



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

November 19, 2019

To Whom It May Concern:

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

- Cisco WebEx Meetings Server (CWMS) version 4.0

During the course of the review, Acumen Security confirmed that the following FIPS 140-2 cryptographic module is incorporated into the product,

- Cisco FIPS Object Module (FOM) (Software Version 6.0) – Cert # 2505

Acumen Security confirmed that the following features leverage the embedded Cisco FIPS Object Module (FOM) to provide cryptographic services for **TLS (SIP, HTTPs) and SSH**

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

Additionally, Acumen Security confirmed that the above referenced cryptographic module is initialized in a manner consistent with the instructions provided in the non-proprietary Security Policy.

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 drawn through it.

Ashit Vora
Laboratory Director
Acumen Security