Acumen Security

May 28, 2015

Whom It May Concern:

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

- IOS-XE 3.13

The software is known to operate on the following platforms:

- ASR 1001 Router
- ASR 1001-X Router
- ASR 1002 Router
- ASR 1002-X Router
- ASR 1004 Router
- ASR 1006 Router
- ASR 1013 Router

With the following modules installed, when applicable:

- Route Processor 1 (RP1)
- Route Processor 2 (RP2)
- Embedded Service Processor 5 (ESP5)
- Embedded Service Processor 10 (ESP10)
- Embedded Service Processor 20 (ESP20)
- Embedded Service Processor 40 (ESP40)
- Embedded Service Processor 100 (ESP100)
- Embedded Service Processor 200 (ESP200)

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

- ASR 1001-X Router

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

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

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for ***TLS***, ***SSH***, ***SNMPv3***, and ***IKE/IPsec***:

1. Session establishment supporting each service,
2. All underlying cryptographic algorithms supporting each services' key derivation functions,
3. Hashing for each service.

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for ***TLS***, ***SSH***, and ***SNMPv3***:

1. Symmetric encryption for each service.

Additionally, Acumen Security confirmed that the host platforms use the following CAVP validated AES implementation for ***IPsec*** bulk encryption.

Hardware Component	Triple DES	AES
Embedded Service Processor 5 (ESP5)	Cert #397	Cert #333
Embedded Service Processor 10 (ESP10)	Cert #397	Cert #333
Embedded Service Processor 20 (ESP20)	Cert #397	Cert #333
Embedded Service Processor 40 (ESP40)	Cert #397	Cert #333
Embedded Service Processor 100 (ESP100)	Cert #1469	Cert #2346
Embedded Service Processor 200 (ESP200)	Cert #1469	Cert #2346

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.

Please let us know if you have any questions.

Sincerely,

Ashit Vora

Laboratory Director