



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

January 15, 2019

To Whom It May Concern:

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

- Cisco Integrated Management Controller version 4.0

The software is known to operate on following platforms,

- Cisco Unified Computing System (C-Series, S-Series)

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: 6.0, FIPS 140-2 certificate #2505

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

- Encryption and Decryption associated with the following services:
 - SSH,
 - TLS,
 - SNMPv3.
- Hashing associated with the following services:
 - SSH,
 - TLS,
 - SNMPv3.
- Key Derivation associated with the following services,
 - SSH,
 - TLS.
- Diffie Hellman and Asymmetric Encryption associated with the following services,
 - SSH,
 - TLS.

Additionally, Acumen Security confirmed that the above referenced 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,

A handwritten signature in black ink, appearing to read 'Ashit Vora', with a horizontal line underneath.

Ashit Vora
Laboratory Director