Acumen Security

November 28, 2016

To Whom It May Concern:

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

- Cisco Wireless IP Phone 8821 v11.0 (which is compatible with CUCM versions 9.1(2), 10.5(2), 11.0(1), 11.5(1) and later),
- Cisco Wireless IP Phone 8821-EX v11.0 (which is compatible with CUCM versions 9.1(2), 10.5(2), 11.0(1), 11.5(1) and later).

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 products leverage the above referenced cryptographic module to provide cryptography for the following services, ***Transport Layer Security***, ***sRTP***, ***Secure Storage, RSA Signature Verification, File Authentication and Encryption,*** and ***Image Authentication***.

The cryptographic module provides all of the cryptographic functionality for each of the services listed above, including:

- Session establishment and key derivation functions (TLS),
- Hashing and Authentication (TLS, sRTP, File Authentication, Image Authentication),
- Symmetric encryption (TLS, sRTP, Secure Storage, File Encryption),
- Asymmetric cryptography (TLS, RSA Signature Verification).

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