Acumen Security

November 3, 2017

To Whom It May Concern:

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

- Cisco Catalyst 9300
- Cisco Catalyst 9400
- Cisco Catalyst 9500

The hardware is known to operate with the following operating system,

- Cisco IOS 16.6

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

- IOS Common Cryptographic Module, Release 5, FIPS 140-2 certificate # 2388

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

- Encryption and Hashing associated with the following services:
  - SSH,
  - TLS,
  - SNMPv3,
  - IPSec/IKE v2.
- Key Derivation associated with the following services,
  - SSH,
  - TLS,
  - SNMPv3,
  - IPSec/IKE v2.
- Diffie Hellman and Asymmetric Encryption associated with the following services,
  - SSH,
  - TLS,
  - IPSec/IKE v2.

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