National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Cisco Jabber for Windows

Report Number:	**CCEVS-VR-10659-2015**
Dated:	**November 13, 2015**
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

Members from

The Aerospace Corporation,
The MITRE Corporation,

Common Criteria Testing Laboratory

Acumen Security, LLC

Table of Contents

List of Tables

1 Executive Summary

This report 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 in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with the Assurance Activity Report (AAR) and this Validation Report (VR), which describe how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 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 Cisco Jabber for Windows Voice Over IP (VOIP) client. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (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 as documented in the ST.

The evaluation of Cisco Jabber for Windows was performed by Acumen Security, LLC Common Criteria Testing Laboratory (CCTL) in Montgomery Village, Maryland, in the United States and was completed in November 2015. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in Protection Profile for Voice Over IP (VOIP) Applications, version 1.3. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www,niap-ccevs.org).

The Acumen Security evaluation team determined that Cisco Jabber for Windows is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the AAR and associated test report produced by the Acumen Security evaluation team.

The TOE is a software solution that consists of the Cisco Jabber client, version 11.0, running on evaluated Windows 8 Pro and Enterprise Edition systems as described in Windows 8 ST (NIAP VID 10520; https://www.niap-ccevs.org/st/Compliant.cfm?pid=10520).

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the 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.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Cisco Jabber for Windows, version 11.0
Sponsor & Developer	Cisco Systems, Inc.

Item	Identifier
CCTL	Acumen Security, LLC Common Criteria Testing Laboratory Montgomery Village, MD, USA
Completion Date	November 2015
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Protection Profile for Voice Over IP (VOIP) Applications, Version 1.3
Evaluation Class	None
Disclaimer	The information contained in this Validation Report is not an endorsement of the Cisco Jabber for Windows client by any agency of the U.S. Government and no warranty of Cisco Jabber for Windows is either expressed or implied.
Validation Body	National Information Assurance Partnership, CCEVS

2 Identification

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Cisco Jabber for Windows Security Target
ST Version	1.0
Publication Date	November 12, 2015
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Jabber for Windows, Jabber
TOE Hardware Models	N/A
TOE Software Version	11.0
Keywords	Authentication, Voice, Telephony

2.1 Threats

The PP (and thus the ST) identifies the following threats that the TOE and its operational environment are intended to counter:

- The ST does not include requirements that can protect against an insider threat. Authorized users are not considered hostile or malicious and are trusted to follow appropriate guidance. Only authorized personnel should have access to the client device on which the VoIP Application is installed. Therefore, the primary threat agents are the unauthorized entities that try to gain access.

  The remote endpoint of the voice communication can be both geographically and logically distant from the TOE, and pass through a variety of other systems. These intermediate systems may be under the control of the adversary, and offer an opportunity for communications over the network to be compromised.

  Plaintext communication over the network may allow critical data (such as passwords, configuration settings, and user data) to be read and/or manipulated directly by intermediate systems, leading to a compromise of the TOE. SDES-SRTP can be used to provide protection for this communication; however, there are a myriad of options that can be implemented for the protocol to be compliant to the protocol specification listed in the RFC. Some of these options can have negative impacts on the security of the connection. For instance, using a weak encryption algorithm (even one that is allowed by the RFC, such as DES) can allow an adversary to read and even manipulate the data on the encrypted channel, thus circumventing countermeasures in place to prevent such attacks. Further, if the protocol is implemented with little-used or non-standard options, it may be compliant with the protocol specification but will not be able to interact with other, diverse equipment that is typically found in large enterprises.

  Even though the communication path is protected, there is a possibility that the remote SIP Server could be duped into thinking that a malicious third-party user or system is the TOE. For instance, a middleman could intercept a connection request to the TOE, and respond to the SIP Server as if it were the TOE. In a similar manner, the TOE could also be duped into thinking that it is establishing communications with a legitimate remote SIP Server when in fact it is not. An attacker could also mount a malicious man-in-the-middle-type of attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and modified by this system. This attack can even be mounted via encrypted communication channels if appropriate countermeasures are not applied. These attacks are, in part, enabled by a malicious attacker capturing network traffic (for instance, an authentication session) and “playing back” that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.

- Configuring VoIP tunnels is a complex and time-consuming process, and prone to errors if the interface for doing so is not well-specified or well-behaved. The inability to configure certain aspects of the interface may also lead to the mis-specification of the desired communications policy or use of cryptography that may be desired or required for a particular users’ site. This may result in unintended weak or plain-text communications while the user thinks that their data are being protected. Other aspects of configuring the TOE or using its security mechanisms (for example, the update process) may also result in a reduction in the trustworthiness of the VoIP Application.
- Since one of the most common attack vectors used involves attacking unpatched versions of software containing well-known flaws, updating the VoIP client application is necessary to ensure that changes to threat environment are addressed. Timely application of patches ensures that the client is a “hard target”, thus increasing the likelihood that product will be able to maintain and enforce its security policy. However, the updates to be applied to the product must be trustable in some manner; otherwise, an attacker can write their own “update” that instead contains malicious code of their choosing, such as a rootkit, bot, or other malware. Once this “update” is installed, the attacker then has control of the system and all of its data.

  Methods of countering this threat typically involve hashes of the updates, and potentially cryptographic operations (e.g., digital signatures) on those hashes as well. However, the validity of these methods introduces additional threats. For instance, a weak hash function could result in the attacker being able to modify the legitimate update in such a way that the hash remained unchanged. For cryptographic signature schemes, there are dependencies on

  1) the strength of the cryptographic algorithm used to provide the signature, and

  2) the ability of the end user to verify the signature (which typically involves checking a hierarchy of digital signatures back to a root of trust (a certificate authority)).

  If a cryptographic signature scheme is weak, then it may be compromised by an attacker and the end user will install a malicious update, thinking that it is legitimate. Similarly, if the root of trust can be compromised, then a strong digital signature algorithm will not stop the malicious update from being installed (the attacker will just create their own signature on the update using the compromised root of trust, and the malicious update will then be installed without detection).
- Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.

2.2 Organizational Security Policies

There are no Organizational Security Policies for the VOIP PP.

3 Architectural Information

The TOE is a software solution that is installed on the following Common Criteria certified Microsoft Window operating systems:

- Microsoft Windows 8 Pro and Enterprise Edition, 32 bit and 64 bit—supported in Jabber Desktop mode only

Refer to the Microsoft Windows 8 Security Target for information regarding the evaluated configuration requirements.

The TOE also 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. As such there are configuration settings that are pushed to Jabber for Windows that are required in the evaluated configuration. These settings cannot be changed. Refer to the Cisco Unified Communications Manager (CUCM) Security Target for information regarding the evaluated configuration requirements of CUCM 11.0.

The TOE is comprised of several security features:

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

In addition, the TOE implements all RFCs of the VoIP PPv1.3 as necessary to satisfy testing/assurance measures prescribed therein.

The TOE provides cryptography in support of other Cisco Jabber for Windows security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 1.

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

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 provides the capability to manage the following functions:

- Identify SIP Servers used for communications;
- Specify the credentials used for connections;
- Enforce the password requirements for SIP authentications;
- Cryptographic functionality; and

- Update to the TOE.

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

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- It is assumed that network resources shall be available to allow VoIP clients to satisfy mission requirements and to transmit information.
- It is assumed that 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. In particular, the Cisco CUCM identified above is the only SIP server to which the Cisco Jabber for Windows Client can be connected in the evaluated configuration.
- It is assumed that personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

4.1 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:

1. 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 claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Cryptographic Support

The TOE Client Device Platform provides cryptography in support of other Cisco Jabber for Windows security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 1.

The TOE Client Device Platform 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 TOE Client Device Platform uses the X.509v3 certificate for securing TLS and SDES/SRTP connections.

5.2 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.

5.3 Identification and Authentication

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

5.4 Security Management

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

- Configure cryptographic algorithms;
- Load X5.09v3 certificates;
- Configure certificate revocation check; and
- Ability to update the TOE, and to verify the updates.

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

5.5 Protection of the TSF

The TOE Client Device Platform protects against interference and tampering by untrusted subjects by implementing authentication and access controls to limit configuration to the administrative user.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

5.6 Trusted Path/Channels

The TOE allows secure communications between itself and a remote CUCM SIP Server using TLS.

6 Documentation

The following documents were available with the TOE for evaluation:

1. Cisco Jabber for Windows Security Target [ST], version 1.0;
2. Cisco Jabber for Windows Common Criteria Configuration Guide [AGD], version 1.0.

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

Test Plan for a Target of Evaluation, Cisco Jabber for Windows Version 11.0, Version 1.2, November 9th, 2015.

Assurance Activity Report for a Target of Evaluation, Cisco Jabber for Windows Version 11.0, version 1.2, November 9th, 2015

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to VOIP PP version 1.3.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in VIOP PP. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above. A summary of that testing is contained in the AAR and is not repeated here.

Independent testing took place at the CCTL location in Montgomery Village, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE (on Windows 8 Pro 64-bit, configured as per the Microsoft Windows 8 and Windows Server 2012 ST) in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for VOIP PP version 1.3 were fulfilled.

8 Evaluated Configuration

The Cisco Jabber for Windows version 11.0 running on any of

- Microsoft Windows 8 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 8 Enterprise Edition (32-bit and 64-bit versions)

TOE Hardware Identification: Hardware consist with that defined in the Microsoft Windows 8 and Windows Server 2012 ST.

In addition, the Cisco CUCM is the only SIP server that can be used by Cisco Jabber for Windows.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Voice Over IP (VOIP), Version 1.3, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

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 claimed PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Acumen CCTL. A summary of the assessment is contained in the *Cisco Jabber for Windows VOIP PP Assurance Activity Report, version 1.3, November 11th, 2015*. The security assurance requirements are listed in the following table.

Table 3: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

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

Name	Description
ST Title	Cisco Jabber for Windows Security Target
ST Version	1.0
Publication Date	12 November, 2015

13 Abbreviations and Acronyms

AAA	Authentication, Authorization and Accounting
AAR	Assurance Activities Report
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	CC Testing Laboratory
CEM	Common Methodology for IT Security Evaluation
CLI	Command Line Interface
EP	Extended Package
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IOS	Inter-network Operating System
IPsec	Internet Protocol security
IT	Information Technology
LAN	Local Area Network
NIAP	National Information Assurance Partnership
NIM	Network Interface Module
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PCL	Product Compliant List
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment
SA	Security Association
SAR	Security Assurance Requirement
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell version 2
SSL	Secure Sockets Layer
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
USB	Universal Serial Bus
VPN	Virtual Private Network
VR	Validation Report
WAN	Wide Area Network

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, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Cisco Unified Communications Manager Security Target, Version 1.0, 12 November, 2015.

[6] [ETR] Cisco Jabber for Windows Security Target Evaluation Technical Report, version 1.0, 11 November, 2015.

[7] [Guidance Docs] Cisco Jabber for Windows Common Criteria Configuration Guide [AGD], version 1.0, 11 November, 2015.

[8] [AAR] Cisco Jabber for Windows VOIP PP Assurance Activity Report, version 1.3, 11 November, 2015