



2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

November 27, 2017

Whom It May Concern:

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

- Cisco IOS version 15.5SY

The software version is known to operate on the following platform(s)

- Catalyst 6500 Series with Sup2T and Sup6T:
 - Catalyst 6503-E
 - Catalyst 6504-E
 - Catalyst 6506-E
 - Catalyst 6509-E
 - Catalyst 6513-E
- Catalyst 6800-X Series:
 - Catalyst 6816-X
 - Catalyst 6824-X
 - Catalyst 6832-X
 - Catalyst 6840-X
 - Catalyst 6880-X
- Catalyst 6807-XL with Sup2T and Sup6T

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

- IOS Common Cryptographic Module (IC2M) Rel5 – Cert #2388

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

- Session establishment supporting each service,
- All underlying cryptographic algorithms supporting each services' key derivation functions,
- Hashing for each service.
- Symmetric encryption for each service.

Additionally, Acumen security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for **Radius and TACACS**.

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,

A handwritten signature in black ink, appearing to read 'Ashit Vora', is written over a light blue horizontal line.

Ashit Vora
Laboratory Director