June 15, 2022

To Whom It May Concern

A conformance review of Cisco Catalyst 9800 Series Wireless LAN Controllers (9800-40, 9800-80, 9800-L, and 9800-CL) version 16.12 ("the Product") 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. #4174)
2. Cisco IOS Common Crypto Module (IC2M) (FIPS 140-2 Cert. #4222)

Cisco confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for DTLS, TLS, SNMPv3, and IKE/IPSec (#4174) and SSH (#4222):

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.

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
SVP Engineering
Cisco S&TO