Acumen Security, LLC
2400 Research Blvd.
Suite 395
Rockville, MD 20850
Tel. +1 703 375 9820
acumensecurity.net

08/16/2020

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 17.3

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

- Cisco Unified Border Element (CUBE) on Cisco Cloud Services Router (CSR) 1000v.

During the course of 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

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 sRTP	• 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.

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