

November 10, 2020

Whom It May Concern:

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

- Firmware Version IOS-XE 17.3

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

- Cisco Aironet 1562e/i/d/ps Wireless LAN Access Points
- Cisco Aironet 2802e/i Wireless LAN Access Points
- Cisco Aironet 3802e/i/p Wireless LAN Access Points
- Cisco Aironet 4800 Wireless LAN Access Point
- Cisco Aironet IW6300H-AC/DC/DCW Wireless LAN Access Points
- Cisco Aironet ESW6300 Wireless LAN Access Points

As a part of review, the firmware was tested on the following product(s):

- Cisco Aironet 1562e/i Wireless LAN Access Points
- Cisco Aironet 2802e/i Wireless LAN Access Points
- Cisco Aironet 3802e/i Wireless LAN Access Points
- Cisco Aironet 4800 Wireless LAN Access Point
- Cisco Aironet IW6300H-AC Wireless LAN Access Point

During the course of review, Acumen Security confirmed that the following cryptographic module is properly incorporated into the product:

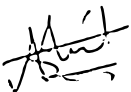
- CiscoSSL FIPS Object Module (Version 6.2), Cert #2984

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for **DTLS and Client Authentication using 802.11**.

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



Ashit Vora
Laboratory Director

