National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Cisco Systems, Inc. Jabber 15.2

Report Number: CCEVS-VR-VID11635-2026
Dated: June 25, 2026
Version: 1.0

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

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

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
Patrick Mallett
The Aerospace Corporation

Anne Gugel
Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Douglas Kalmus
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 Cisco Jabber 15.2 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation 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 June 2026. 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 Extended, 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 Target of Evaluation (TOE) is the Cisco Jabber 15.2.

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). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Cisco Jabber 15.2 Security Target, version 0.5, June23, 2026 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 Common Criteria Testing Laboratories (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 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 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 15.2 (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	Cisco Jabber 15.2 Security Target, version 0.5, June 23, 2026
Evaluation Technical Report	Evaluation Technical Report for Cisco Jabber 15.2, version 0.2, June 25, 2026
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	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jerome Myers, Patrick Mallett, Anne Gugel

3 Architectural Information

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

Cisco Jabber provides users within an organization a number of features for collaborative communication:

Integrated Voice and Video Telephony - Securely make, receive, and control phone calls. Users have a variety of call control options including mute, call transfer, call forwarding, and impromptu conferencing.

Instant Messaging and Presence - View real-time availability of co-workers and securely chat in real time using instant messaging to save time and reduce phone tag.

Online Web Conferencing – Securely access online web conferencing services to collaborate in real-time.

Voicemail Services – Securely access voicemail and tools for managing messages.

The Common Criteria evaluation was limited to the Integrated Voice and Video over IP (VVoIP) telephony features of Cisco Jabber that it secures with SRTP and TLS 1.2. Video, Instant Messaging and Presence, Online Web Conferencing, and Voicemail Services is not covered by the evaluation. Additionally, call control options other than call placement and call receipt were not evaluated. Advanced features such as call transfer, call forwarding, and impromptu conferencing make use of SIP TLS 1.2, which is part of the evaluation.

3.1 TOE Description

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 depicts the TOE in relation to the IT environment.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The TOE has required environmental components to allow for operation and evaluation.

Component	Usage/Purpose Description for TOE performance
Windows Platform	The TOE requires a Windows OS platform.
Enterprise Session Controller	The Cisco Unified Communications Manager (CUCM) is the SIP Server that provides the TOE with call control and management. CUCM also acts as the configuration server.

Component	Usage/Purpose Description for TOE performance
Remote VoIP Application	This is the peer VoIP Application that the TOE interacts with using Security Real Time Transport Protocol (SRTP).
Certificate Authority	The Certification Authority provides X.509 certificates. The CA also provides a method to check the certificate revocation status of the CUCM Server.

3.4 Physical Boundaries

The TOE is a software-only client application that executes on a Windows 11 platform. For this evaluation, the Windows 11 device was a laptop with an Intel Core i5-1135G7 (Tiger Lake) CPU.

4 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. Protection of the TSF
7. Trusted Path/Channels

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 path/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 & 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)
- The PP-Module for 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, 01 March 2019 (PKGTLS11)

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

The scope of this evaluation was limited to the functionality and assurances covered in the 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.

Clarification of scope

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.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP14/VVoIP10/PKGTLS11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

Excluded Functionality

The following functionality is not included in the CC evaluation:

Table 2. Excluded Functionality and Rationale

Function Excluded	Rationale
Platforms other than Windows 11	The TOE was only evaluated on a Windows 11 Platform
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.

6 Documentation

The following documents were available with the TOE for evaluation:

- Cisco Jabber 15.2 Common Criteria Configuration Guide, Version 0.5, February 12, 2026

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 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 Cisco Jabber 15.2, Version 0.2, June 25, 2026 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team 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 AAR, in sections 1.1 and 3.4 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The evaluated configuration is a single instance of Cisco Jabber operating in FIPS and CC mode.

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-Premise deployment mode for softphones. Refer to the Cisco Jabber 15.2 Common Criteria Configuration Guide for specific information regarding configuring CUCM in the On-Premise deployment mode for softphones.

The specific software evaluated was 15.2.0.

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 Jabber 15.2 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 Cisco Jabber 15.2 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 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 Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the ASPP14/VVoIP10/PKGTLS11 related to the examination of the information contained in the TSS.

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.

9.3 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 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.

9.4 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 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 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 a Test Report, summarized in the AAR.

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.

9.6 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 evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

On June 25, 2026 the evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search), MITRE CVE Database and Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog, ref KEV) with the following search terms: “Cisco Jabber”, “Cisco SIP”, “Cisco SRTP”, “Cisco TCP”, “Windows 11”, “Intel Core i5-1135G7”, “Tiger Lake”, “nghttp2”, “gssapi32”, “tiny-xml”, “leveldb”, “plantronics software”, “chromium”, “openvino toolkit”, “krbcc32”, “kfwlogon”, “ippsp legacy”, “iintel integrated performance primitives”, “signal processing legacy”, “angle”, “ippsc legacy iintel integrated performance primitives”, “speech codecs legacy”, “visual-studio-runtime”, “microsoft windows operating system”, “openjpeg”, “libusb”, “leashw32”, “microsoft edge embedded browser webview loader”, “krb5_32”, “kerberos”, “skia”, “json-cpp”, “gloox”, “opencore-amr”, “plantronics jabber plugin”, “debugging tools for windows”, “gstreamer”, “zlib”, “free-type”, “threading-building-blocks”, “oneapi threading building blocks”, “sqlite”, “io-warrior-sdk”, “sigc++”, “libxml2”, “glib”, “re2”, “zlib”, “cyrus-sasl”, “libvorbis”, “pdfium”, “tidy”, “curl”, “boringssl”, “openssl”, “libjpeg-turbo”, “direct3d”, “protobuf”, “open-ldap”, “expat”, “gsoap”, “libcxx”, “cef”, “json-c”, “libxslt”, “pcre”, “jansson”, “libvpx”, “sql-cipher”, “xpprof32”, “blink”, “k5sprt32”, “boost”, “libjpeg”, “libphonenumber”, “opus”, “libpng”, “safestring”, “libwebp”, “glew”, “hunspell”, “rapidxml”, “speexdsp”, “comerr32”, “CertVerifyCertificateChainPolicy”, “CertGetCertificateChain”, “CryptAcquireContext”, “CryptCreateHash”, “CryptHashData”, “CryptGetHashParam”, “BCryptGenRandom”, “BCrypt”, “international components for unicode”, “Google v8”, “Apache Portable Runtime”, and “OpenType Sanitizer”.

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.

9.7 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 guidance documentation referenced in Section 6 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. 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 be relied upon when configuring or operating the device as evaluated.

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. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Jabber 15.2 Security Target, Version 0.5, June 23, 2026*.

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

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

[6] Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11).

[7] Cisco Jabber 15.2 Security Target, Version 0.5, June 23, 2026 (ST).

[8] Assurance Activity Report for Cisco Jabber 15.2, Version 0.2, June 25, 2026 (AAR).

[9] Detailed Test Report for Cisco Jabber 15.2, Version 0.2, June 25, 2026 (DTR).

[10] Evaluation Technical Report for Cisco Jabber 15.2, Version 0.2, June 25, 2026 (ETR).

[11] Cisco Jabber 15.2 Common Criteria Configuration Guide , Version 0.5, February 12, 2026