

August 17, 2017

Whom It May Concern:

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

- Cisco Network Convergence System Routers (IOS-XE16.6)
- Cisco Aggregation Services Routers (IOS-XE 16.6)

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

- Cisco NCS 4201
- Cisco NCS 4202
- Cisco NCS 4206
- Cisco NCS 4216
- Cisco ASR 903
- Cisco ASR 907
- Cisco ASR 920
- Cisco ASR 902

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

As part of the review, the software was tested on the following platforms:


- Cisco Network Convergence System (NCS) 4206
- Cisco Aggregation Services Router (ASR) 903
- Cisco Aggregation Services Router (ASR) 920

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

Service	Cryptography
SSH	Key derivation, Hashing, Symmetric encryption, signature verification
SNMP	Key derivation, Hashing, Symmetric encryption
TLS	Key derivation, Hashing, Symmetric encryption, signature verification
IKE	Key derivation, Hashing, Symmetric encryption, signature verification
IPsec	Key derivation, Hashing, Symmetric encryption (non-accelerated), signature verification
OSPFv3 (when tunneled via IPsec)	Key derivation, Hashing, Symmetric encryption (non-accelerated), signature verification
NTP (when tunneled via IPsec)	Key derivation, Hashing, Symmetric encryption (non-accelerated), signature verification
BGP (when tunneled via IPsec)	Key derivation, Hashing, Symmetric encryption (non-accelerated), signature verification
Radius (when tunneled via IPsec)	Key derivation, Hashing, Symmetric encryption (non-accelerated), signature verification
Protected Passwords	Hashing

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