



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

Jan 26, 2018

Whom It May Concern:

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

- NCS 5500 Series Routers

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

- IOS XR version 6.3

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, OSPF over IKE/IPsec, RSA Key Generation and SNMPv3.

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

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

Ashit Vora
Laboratory Director