

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

July 8, 2021

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 17.4

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

- Cisco C8500L Series Edge Routers
- Cisco C8200 Series Edge 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

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

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







July 8, 2021

To Whom It May Concern,

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

Cisco IOS-XE SD-WAN Release 17.4

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

- Cisco C8500L Series Edge Routers
- Cisco C8200 Series Edge Routers

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	Session establishment supporting each service,
SNMPv3	
SSH	All underlying cryptographic algorithms
TLS	supporting each services' key derivation
TLS(HTTPS)	functions,
	Hashing for each service,
	Symmetric encryption for each service.
Encrypted Passwords	Symmetric encryption
RADIUS	Session establishment supporting each
TACACS	service,
BGP	All underlying cryptographic algorithms
IKE/IPsec	supporting each services' key derivation
OSPF	functions,
NTP IS-IS	 Hashing for each service,
13-13	
	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

