



2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

November 29th, 2018

To Whom It May Concern:

Acumen Security verified that the following product faithfully embeds a FIPS 140-2 validated cryptographic module,

- Cisco Jabber version 12.5

The software version is known to operate on the following platforms:

- Apple iOS 12
- Android 9
- Microsoft Windows 10

During the course of the review, Acumen Security confirmed that the following cryptographic module is properly incorporated into the product:

- CiscoSSL FIPS Object Module, version 6.2, FIPS 140-2 Certificate #2984

As part of the review, the software was tested on the following platforms:

- Apple iPad - iOS 12
- Google Pixel - Android 9
- IBM ThinkPad - Microsoft Windows 10

Acumen Security confirmed that the following features leverage at least one of the embedded cryptographic modules to provide cryptographic services for **sRTP and TLS** (HTTPS, SIP and XMPP).

- Session establishment supporting each service.
- All underlying cryptographic algorithms supporting each services' key derivation functions.
- Hashing for each service.
- Symmetric encryption for each service.

Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties. This letter represents the independent opinions of Acumen Security and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ashit Vora', with a horizontal line underneath.

Ashit Vora
Laboratory Director