



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

July 18, 2018

To Whom It May Concern:

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

- Cisco Unified Border Element (CUBE) on Cloud Services Router (CSR) 1000V, version IOS XE 16.9

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

- Cisco FIPS Object Module (FOM) (Software Version 6.0) – Cert # 2505
- Cisco IOS Common Cryptographic Module Rel5 (IC2M Rel5) – Cert # 2388

Acumen Security confirmed that the following features leverage the embedded Cisco FIPS Object Module for **sRTP** and Cisco IOS Common Cryptographic Module Rel5 for **TLS (HTTPS and SIP)** for the following cryptographic services,

- 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 underneath.

Ashit Vora
Laboratory Director
Acumen Security