October 28, 2016

To Whom It May Concern:

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

- Cisco Email Security Appliance (ESA) 9.8.

The software is known to operate on the following platforms:

- C100V,
- C300V,
- C600V,
- ESA C170,
- ESA C190
- ESA C370,
- ESA C380,
- ESA C390
- ESA C670,
- ESA C680,
- ESA C690,
- ESA C690X
- ESA C1070.

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

- CiscoSSL FIPS Object Module Version: 6.0, FIPS 140-2 certificate #2505,

Acumen Security confirmed that the following features leverage the embedded module to provide cryptographic services,

- Encryption, Hashing, Key Derivation, Key Exchange, and Asymmetric Cryptography associated with the following services:
    - o TLS,
    - o SSH,
    - o SCP.
- Hashing and Asymmetric Cryptography associated with the following services:
    - o DKIM.

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