October 16, 2025

To Whom It May Concern

A compliance review of Cisco IOS XE Release v17.18 (“the Product”) deployed in the following platforms:

IE-3200	IE-3300	IE-3400	IE-3500
IE-3200-8T2S	IE-3300-8T2S	IE-3400-8T2S	IE-3500-8T3S
IE-3200-8P2S	IE-3300-8P2S	IE-3400-8P2S	IE3500-8T3X
	IE-3300-8T2X		IE-3500-8P3S
	IE-3300-8U2X		IE3500-8U3X
			IE-3505-8T3S
			IE-3505-8P3S

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

- 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:

- SSHv2
- SNMPv3

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