July 25, 2016

To Whom It May Concern:

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

- Cisco Emergency Responder software version 11.5.

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

- Cisco FIPS Object Module (Version 6.0), certificate #2505,
- RSA BSAFE® Crypto-J JSAFE and JCE Software Module (version 6.1), certificate #2058.

Acumen Security confirmed that the following features leverage the embedded modules to provide cryptographic services, including, encryption, hashing, key derivation, key exchange, and asymmetric s:

- Cisco FIPS Object Module (Version 6.0):
    - Certificate Management for self-signed certificate generation.
- RSA BSAFE® Crypto-J JSAFE and JCE Software Module (version 6.1):
    - HTTPS (TLS),
    - SOAP AXL Interface,
    - SFTP for Disaster Recovery System,
    - JTAPI Communication,
    - Email Communication.

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,

Ashit Vora
Laboratory Director