July 24, 2018

To Whom It May Concern

Cisco completed its conformance review of Cisco Hyperflex (Version:3.0)("the Product") and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic module:

1. Cisco FIPS Object Module (FIPS 140-2 Cert. #2505)

Specifically, Cisco's review confirmed that:

1. The cryptographic module (mentioned above) is initialized in a manner that is compliant with its individual security policy. Note: the cryptographic module supports pre-SP800-131 key strength (less than 112-bits). In order to operate in an approved mode of operation, applications must only use cryptographic services with key strength of 112-bit or greater.
2. All cryptographic algorithms used in SSH v2 and TLS for sessions establishment, are offloaded to Cisco FIPS Object Module with FIPS 140-2 Cert. #2505
3. Bulk data encryption for the established SSH v2 and TLS secure connections use the Cisco FIPS Object Module with FIPS 140-2 Cert. #2505

Details of Cisco's review, which consisted of source code review and operational testing, can be provided upon request.

Moreover, the FIPS conformance claims made for Cisco Hyperflex, version 2.5, verified by Acumen Security, LLC., hold true for Cisco Hyperflex, version 3.0, with no additions or removal of cryptographic services or cryptographic implementations.

The intention of this letter is to provide our assessment that the Product correctly integrates and uses validated cryptographic modules within the scope of the claims indicated above. Cisco offers no warranties or guarantees with respect to the above described conformance review. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed Cisco's analysis, testing or 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