Acumen Security

February 5, 2016

To whom it may concern,

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

- IOS 15.5M

The referenced software is known to operate on the following routing platforms,

- ISR 1905
- ISR 1921
- ISR 1941
- ISR 2901
- ISR 2911
- ISR 2921
- ISR 2951
- ISR 3925
- ISR 3945
- ISR 3925E
- ISR 3945E
- ESR 5900

As part of the review, the software was tested on the following products,

- ISR 1921
- ISR 2911
- ISR 2921
- ISR 2951
- ISR 3945E
- ESR 5900

During the course of the Vendor provided documentation review, physical testing of referenced software running on the listed platforms and source code review, Acumen Security confirmed that the following cryptographic module is properly incorporated into the product:

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

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

- Hashing and bulk Encryption associated with the following cryptographic services:
  - SSH,
  - SNMP,
  - IKE/IPsec,
  - TLS
  - sRTP
- Asymmetric authentication and Diffie-Hellman associated with the following services:
  - SSH,
  - IKE/IPsec
  - 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 the 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