



June 28, 2022

To Whom It May Concern

Cisco Systems, Inc performed a conformance review of the following devices (the "Product") running IOS-XE Release v17.6:

- Catalyst 9200 Series Switches
- Catalyst 9300 Series Switches
- Catalyst 9400 Series Switches
- Catalyst 9500 Series Switches
- Catalyst 9600 Series Switches

The Product integrates the following FIPS 140-2 approved cryptographic modules:

- Cisco IOS Common Cryptographic Module (IC2M) (FIPS 140-2 Cert. #4222)

Cisco confirms that the following features leverage the embedded cryptographic module to provide cryptographic services:

- Security protocols – IKEv2, IPsec, SSH, SNMPv3
 - All cryptographic algorithms necessary to support each protocol's key derivation function
 - Session establishment
 - Hashing
 - Symmetric encryption

Details of Cisco's review, which consisted of source code review and operational testing, are available upon request. The intention of this letter is to provide an assessment and assurance that the Product correctly integrates and uses the validated cryptographic module within the scope of the claims indicated above. The Cryptographic Module Validation Program (CMVP) has not independently reviewed this analysis, testing, or the results.

Direct questions regarding these statements to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

A handwritten signature in cursive script that reads "Edward D Paradise".

Ed Paradise
SVP Engineering
Cisco S&TO