Acumen Security

1/10/2017

Whom It May Concern:

Acumen Security verified that the following product faithfully embeds a FIPS 140-2 validated cryptographic module, ***Cisco IOS-XE version 16.3***.

The software version is known to operate on the following platforms:

- Aggregation Services Router (ASR) 1000 Series.

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,

Feature	**Cryptographic Service**
IKE/IPsec SNMPv2 SSH 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.
Encrypted Password	Symmetric encryption.
Radius TACACS BGP OSPF NTP	• Session establishment supporting each service, • All underlying cryptographic algorithms supporting each services' key derivation functions, • Hashing for each service, • Symmetric encryption for each service. When transmitted through an IKE/IPsec tunnel.

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