December 1, 2023

To Whom It May Concern

A conformance review of Cisco IOS-XE Release v17.12 (“the Product”) deployed on the following devices:

- Catalyst 9200 Series Switches
- Catalyst 9300 Series Switches
- Catalyst 9400 Series Switches
- Catalyst 9500 Series Switches
- Catalyst 9600 Series Switches

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) https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4222
- FIPS Object Module (FOM) 7.2a (FIPS 140-2 Cert. #4036 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4036.

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

- Security protocols – IKEv2/IPsec, TLSv1.2, SSHv2, SNMPv3.

The review/testing confirmed that:

1. The cryptographic modules (mentioned above) are initialized in a manner that is compliant with its Security Policy.
2. All cryptographic algorithms used for session establishment are handled within the cryptographic module.
3. All underlying cryptographic algorithms support each service’s key derivation function.

This letter has been generated in accordance with guidance provided by the Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules).

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