National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
SecuSUITE v5.0 and SteelBox v5.0

Report Number: CCEVS-VR-11282-2022
Dated: December 9, 2022
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

Jenn Dotson
Lisa Mitchell
Lori Saren
Chris Thorpe
The MITRE Corporation

Common Criteria Testing Laboratory

Matai Spivey
Khai Van
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of SecuSUITE v5.0 and SteelBox v5.0 solution provided by BlackBerry Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in December 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints, Version 1.1, 31 May 2022 which includes the Base PP: Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14) and the PP-Module for PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0, 28 October 2020 (VVoIP10) with the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11).

The TOE is the SecuSUITE v5.0 and SteelBox v5.0.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 VR 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 (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

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

The technical information included in this report was obtained from the SecuSUITE v5.0 and SteelBox v5.0 Security Target, version 0.6, December 8, 2022 and analysis performed by the validation team.

2 Identification

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

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

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	SecuSUITE v5.0 and SteelBox v5.0 (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints, Version 1.1, 31 May 2022 which includes the Base PP: Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14) and the PP-Module for PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0, 28 October 2020 (VVoIP10) with the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)
ST	SecuSUITE v5.0 and SteelBox v5.0 Security Target, version 0.6, December 8, 2022
Evaluation Technical Report	Evaluation Technical Report for SecuSUITE v5.0 and SteelBox v5.0, version 0.3, December 8, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	BlackBerry Ltd
Developer	BlackBerry Ltd
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Lisa Mitchell, Lori Saren, Chris Thorpe

3 Assumptions & Clarification of Scope

Assumptions

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

- Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14)
- PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0, 28 October 2020 (VVoIP10)
- Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 (PKGTLS11)

That information has not been reproduced here and the ASPP14/VVoIP10/PKGTLS11 should be consulted if there is interest in that material.

Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14/VVoIP10/PKGTLS11 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Application Software Protection Profile with the PP-Module for Voice and Video over IP and the TLS Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Voice over IP Client models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- 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.

4 Architectural Information

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

The TOE is SecuSUITE v5.0 and SteelBox v5.0.

The TOE, herein referred to as the SecuSUITE/SteelBox Client or the TOE, is a VoIP application that executes on an Android 11 or iOS 14 mobile device operating system.

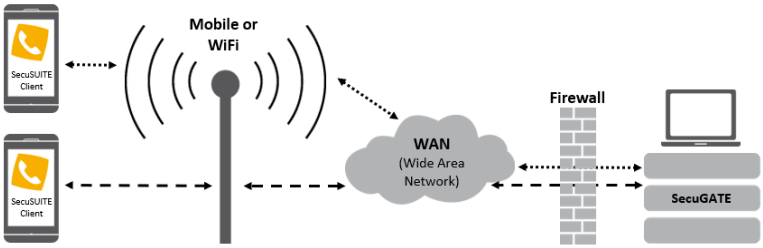

Figure 1 TOE Usage

User Context

The TOE user downloads the TOE from an app store (e.g. Apple Store, Google Play) or it is pushed via a Mobile Device Management (MDM) server (e.g. BlackBerry Enterprise Server) and installs the app to their mobile device. On first use of the app, the user must go through a registration process in order to register to a specified BlackBerry SecuGATE (identified by URI).

Once registered, the user can place secure VoIP calls using the app with largely the same interactions as with a normal phone call. The SecuSUITE Client provides encryption of user call signaling and voice data.

SecuSUITE Context

The TOE is part of the SecuSUITE Security Solution shown in Figure 2. The TOE does not work in isolation but relies on BlackBerry SecuGATE components to enable a secure VoIP communication.

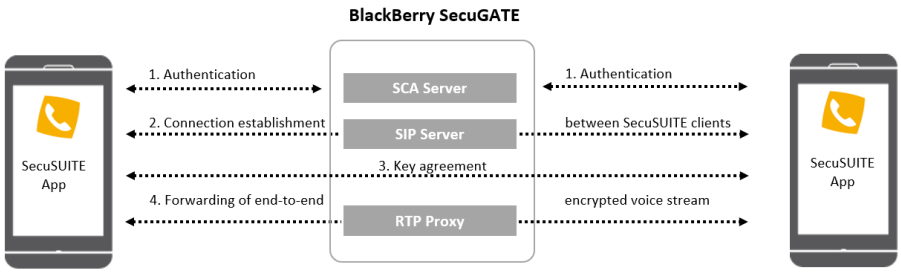

Figure 2 SecuSUITE Security Solution

VoIP Client

The SecuSUITE Client establishes a secure tunnel for voice communications with another SecuSUITE/SteelBox client or the SecuGATE SIP server. The tunnel provides confidentiality, integrity, and data authentication for information that travels across the public network. This occurs using the Secure Real-Time Transport Protocol (SRTP) that has been established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDES) for SDP - the TOE supports SDES-SRTP.

The TOE Client also protects communications between itself and the SIP Server by using a Transport Layer Security (TLS)-protected signaling channel. To register the TOE within the domain, the TOE is required to be password authenticated by the SIP Server. The TOE also makes use of certificates to authenticate both the SIP server end and the TOE itself through the TLS connection.

Group/Conference Calls

Besides the peer-to-peer calls between two instances of the TOE, the SecuSUITE/SteelBox solution also allows the set-up of a secure conference call between a group of SecuSUITE users.

Secure Text Messaging

The TOE client allows encrypted instant message transfer between client applications. Secure Text Messaging utilizes the same TLS protected communication channel that is used during initial SCA registration used to transfer client configuration settings and SIP credentials between SecuGATE and client.

Group Messaging

Besides the peer-to-peer text messaging between two instances of the TOE, the SecuSUITE/SteelBox solution also allows the set-up of messaging groups between an arbitrary number of SecuSUITE users. The messages are individually encrypted for all TOE users participating in the group messaging session the same way peer to peer messages are protected.

Calls Destined Beyond the SecuGATE SIP server

The TOE always encrypts the user's call signaling and data (voice) transmitted to other TOE VoIP endpoints registered with the SecuGATE and transmitted to the SecuGATE itself. The SecuGATE administrator can configure calling to additional endpoints, endpoints reached through a PBX (another SIP server connected to local/internal landline phones and potentially connected to outside phone lines). If so configured, the TOE can then place calls to additional endpoints beyond the SecuGATE through the configured PBX; however, because the call signaling and call data travels beyond the SecuGATE itself, its security ultimately lies beyond the TOE and SecuGATE SIP server's control.

While the ability of the SecuGATE SIP server to route calls to additional endpoints through a PBX lies beyond the scope of this ASPP14/PKGTLS11/VVoIPAS10 evaluation, the TOE can indicate when a user's call travels beyond the SecuGATE SIP server.

CACI SteelBox Client

The CACI SteelBox Client is a branded version of the SecuSUITE client that is identical from functional and security implementation perspective. The SteelBox client is distributed by BlackBerry's partner CACI and differs basically in the used UI assets and product publishing. The relevant deltas are:

- Different splash screens during client start-up
- Replaced UI Assets and Text elements (e.g., SteelBox logo, product name, app icon, status bar icon, EULA text and About screen).
- Changes required to distribute the client under an independent publisher/developer in the App Stores (e.g. developer signing).

4.1 TOE Architecture

The TOE is comprised of the SecuSUITE v5.0 and SteelBox v5.0.

To operate the SecuSUITE Client must be registered to *SecuSUITE* and to the BlackBerry SecuGATE SIP Server (also referred to as the Enterprise Session Controller, or ESC). Once properly registered, the Client can initiate or receive a "Call". Call data is exchanged with a VVoIP endpoint through SecuGATE which provides an SRTP proxy. The Enterprise Session Controller is also referred to as the SIP server.

4.2 Physical Boundaries

The TOE boundary is illustrated in Figure 3 TOE Boundary.

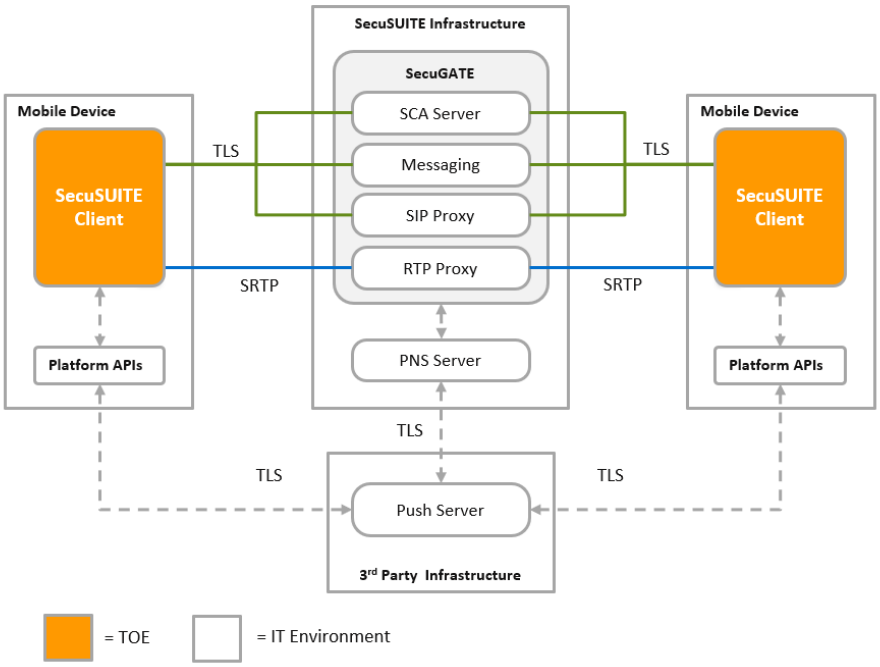

Figure 3 TOE Boundary

5 Security Policy

This section summaries the security functionality of the TOE:

1. Communication
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security management
6. Privacy
7. Protection of the TSF
8. TOE access

9. Trusted path/channels

5.1 Communication

The TOE utilizes the Opus codec by default to transmit voice media. The Opus codec utilizes a fixed bit-rate.

The TOE also includes the SILK vocoder to transmit voice media. The vocodec has been modified to pad the bit-rate in order to provide a constant bit-rate. This codec's purpose is to provide backwards compatibility with the TOE's previous versions, and this codec is only used if the peer VoIP client does not support the Opus codec.

5.2 Cryptographic support

The TOE includes its own cryptographic module to perform operations in support of authentication actions and network communications using the TLS and SRTP protocol. The TOE implements TLS version 1.2 with mutual authentication using elliptic-curve cryptography. The TOE also relies upon its platform for certain cryptographic operations including providing random data to seed the TOE's own DRBG. The TOE relies upon the platform (i.e., iOS and Android) cryptographic libraries for operations related to protecting keys in platform offer storage (i.e., a key store).

5.3 User data protection

The TOE enforces the media transmission policy when communicating with remote VVoIP endpoints which use TLS and SRTP protocols. The TOE also ensures that communication with an SCA server is protected using TLS. The TOE protects user data by utilizing platform services for data storage.

5.4 Identification and authentication

The TOE authenticates TLS peers using X.509v3 certificates. It performs extensive X.509 certificate validation checks on these certificates rejecting invalid or revoked certificates.

5.5 Security management

The TOE receives configuration setting during its registration with an SCA server. The client allows management operations that specify the SIP Server to use for connections.

5.6 Privacy

The TOE does not transmit Personally Identifiable Information over any network interfaces.

5.7 Protection of the TSF

The TOE relies on the physical boundary of the evaluated platform as well as the Android and iOS operating systems for the protection of the TOE's application components.

The TOE relies upon these platforms to indicate the current TOE version. If an update is needed, it is obtained from the platform's application store. The TOE's software is digitally signed in accordance with the requirements of each application store.

The native Apple and Android cryptographic library, which provides some of the TOE's cryptographic services, have built-in self-tests that are run at client start-up to ensure that the algorithms are correct. If any self-tests fail, the TOE will not be able to perform its cryptographic services. The TOE includes its own cryptographic library that also includes self-tests that are run when the client starts.

5.8 TOE access

The TOE includes a 15 second default timeout that can terminate idle voice/video transmission. This timeout value can be changed by the configuration obtained from the SCA server.

5.9 Trusted path/channels

The TOE encrypts all data transmitted with an SCA server or Enterprise Session Controller using TLS. The TLS channel established with an ESC can be used to exchange SIP messages or to initiate the use of SRTP for voice/video traffic.

6 Documentation

The following documents were available with the TOE for evaluation:

- Common Criteria Configuration Guide SecuSUITE v5.0 SteelBox v5.0, Version 1.1, 05-Dec-2022

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

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

7 Evaluated Configuration

The TOE executes on the following mobile devices[1]:

Samsung Galaxy devices with Android 11:

a) Samsung Devices (US Carrier)
- Snapdragon 888: **Galaxy S21 Ultra 5G**
  i. equivalent:
    1. Galaxy S21 5G
    2. Galaxy S21+ 5G
- Snapdragon 865: **Galaxy S20+ 5G**
  i. equivalent:
    1. Galaxy Z Fold2 5G
    2. Galaxy Note20 Ultra 5G
    3. Galaxy Note20 5G
    4. Galaxy Tab S7/S7+
    5. Galaxy Z Flip 5G
    6. Galaxy S20 Ultra 5G
    7. Galaxy S20 5G/FE

b) Samsung Devices (International Carriers)
- Exynos 2100: **Galaxy S21 Ultra 5G**
  i. equivalent:
    1. Galaxy S21 5G
    2. Galaxy S21+ 5G
- Exynos 990: **Galaxy S20+ 5G**
  i. equivalent:
    1. Galaxy S20 Ultra 5G
    2. Galaxy S20+ LTE
    3. Galaxy S20 5G/LTE/FE
    4. Galaxy Note20 Ultra 5G/LTE
    5. Galaxy Note20 5G/LTE
- Exynos 9611: Galaxy **XCover Pro**
  i. equivalent:
    1. Samsung A51

Apple devices running iOS14:

- **iPhone Xs**, Xs Max, XR
- **iPhone 12**, 12 Pro, 12 Pro Max, 12 Mini
- **iPhone 11**, 11 Pro, 11 Pro Max

Non-TOE Components

The TOE is part of the SecuSUITE security solution and requires the following components to be present in the environment:

[1] Note the list of equivalent devices is taken from the evaluated devices' Security Targets.

c) SecuSUITE SCA Server. The SCA Server authenticates users and facilitates VoIP client enrollment and pushes client SIP configuration to the client.

d) SecuSUITE SIP Server. The SIP Server is used to establish the secure connection between the mobile devices. The use of a TLS connection, providing encryption and mutual authentication, ensures that the devices connect with authorized SIP servers only and the dialed call numbers are transmitted encrypted.

e) SecuSUITE RTP Proxy. The Real-time Transport Protocol (RTP) Proxy bridges media packets sent between clients. The RTP Proxy is part of the SecuSUITE SIP Server. The SIP Server creates and deletes RTP and Real-time Transport Control Protocol (RTCP) bridging sessions in the RTP Proxy.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary Detailed Test Report for SecuSUITE v5.0 and SteelBox v5.0, Version 0.4, December 8, 2022 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14/VVoIP10/PKGTLS11 including the tests associated with optional requirements. The DTR in section 2 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

9 Results of the Evaluation

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

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the SecuSUITE and CACI SteelBox TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/VVoIP10/PKGTLS11.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the SecuSUITE v5.0 and SteelBox v5.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally the evaluation team performed the assurance activities specified in the ASPP14/VVoIP10/PKGTLS11 related to the examination of the information contained in the TSS.

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

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted

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

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

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

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the ASPP14/VVoIP10/PKGTLS11 and recorded the results in the DTR, summarized in the AAR.

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

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluation team searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "webrtc ", "Boost ", "ZLIB ", "BZip2 ", "Openssl 1.0.2", "pjproject ", "PocoCpp ", "libphonenumber ", "icu 63.1", "protobuf ", "opus ", "silk ", "libsrtp ", "secusmart", "secusuite", "pcsclite ", "androidx.lifecycle ", "androidannotations ", "bumptech.glide ", "PhotoView", "androidx.appcompat ", "androidx.biometric", "androidx.constraintlayout ", "androidx.recyclerview ", "android.material ", "joda-time", "spongycastle", "facebook.shimmer ", "androidx.emoji ", "firebase ", "zxing barcode scanner ", "YYImage ", "cryptocomply".

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

9.7 Summary of Evaluation Results

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

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

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Common Criteria Configuration Guide SecuSUITE v5.0 SteelBox v5.0, Version 1.1, 05-Dec-2022. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The ST is identified as: *SecuSUITE v5.0 and SteelBox v5.0 Security Target, version 0.6, December 8, 2022*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluation team to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

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

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

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

[4] PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints, Version 1.1, 31 May 2022.

[5] Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14)

[6] PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0, 28 October 2020 (VVoIP10).

[7] Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 (PKGTLS11).

[8] SecuSUITE v5.0 and SteelBox v5.0 Security Target, Version 0.6, December 8, 2022 (ST).

[9] Assurance Activity Report for SecuSUITE v5.0 and SteelBox v5.0, Version 0.4, December 8, 2022 (AAR).

[10] Detailed Test Report for SecuSUITE v5.0 and SteelBox v5.0, Version 0.4, December 8, 2022 (DTR).

[11] Evaluation Technical Report for SecuSUITE v5.0 and SteelBox v5.0, Version 0.3, December 8, 2022 (ETR).

[12] Common Criteria Configuration Guide SecuSUITE v5.0 SteelBox v5.0, Version 1.1, 05-Dec-2022 (AGD).