Acumen Security

June 27, 2016

To whom it may concern,

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

- Cisco TelePresence Video Communication Server (VCS) Software (version X8.8)
- Cisco Expressway Series (version X8.8)

The referenced software is known to operate on the following products.

- Cisco Video Communication Server (VCS)
- Cisco Expressway Series

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

- Cisco 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, Key Derivation, and hashing associated with the following services:
  - SSH,
  - SNMP,
  - TLS,
  - sRTP,
  - H.323.
- Diffie-Hellman associated with the following services:
  - SSH,
  - TLS,
  - sRTP,
  - H.323.
- Asymmetric Key based authentication associated with the following services:
  - SSH,
  - TLS,
  - H.323.

Each of the above referenced services can be configured in a manner that restricts algorithm selection to only FIPS 140-2 approved algorithms.

Additionally, Acumen Security confirmed that the above referenced embedded 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