October 21, 2022

To Whom It May Concern

A conformance review of Cisco IOS-XE Release v17.9 ("the Product") deployed on the following devices:

- Cisco ESS 3300 Embedded Switch

was completed and found that the Product integrates the following FIPS 140-2 approved cryptographic module:

- Cisco IOS Common Cryptographic Module (IC2M) (FIPS 140-2 Cert. #4222).

Cisco confirms that the embedded cryptographic module listed above provides all cryptographic services for the following: SSH

The review/testing confirmed that:

1. The cryptographic module is initialized in a manner that is compliant with its security policy
2. All cryptographic algorithms used in session establishment for the protocols above are handled within the cryptographic module
3. All cryptographic algorithms needed to support Image authentication, file authentication and encryption, RSA signature verification, and secure storage

In keeping with the last paragraph of the Cryptographic Module Validation Program (CMVP) requirements for validated modules (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules), this signed letter serves as confirmation that the product, with the embedded cryptographic module, which is a validated module found on the CMVP website (https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4222), provides the cryptographic services listed above. The information within this letter can be verified against the CMVP validation entry for certificate #4222.

The CMVP has not independently reviewed this analysis, testing, or 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
Cisco Senior Vice President
Foundational & Government Security