Acumen Security

May 28, 2015

To Whom It May Concern,

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

1. IOS-XE 3.13.(1)S

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

1. ASR 902
2. ASR 903
3. ASR 920

The reference platform used within this review was the ASR 903 platform.

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

1. 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:

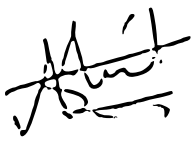
1. Hashing and bulk encryption associated with the following cryptographic services:
    a. SSH,
    b. SNMP,
    c. IKE/IPsec.
2. Asymmetric authentication and Diffie-Hellman associated with the following services:
    a. SSH,
    b. IKE/IPsec

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 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

18504 Office Park Dr • Montgomery Village MD 20886 • USA
Tel.: +1.703.375.9820 | info@acumensecurity.net | www.acumensecurity.net