December 5, 2025

To Whom It May Concern:

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

- Cisco Catalyst 9200 Series Switches, which includes:

Modular Switches	Fixed Uplink Switches	Compact Switches
C9200-24T	C9200L-24T-4G	C9200CX-8P-2X2G
C9200-24P	C9200L-24P-4G	C9200CX-8P-2XGH
C9200-24PB	C9200L-48T-4G	C9200CX-8UXG-2X
C9200-24PXG	C9200L-48P-4G	C9200CX-8UXG-2XH
C9200-48T	C9200L-48PL-4G	C9200CX-12P-2XGH
C9200-48P	C9200L-24T-4X	C9200CX-12T-2X2G
C9200-48PL	C9200L-24P-4X	C9200CX-12P-2X2G
C9200-48PB	C9200L-48T-4X	
C9200-48PXG	C9200L-48P-4X	
	C9200L-48PL-4X	
	C9200L-24PXG-4X	
	C9200L-48PXG-4X	
	C9200L-24PXG-2Y	
	C9200L-48PXG-2Y	

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

- Cisco IOS Common Cryptographic Module (IC2M) Rel5b (CMVP Cert. #4752)
- FIPS Object Module (FOM) 7.3a (CMVP Cert. #4747)

Cisco confirms that the cryptographic modules listed above provide cryptographic services for the following as applicable:

- TLSv1.2
- SSHv2
- SNMPv3

The review/testing confirmed that:

1. The cryptographic modules (mentioned above) initialize in a manner that is 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