October 2, 2025

To Whom It May Concern,

A compliance review of Cisco Catalyst Center, version 3.1 (“the Product”) deployed in various docker set-ups

was completed and found that the Product integrates the following FIPS 140-3 approved cryptographic module:

1. Cisco FIPS Object Module 7.3a (Certificate #4747)
2. CiscoSSL FIPS Provider (Certificate #4891)
3. BC-FJA (Bouncy Castle FIPS Java API) (Certificate #4743)

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

- SSHv2
- TLSv1.2 and v1.3
- SNMPv3

The review/testing confirmed that:

1. The cryptographic modules (mentioned above) do initialize in a manner that is compliant with its various Security Policy.
2. All applicable cryptographic algorithms used for session establishment are handled within the perspective 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