February 9, 2022

To Whom It May Concern,

A conformance review of Cisco Catalyst 9100, Wave 2, and IoT Series Access Points with software version 17.6 was completed and found that the Product integrates the following FIPS 140-2 approved cryptographic module:

1. Cisco FIPS Object Module (FIPS 140-2 Cert. #4036)

Cisco confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for DTLS and 802.1x Authentication:

1. Session establishment supporting each service,
2. All underlying cryptographic algorithms supporting each services' key derivation functions,
3. Hashing for each service,
4. Symmetric encryption for each service.

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

1. C9115AXI/AXE Wireless LAN Access Points
2. C9120AXI/AXE/AXP Wireless LAN Access Points
3. C9130AXI/AXE Wireless LAN Access Points
4. C9105AXI/AXW Wireless LAN Access Points
5. C9124AXI/AXE/AXD Wireless LAN Access Points
6. Cisco Aironet 1562E/I/D/P Wireless LAN Access Points
7. Cisco Aironet 2802E/I Wireless LAN Access Points
8. Cisco Aironet 3802E/I/P Wireless LAN Access Points
9. Cisco Aironet 4800 Wireless LAN Access Point
10. Cisco Aironet IW6300H-AC/DC/DCW Wireless LAN Access Points
11. Cisco Aironet ESW6300 Wireless LAN Access Points

Details of Cisco's review, which consisted of source code review and operational testing, can be provided upon request. The intention of this letter is to provide an assessment and assurance that the Product correctly integrates and uses the validated cryptographic module within the scope of the claims indicated above. The Cryptographic Module Validation Program (CMVP) has not independently reviewed this analysis, testing or the results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Edward D Paradise

Ed Paradise
VP Engineering
Cisco S&TO