October 16, 2025

To Whom It May Concern

A compliance review of Cisco IOS XE version 17.18 (“the Product”) deployed on the following platforms:

- Cisco Unified Border Element (CUBE)

running on:

- ASR 1006-X
- C8000v
- C8200L-1N-4T
- C8200-1N-4T
- C8300-1N1S-6T
- C8300-1N1S-4T2X
- C8300-2N2S-6T
- C8300-2N2S-4T2X
- ISR 4461

was completed and found that the Product incorporates the following FIPS 140-3 validated cryptographic modules:

- Cisco IOS Common Cryptographic Module (IC2M) Rel5b (CMVP Certificate: #4752)

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

- IPsec
- SSHv2
- SNMPv3
- TLSv1.2/v1.3

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