

August 3, 2016

To Whom It May Concern:

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

- Cisco Meeting Server 2.0

The software is known to operate on the following platforms

- VMware
- Microsoft Hyper-V
- X-Series Hardware

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

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

- VMware

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for **TLS (SIP, HTTPS, XMPP), SSH, and sRTP**:

1. Session establishment supporting each service,
2. All underlying cryptographic algorithms supporting each services' key derivation functions,
3. Hashing for each service,
4. 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,



Ashit Vora
Laboratory Director
Acumen Security