National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cisco Jabber 11.8 for Windows 10

Report Number:	**CCEVS-VR-10802-2017**
Dated:	**6/13/2017**
Version:	**1.0**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant

Joanne Fitzpatrick

The MITRE Corporation

Jerome Myers

The Aerospace Corporation

Common Criteria Testing Laboratory

Pascal Patin

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 VR, 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 for Windows 11.8 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR 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 May, 2017. 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 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Voice over IP (VoIP) Applications.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Voice over IP (VoIP) Applications Protection Profile. 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 functional requirements and assurance requirements stated in the Security Target (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 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 Protection Profile containing Assurance Activities, which are interpretation of 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 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 Product Compliance 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 11.8 for Windows 10
Protection Profile	Protection Profile for Voice Over IP (VoIP) Applications, Version 1.3
Security Target	Cisco Jabber for Windows 10 Security Target
Evaluation Technical Report	VID10802_AAR.doc
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Sheldon Durrant Joanne Fitzpatrick Jerome Myers

3 Architectural Information

The TOE is Cisco Jabber v11.8 for Windows 10 (herein after referred to as Cisco Jabber, VoIP Client, or the TOE). Cisco Jabber is an application that provides a single, intuitive interface for integration of collaborative communications including:

- Presence - View real-time availability of co-workers and colleagues within the enterprise network.
- Instant messaging (IM) - Chat in real time using instant messaging to save time and reduce phone tag.
- Voice over Internet Protocol (VoIP), voice messaging, and video calling capabilities with the ability to escalate calls into a Cisco WebEx meeting.

The focus of the evaluation is on the VoIP capabilities of Cisco Jabber.

4 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- 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. In addition, the TOE implements all RFCs of the [VoIP PP], as necessary to satisfy testing/assurance measures prescribed therein.

Cryptographic Support

The TOE provides cryptography in support of SIP connections via Security 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 also protects communications between itself and the CUCM SIP Server by using a Transport Layer Security (TLS)-protected signaling channel.

The cryptographic algorithm implementation has been validated for CAVP conformance.

The TOE Platform provides cryptography to support digital signature verification of X.509v3 certificates used to authenticate TLS and SDES/SRTP connections.

User Data Protection

The TOE ensures that voice data is not transmitted when a call is placed on hold, call placed on mute and when not connected.

Identification and authentication

The TOE performs authentication using passwords for SIP Register functions. The passwords must be at least eight (8) characters and include the use of upper and lower case characters, numbers and special characters.

The TOE Platform validates certificates using Online Certificate Status Protocol (OCSP). The certificates are used to support authentication for SDES/SRTP and TLS connections

Security Management

The TOE provides the capability to manage the following functions:

- Specify/Prompt the SIP Server to use for connections;
- Specify/Prompt the user to enter VoIP client credentials to use for connections;

- Specify/Prompt the password requirements for SIP authentications;
- Configure cryptographic algorithms;
- Ability to query the current version of the TOE; and
- Action taken when connection to verify validity of certificate cannot be established.

The TOE supports the administrative user to perform the above security relevant management functions.

The TOE Platform provides the capability to manage the following functions:

- Load X.509v3 certificates;
- Configure certificate revocation check; and
- Ability to update the TOE, and to verify the updates.

The TOE Platform supports the administrative user to perform the above security relevant management functions

Protection of the TSF

The TOE performs a suite of self-tests during initial start-up to verify correct operation of its CAVP validated algorithms. Upon execution, the integrity of the TOEs software executables is also verified.

The TOE Platform provides for verification of TOE software updates prior installation.

Trusted Channels

The TOE’s implementation of SDES-SRTP allows secure voice communications between itself and a remote VoIP application. In addition, the TOE provides secure signaling communications between itself and a remote CUCM SIP Server using TLS.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections 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.

Assumption	Assumption Definition
A.AVAILABILITY	Network resources shall be available to allow VoIP clients to satisfy mission requirements and to transmit information.
A.OPER_ENV	The operational environment of the TOE appropriately addresses those requirements, threats, and policies not applicable to the TOE itself, but that are necessary to support the correct operation of the TOE.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	Threat Definition
T.TSF_CONFIGURATION	Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	Voice data may be inadvertently sent to a destination not intended because it is sent outside the voice call.

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 VoIP PP.
- Consistent with the expectations of the Protection Profile, 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.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Jabber 11.8 for Windows 10 Security Target, Version 0.8
- Cisco Jabber 11.8 for Windows 10 Common Criteria Configuration Guide, Version 0.4

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a VoIP client application executing on a Microsoft Windows 10 platform. It requires one of the following Common Criteria certified Microsoft Windows 10 Operating System to run:

- Microsoft Windows 10 Home Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Enterprise Edition (32-bit and 64-bit versions)

Refer to the Microsoft Windows 10 Security Target[1] certified on 2016-04-05 for information regarding the evaluated configuration requirements.

The TOE requires support of Cisco Unified Communications Manager (CUCM), release 11.0 or later as the SIP Server. Cisco CUCM serves as the call-processing component for voice that includes IP telephony, mobility features and calls controls. In addition, there are configuration settings pushed to the Cisco Jabber TOE that are required in the evaluated configuration. This form of management is permitted in [VoIP PP].

The Cisco CUCM is required to deploy Cisco Jabber for *On-Premise* deployment scenario, that is one in which the Administrator sets up, manages, and maintains all services on the organization's network. Additionally, Cisco Jabber must be deployed in *Phone Mode*, where the user's primary authentication is to Cisco Unified Communications Manager. In Phone Mode, the user is provisioned with VoIP capabilities without the functionality of presence or instant messaging (IM).

7.2 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Presence, instant messaging (IM), voice messaging, and video functionality.	These Jabber functions are not covered in the CC evaluation.
SIP connection over TLS using NULL-SHA encryption	Provides only integrity and authentication without encryption.

[1] http://www.commoncriteriaportal.org/products/

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Cisco Jabber for Windows 11.8, which is not publicly available. The Assurance Activities Report provides an overview of testing, including test configuration and testbeds (AAR section 4.9), as well as the prescribed assurance 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 the vendor-provided guidance documentation and ran the tests specified in the VoIP PP. The Independent Testing activity is documented in the Assurance Activities 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 Evaluation Technical Report (ETR). The reader of this document can assume that 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 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Jabber for Windows 11.8 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the VoIP 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 for Windows 11.8 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 VoIP PP.

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 Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the VoIP PP 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 specified in the VoIP PP 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 Activities in the VoIP PP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

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 in the VoIP PP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing, and did not discover any issues with the TOE. A list of databases searched, and keywords used, may be found in section 4.8.2 of 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 addressed the vulnerability analysis Assurance Activities in the VoIP PP, 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 by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the VoIP PP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

This section contains observations, recommendations, and caveats formulated by the validation team during the course of the evaluation and validation effort.

- As mentioned in previous portions of this report, the Cisco Jabber client can only be used with the evaluated Cisco CUCM server. The CUCM server offers functionality that is needed for Jabber to operate in the manner in which it was tested against the Assurance Activities in the VOIP PP.

11 Annexes

Not applicable.

12 Security Target

Cisco Jabber 11.8 for Windows 10 Security Target, Version 0.5

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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.