



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 9300 Series Switches, which includes:

Modular Uplink Switches	Fixed Uplink Switches
C9300-24H C9300-24P C9300-24S C9300-24T C9300-24U C9300-24UB C9300-24UX C9300-24UXB C9300-48H C9300-48P C9300-48S C9300-48T C9300-48U C9300-48UB C9300-48UN C9300-48UXM C9300X-12Y C9300X-24HX C9300X-24Y C9300X-48HX C9300X-48HXN C9300X-48TX	C9300L-24P-4G C9300L-24P-4X C9300L-24T-4G C9300L-24T-4X C9300L-24UXG-2Q C9300L-24UXG-4X C9300L-48P-4G C9300L-48P-4X C9300L-48PF-4G C9300L-48PF-4X C9300L-48T-4G C9300L-48T-4X C9300L-48UXG-2Q C9300L-48UXG-4X C9300LM-24U-4Y C9300LM-48T-4Y C9300LM-48U-4Y C9300LM-48UX-4Y

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

- Cisco IOS Common Cryptographic Module (IC2M) Rel5b (Cert. [#5356](#))
- FIPS Object Module (FOM) 7.3a (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,

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security