March 26, 2021

To Whom It May Concern

A conformance review of Cisco Integrated Management Controller (CIMC), version 4.1 ("the Product") was completed and found that the Product incorporates the following FIPS 140-2 validated cryptographic module:

1. Cisco FIPS Object Module version 7.2 (FIPS 140-2 Cert #3790)

Cisco confirmed that the following features leverage the embedded cryptographic modules listed above and provides all the cryptographic services for TLS, SSH and SNMP protocols used by CIMC:

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.

Cisco Integrated Management Controller (CIMC), enters FIPS mode when it gets selected under Security Management/Security Configuration the down the page under Federal Information Processing Standard (FIPS) and Common Criteria (CC) Configuration select Enable FIPS.

Details of Cisco's review, which consisted of build process, 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 modules listed above 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,

Ed Paradise
VP Engineering
Cisco S&TO