February 11, 2024

To Whom It May Concern:

A conformance review of Cisco IOS XE version 17.15 (“the Product”) deployed on the following devices:

- C1100TGX-1N24P32A
- C1100TG-1N24P32A
- C1100TG-1N32A

was completed and found that the Product incorporates the following FIPS 140-2 validated cryptographic module:

- Cisco IOS Common Cryptographic Module IC2Mrel5a ((FIPS 140-2 Cert. #4222)
- FIPS Object Module (FOM) 7.2a (FIPS 140-2 Cert. #4036)

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

- IPsec[1]
- SNMPv3
- SSH
- TLS

The review/testing confirmed that:

1. The cryptographic module (mentioned above) initializes in a way compliant with its Security Policy.
2. All applicable cryptographic algorithms used for session establishment are handled within the cryptographic module.
3. All applicable 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). The CMVP has not independently reviewed this analysis, testing, or the results.

Any questions regarding these statements may be directed via e-mail to the Cisco Global Certification Team (GCT) at certteam@cisco.com.

Sincerely,

Edward D Paradise

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security

[1] IPsec is validated for control plane only. The ModP calculation for Diffie-Hellman is offloaded to hardware, and then used in the software implementation. The hardware acceleration chip used in the ModP calculation is not validated as part of this compliance review.