



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

February 26, 2019

To Whom It May Concern:

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

- NX-OS version 8.3

The software is known to operate on the following platforms:

- MDS 9000 Series Switches

During the course of the review, Acumen Security confirmed that the following FIPS 140-2 cryptographic module is incorporated into the product,

- CiscoSSL FIPS Object Module Version: 6.2, FIPS 140-2 certificate #2984

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for **SSH** and **SNMPv3**:

- Session establishment supporting each service,
- All underlying cryptographic algorithms supporting each services' key derivation functions,
- Hashing for each service,
- Symmetric encryption for each service,
- Asymmetric encryption for each service,
- Diffie-Hellman Key Exchange 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', with a horizontal line drawn through it.

Ashit Vora
Laboratory Director