

November 10, 2020

Whom It May Concern:

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

- Firmware Versions: AireOS 8.10MR3 and IOS-XE 17.3

The Firmware versions are known to operate on the following hardware platform(s):

- Cisco Aironet 9115AXI/AXE Wireless LAN Access Points
- Cisco Aironet 9120AXI/AXE/AXP Wireless LAN Access Points
- Cisco Aironet 9130AXI/AXE Wireless LAN Access Points
- Cisco Aironet 9105AXI/AXW Wireless LAN Access Points

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

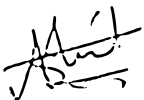
- CiscoSSL FIPS Object Module (Version 6.2), Cert #2984

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

