Acumen Security

June 5, 2017

Whom It May Concern:

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

- IOS XR version 6.2

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

- ASR 9000 Series Routers with/without Tomahawk 100GE MACsec Module
- CRS-1 Router (4 slot/8 slot/16 slot)
- NCS 5000 Series Routers
- NCS 5500 Series Routers
- NCS 1000 Series Routers
- NCS 4000 Series Routers
- NCS 6000 Series Routers

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

- CiscoSSL FIPS Object Module Version: 6.0, FIPS 140-2 certificate #2505

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for **SSH, TLS, IKE/IPsec, RSA Key Generation** ***Transport Layer Security (TLS 1.0/SSL 3.1)***, ***Secure Shell (SSH v2)***, **RSA Key Generation**, and ***Simple Network Management Protocol (SNMPv3)***

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

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