April 15, 2020

To Whom It May Concern,

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

- IOS XR version 6.6

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

- ASR 9000 Series Routers
- NCS 5000 Series Routers
- NCS 5500 Series Routers
- NCS 6000 Series Routers
- NCS 500 Series Routers

During the course of the review, Acumen Security confirmed that the following cryptographic module is properly incorporated into the product:
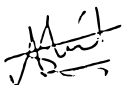
- Cisco FIPS Object Module Version: 6.0, FIPS 140-2 certificate #2505

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services.

1. Session establishment supporting the following service:
    o SSHv2

2. All underlying cryptographic algorithms supporting the following service key derivation function:
    o SSHv2

3. Hashing for the following services:
    o SSHv2
    o SNMPv3
    o OSPF over IPsec

4. Asymmetric key based encryption/authentication for the following services:
    o SSHv2
    o RSA Key Generation

5. Symmetric encryption/decryption for the following services:
    o SSHv2
    o SNMPv3
    o OSPF over IPsec

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
Acumen Security