National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cisco Jabber 14.0 for Windows 10, Version 1.0

Report Number: CCEVS-VR-VID11251-2022
Dated: September 09, 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

Daniel Faigin: Senior Validator

Anne Gugel: Lead Validator (Trainee)

Patrick Mallett, PHD: Lead Validator

Richard (Rip) Toren: ECR Team (Trainee)

Common Criteria Testing Laboratory

Dipdev Pudasaini

Kenneth Lasoski

Sandeep Yanamandra

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this validation report, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Jabber 14.0 for Windows 10 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This validation report 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. This validation report applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in September 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements of the Protection Profile for Application Software Version 1.3, PP-Module for Voice and Video over IP (VVoIP) Version 1.0, Functional Package for TLS Version 1.1.

The 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), as interpreted by the Evaluation Activities contained in the Protection Profile for Application Software Version 1.3, PP-Module for Voice and Video over IP (VVoIP) Version 1.0, Functional Package for TLS Version 1.1 and all applicable NIAP technical decisions for the technology. 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 ETR are consistent with the evidence provided.

The validation 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 that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

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.

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) 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	Cisco Jabber 14.0 for Windows 10
Protection Profile	PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints V1.0 2020-10-28 CFG_APP-VVOIP_v1.0 The PP-Configuration includes the following components: • Protection Profile for Application Software V1.3 2019-03-01 PP_APP_v1.3 • PP-Module for Voice and Video over IP (VVoIP) V1.0 2020-10-28 MOD_VVOIP_V1.0 Package Claim: Functional Package for TLS V1.1 2019-03-01 PKG_TLS_V1.1
Security Target	Cisco Jabber 14.0 for Windows 10 Security Target v1.4, August 29, 2022
Evaluation Technical Report	Evaluation Technical Report for Cisco Jabber 14.0 for Windows 10, Version 0.6, September 6, 2022
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Daniel Faigin Anne Gugel Patrick Mallett Richard (Rip) Toren

3 Architectural Information

The TOE is a software-only client application that executes on a Windows 10 platform. It provides protected channels for interactive communication. This functionality fits Use Case 3 (Communication) as described in [App], Use Case 2 (Software Application) as described in [VVoIP], and Use Case 3 (Client-Server Architecture) in [VVoIP]. The focus of the Common Criteria evaluation is on the Video and Voice over IP telephony features of Cisco Jabber that it secures with SRTP and TLS 1.2.

Cisco Jabber allows users of an organization to securely make, receive, and control phone calls through Cisco Unified Communications Manager (CUCM). Users have a variety of call-control options including mute, call transfer, call forwarding, and impromptu conferencing.

4 Security Policy

The TOE provides security features in the following areas:

- Communication
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Channels

These features are described in more detail in the subsections below.

4.1 Communication

The Cisco Jabber TOE transmits voice media using a constant bitrate (CBR) vocoder.

4.2 Cryptographic Support

The Cisco Jabber TOE provides cryptography in support of SIP connections via Security Real-Time Transport Protocol (SRTP) established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDES) for SDP. The TOE also protects communications between itself and the CUCM SIP Server by using a Transport Layer Security (TLS)-protected signaling channel.

The TOE incorporates a CiscoSSL cryptographic module library (v7.2), and the algorithm implementation has been validated for CAVP conformance.

4.3 User Data protection

The TOE ensures that user data is not transmitted when a call is placed on hold, a call is placed on mute, or when the TOE is not registered with the SIP server. Additionally, the TOE restricts access to hardware resources and network communications to only those required.

4.4 Identification and Authentication

The TOE performs X.509 certificate authentication of remote components the TOE interacts with for SDES/SRTP and TLS connections. The Cisco Jabber TOE relies upon the TOE Platform to validate certificates.

4.5 Security Management

The TOE is capable of registering with an Enterprise Session Controller (ESC) and specifying the termination period for idle calls.

4.6 Protection of the TSF

The TOE leverages services and APIs provided by the platform in order to support anti-exploitation features and installation of authorized software updates.

4.7 Trusted Channels

The TOE's implementation of SDES-SRTP allows secure voice and video communication between itself and a remote VVoIP application and secure signaling communication between itself and a remote CUCM SIP Server using TLS.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The characteristics described in Table 2 are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2. TOE Assumptions

Assumption	Assumption Definition
A.PLATFORM	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.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	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.
A.UPDATE_SOURCE	It is assumed that TOE software/firmware updates will be made available on either the call control server that the TOE connects to or a separate file server managed by the organization.

5.2 Threats

Table 3 lists the threats fully or partially mitigated by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 3. Threats

Threat	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.
T.MEDIA_DISCLOSURE	An attacker can use the encrypted variable rate vocoder frames to their advantage to decode transmitted data.
T.UNDETECTED_TRANSMISSION	An attacker may cause the TOE to exfiltrate audio or video media over a remote channel while in a state where the user has a reasonable

Threat	Threat Definition
	expectation that no media is being transmitted.

5.3 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 only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Application Software Version 1.3, March 1, 2019 [App], PP-Module for Voice and Video over IP (VVoIP) Version 1.0, October 28, 2020, Functional Package for TLS Version 1.1, March 1, 2019 [TLS-PKG].
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

Section 7.2 lists functionality that is excluded from this evaluation.

6 Documentation

The following document was provided by the vendor with the TOE for evaluation:

- Cisco Jabber 14.0 for Windows 10 Common Criteria Configuration Guide, version 0.4 [AGD]

Only the Configuration Guide listed above should be trusted for the installation, administration, and use of this product in its evaluated configuration. The documents listed in Table 4 are supplemental documents that describe features and capabilities either excluded from the evaluation configuration or not covered by the evaluation.

Table 4. Cisco Documentation

Title	Link
Planning Guide for Cisco Jabber 14.0	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_0/cjab_b_planning-guide-cisco-jabber-14_0.html
On-Premises Deployment for Cisco Jabber 14.0	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_0/cjab_b_deploy-jabber-on-premises-14_0.html
Feature Configuration for Cisco Jabber 14.0	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_0/cjab_b_feature-configuration-cisco-jabber-14_0.html
Parameters Reference Guide for Cisco Jabber 14.0	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_0/cjab_book_parameters-reference-guide-for-cisco-jabber-14_0.html
Release Notes for Cisco Jabber 14.0	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_0/release-notes-for-cisco-jabber-14_0.html
Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/install/12_5_1/cucm_ll-guide-cucm-imp-1251.html
Administration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU1/adminGd/cucm_b_administration-guide-1251SU1.html
Security Guide for Cisco Unified Communications Manager, Release 12.5(1)SU2	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1SU2/cucm_b_security-guide-1251SU2.html
Virtualization for Cisco Unified Communications Manager (CUCM)	https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a software-only client application that executes on a Windows 10 platform.

The evaluated configuration is a single instance of Cisco Jabber operating in FIPS and CC mode when configured in accordance with the documentation specified in Section 6.

CUCM, release 12.0 or later, is the ESC (also referred to as the SIP Server) that serves as the call control component for voice and video. There are configuration settings the CUCM 'pushes' to the Cisco Jabber TOE, a form of management permitted in [VVoIP].

CUCM is required to be configured in the On-Premises deployment mode for softphones. Refer to the Cisco Jabber 14.0 for Windows 10 Common Criteria Configuration Guide for specific information regarding configuring CUCM in the On-Premises deployment mode for softphones.

Cisco Jabber allows users of an organization to securely make, receive, and control phone calls through Cisco Unified Communications Manager (CUCM). Users have a variety of call-control options including mute, call transfer, call forwarding, and impromptu conferencing.

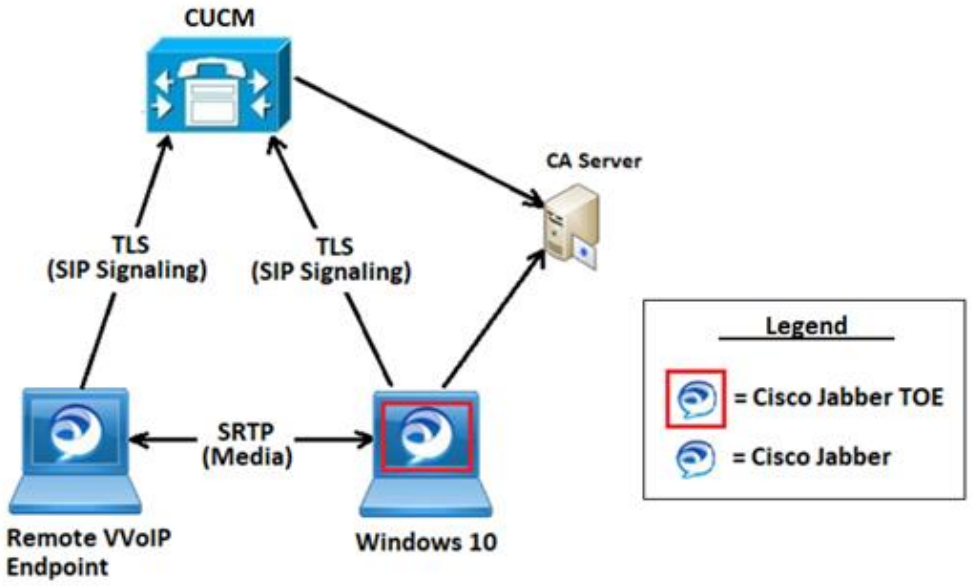

Figure 1 TOE in Relation to the IT Environment

Note: In the test environment, only one instance of Jabber is considered the TOE (outlined in red above). The TOE is limited by the Protection Profile regarding what TLS version and ciphers may be claimed. However, the TOE only exchanges SIP messaging with the ESC (CUCM), and there is nothing requiring other endpoints use TLS 1.2 exclusively, so for non-TOE endpoints, there is no limitation placed on the TLS version.

7.2 Excluded Functionality

The following functionality is not included in the CC evaluation:

Table 5. Excluded Functionality and Rationale

Function Excluded	Rationale
Non-FIPS 140-2 and non-CC modes of operation	FIPS and CC modes of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
SRTP with NULL cipher	SRTP with the NULL cipher does not provide encryption.
Jabber to Jabber calling. Jabber to Jabber calling provides basic voice and video calling capabilities between different Cisco Jabber clients without registering to Cisco Unified Communications Manager.	This feature is not TSF relevant functionality included in the Protection Profiles.
Cisco Instant Message and Presence Service (Instant Messaging and Presence)	This feature is not TSF relevant functionality included in the Protection Profiles.
Cisco Webex® Meetings Server (Online Web Conferencing)	This feature is not TSF relevant functionality included in the Protection Profiles.
Cisco Unity® Connection (Voicemail)	This feature is not TSF relevant functionality included in the Protection Profiles.
IBM Lotus Notes and Google Calendar	This feature is not TSF relevant functionality included in the Protection Profiles.

The functionality listed above is disabled in the TOE evaluated configuration (after following the guidance as specified in the Cisco Jabber 14.0 for Windows 10 Common Criteria Configuration Guide).

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Cisco Jabber 14.0 for Windows 10, which is not publicly available. The Assurance Activity Report provides an overview of testing and the prescribed evaluation activities.

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 the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Application Software Version 1.3, March 1, 2019 [App], PP-Module for Voice and Video over IP (VVoIP) Version 1.0, October 28, 2020, Functional Package for TLS Version 1.1, March 1, 2019 [TLS-PKG]. The Independent Testing activity is documented in Section 4 of the Assurance Activity Report, which is publicly available, and is not duplicated here.

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 documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all 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 Cisco Jabber 14.0 for Windows 10 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

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 Cisco Jabber 14.0 for Windows 10 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for Application Software Version 1.3, March 1, 2019 [App], PP-Module for Voice and Video over IP (VVoIP) Version 1.0, October 28, 2020, Functional Package for TLS Version 1.1, March 1, 2019 [TLS-PKG].

The validator 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 Development Documentation

The evaluation team applied each EAL 1 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's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities related to the examination of the information contained in the TOE Summary Specification.

The validator 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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities related to the examination of the information contained in the operational guidance documents.

The validator 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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/
- https://www.cvedetails.com/

The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on September 06, 2022.Cisco Jabber 14.0

- Cisco Jabber SRTP
- Cisco Jabber TCP
- Cisco Jabber SIP
- Windows API used in the TOE as listed in the ST
- Third-Party Libraries used in the TOE as listed in the ST

The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor. The validator 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 addressed the vulnerability analysis Assurance Activities 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 test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided demonstrates that the evaluation team performed the Assurance Activities 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 guidance document listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness

11 Annexes

Not applicable.

12 Security Target

Please see the Cisco Jabber 14.0 for Windows 10 Security Target v1.4, August 29, 2022 [ST].

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

14 Bibliography

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

1. Assurance Activity Report for Cisco Jabber 14.0 for Windows 10 v0.6, September 6, 2022.
2. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
4. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
5. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
6. Evaluation Technical Report for Cisco Jabber 14.0 for Windows 10, Version 0.6, September 6, 2022
7. Cisco Jabber 14.0 for Windows 10 Common Criteria Configuration Guide, version 0.4, August 17, 2022[AGD]
8. Protection Profile for Application Software Version 1.3, March 1,2019 [App],
9. PP-Module for Voice and Video over IP (VVoIP) Version 1.0, October 28,2020,
10. Functional Package for TLS Version 1.1, March 1,2019 [TLS-PKG].
11. Cisco Jabber 14.0 for Windows 10 Security Target v1.4, August 29, 2022 [ST]