Acumen Security

June 10, 2016

To Whom It May Concern,

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

- Cisco IOS-XE 16.2

The software is known to operate on the following products,

- Catalyst 3650 Series Switches
- Catalyst 3850 Series Switches

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

- Cisco Catalyst 3650
- Cisco Catalyst 3850

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

- IOS Common Cryptographic Module (IC2M), version Rel 5, FIPS 140-2 certificate # 2388

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

- Encryption, hashing, and asymmetric authentication associated with the following services,
  - SSH,
  - SNMP,
  - IKE/IPsec,
  - TLS.
- Diffie-Hellman associated with the following services:
  - SSH
  - TLS.
- Key Derivation associated with the following services:
  - SSH
  - TLS

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