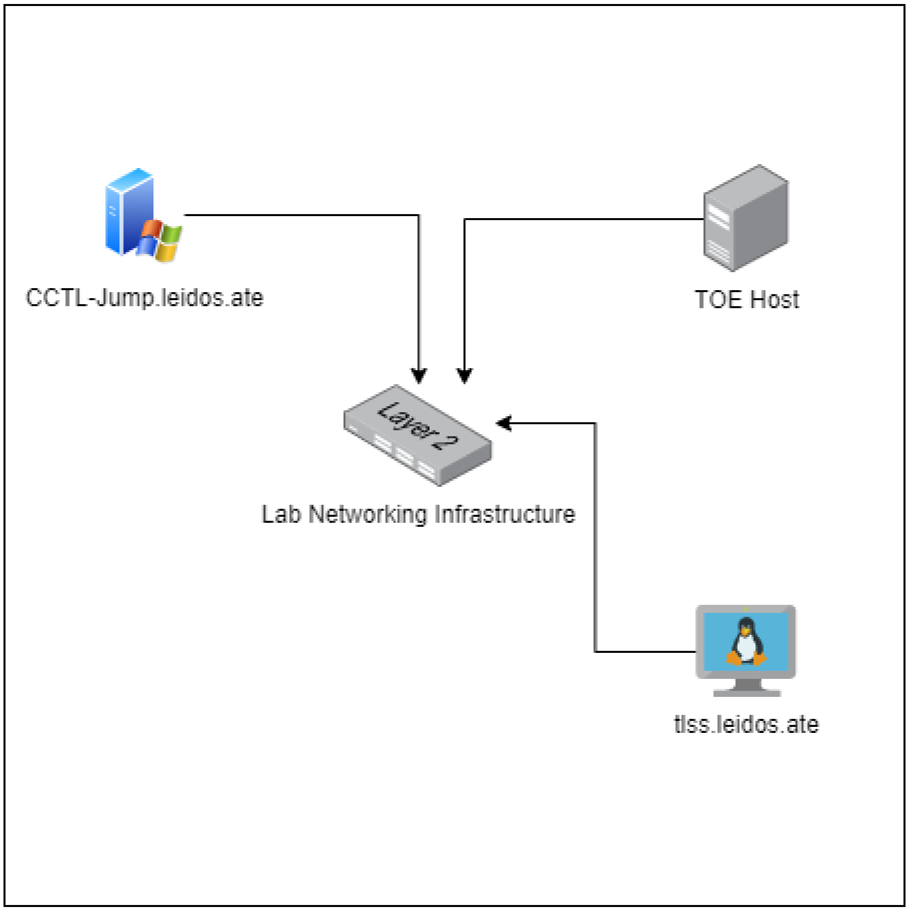
While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform.

This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS, SSH). The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results.

The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

The TOE was tested at Leidos's Columbia, MD location from March 2023 to April 2023. The procedures and results of this testing are available in the DTR document.

The following figure identifies the devices used for testing the TOE and describes the test configuration.



The following components were used to create the test configurations:

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
        - Software utilized: NMAP version 7.60; Wireshark v2.6.10
- 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
        - Software utilized: Chrome v112.0.5615.49.

3.4 Vulnerability Assessment (AVA)

3.4.1 Vulnerability Survey (AVA_VAN.1)

3.4.1.1 Assurance Activity

Modified in accordance with TD0554.

The evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses. The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious.

The evaluator documents the sources consulted and the vulnerabilities found in the report.

For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

For Windows, Linux, macOS and Solaris: The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious.

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 [ST].

No vulnerabilities were identified for the TOE.

The evaluator scanned the installer script using a corporate provided virus scan software (Microsoft Windows Defender) and verified that no virus signatures were detected.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

3.5 Life-Cycle Support (ALC)

3.5.1 Labeling of the TOE (ALC_CMC.1)

3.5.1.1 Assurance Activity

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Section 1.1 of [ST] ("Security Target, TOE and CC Identification") includes the TOE identification. The TOE is identified in terms of the software included in the evaluated configuration. This consists of Wickr Enterprise Server 1.30.0. This is consistent with the version number of the TOE identified in [CCECG] and the version identified by the TOE sample received for testing.

3.5.2 TOE Coverage (ALC_CMS.1)

3.5.2.1 Assurance Activity

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component. Life-cycle support is targeted aspects of the developer's life-cycle and instructions to providers of applications for the developer's devices, rather than an in-depth examination of the TSF manufacturer's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation.

The evaluator shall ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. The evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.

As described in Section 3.5.1 above, the evaluator confirmed the TOE is labelled with unique software version identifiers. Section 6.6 of [ST] ("Protection of the TSF") describes how the TOE uses security features and APIs provided by the Linux platform. This includes data execution protection, AppArmor, and stack-based buffer overflow protection.

3.5.3 Timely Security Update (ALC_TSU_EXT.1)

3.5.3.1 Assurance Activity

The evaluator shall verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator shall verify that this description addresses the entire application. The evaluator shall also verify that, in addition to the TOE developer's process, any third-party processes are also addressed in the description. The evaluator shall also verify that each mechanism for deployment of security updates is described.

The evaluator shall verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator shall verify that this time is expressed in a number or range of days.

The evaluator shall verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the TOE. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.

Section 6.1 of [ST] ("Timely Security Updates") describes the timely security update process used by the developer to create and deploy TOE security updates. The description encompasses the entirety of the TOE.

Wickr normally provides releases on a quarterly basis. Bugs may result in additional releases on accelerated schedules. The releases include bug fixes and security updates for all platform versions of the TOE. Additionally, when updates are made to bundled third-party capabilities, they are obtained by Wickr and included in releases. Wickr support personnel contact the POCs for affected customers. The only mechanism to deploy security updates is through maintenance releases. Upon discovery of a vulnerability, the impact will be assessed for priority based on the severity of the bug. The target timeline for releases ranges from 48 hours for critical bugs to 90 days for low severity bugs. Security reports are communicated from customers to Customer Support through an HTTPS form on the HackerOne platform.