To Whom It May Concern,

Acumen Security verified that the following product faithfully embeds a FIPS 140-2 validated cryptographic module,

- Cisco IOS-XE Release 17.6

The software version is known to operate on the following platform(s):

- Cisco C8500 Series Edge Routers
- Cisco C8300 Series Edge Routers
- Cisco C8200 Series Edge Routers
- Cisco Aggregation Services Router (ASR) 1000 series.
- Cisco Integrated Services Router (ISR) 4000 series.
- Cisco Integrated Services Router (ISR) 1000 series.
- Cisco C8000V Edge Software.
- CUBE
- ESR 6300 Series Embedded Services Routers
- IR 1100, 1800 Series Industrial Routers

During the review, Acumen Security confirmed that the following cryptographic module is properly incorporated into the product:
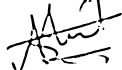
- IOS Common Cryptographic Module (IC2M) Rel5 - Cert #2388
- Cisco FIPS Object Module (FOM) 7.0 - Cert #3341 (CUBE only)

Acumen Security confirmed that the following features leverage the embedded cryptographic module,

Feature	Cryptographic Service
IKE/IPsec SNMPv3 SSH TLS TLS(HTTPS)	• Session establishment supporting each service, • All underlying cryptographic algorithms supporting each services' key derivation functions, • Hashing for each service, • Symmetric encryption for each service.
Encrypted Passwords	• Symmetric encryption
RADIUS TACACS BGP IKE/IPsec OSPF NTP IS-IS	• Session establishment supporting each service, • All underlying cryptographic algorithms supporting each services' key derivation functions, • Hashing for each service, • Symmetric encryption for each service. When transmitted through an IKE/IPsec tunnel.
sRTP	• CUBE Only

Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties. This letter represents the independent opinions of Acumen Security and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,

Ashit Vora
Laboratory Director