June 29, 2022

To Whom It May Concern

Cisco Systems, Inc performed a conformance review of the following devices (the "Product") running IOS-XE SD-WAN Release 17.6 (also known as Controller mode):

- 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 Router
- Cisco IR 1100, 1800, 8100 Series Industrial Routers

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

- Cisco IOS Common Cryptographic Module (IC2M) Rel5a (FIPS 140-2 Cert. #4222)
- FIPS Object Module (FOM) 7.0b (FIPS 140-2 Cert. #4174)

Cisco confirmed that the following features leverage the embedded cryptographic modules to provide cryptographic services:

- Security protocols – IPsec, TLS, SSH, SNMPv3
    - All cryptographic algorithms necessary to support each protocol's key derivation function
    - Session establishment
    - Hashing
    - Symmetric encryption
- Routing protocols – RADIUS, TACACS, BGP, OSPF, NTP, IS-IS
    - All cryptographic algorithms necessary to support each protocol's key derivation function
    - Session establishment
    - Hashing
    - Symmetric encryption for each routing protocol when transmitted through an IKE/IPsec tunnel

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,

Ed Paradise
SVP Engineering
Cisco S&TO

June 29, 2022

To Whom It May Concern

Cisco Systems, Inc performed a conformance review of the following devices (the "Product") running IOS-XE Release 17.6 (also known as Autonomous mode):

- 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 Router
- Cisco IR 1100, 1800, 8100 Series Industrial Routers
- Cisco ESR 6300 Series Embedded Services Routers
- Cisco CUBE
- Cisco VG400 Series Voice Gateways

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

- Cisco IOS Common Cryptographic Module (IC2M) Rel5a (FIPS 140-2 Cert. #4222)
- FIPS Object Module (FOM) 7.0b (FIPS 140-2 Cert. #4174) – for Cisco CUBE only

Cisco confirmed that the following features leverage the embedded cryptographic modules to provide cryptographic services:

- Security protocols – IPsec, TLS, SSH, SNMPv3, SRTP (CUBE Only)
    - All cryptographic algorithms necessary to support each protocol's key derivation function
    - Session establishment
    - Hashing
    - Symmetric encryption
- Routing protocols – RADIUS, TACACS, BGP, OSPF, NTP, IS-IS
    - All cryptographic algorithms necessary to support each protocol's key derivation function
    - Session establishment
    - Hashing
    - Symmetric encryption for each routing protocol when transmitted through an IKE/IPsec tunnel

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,

Edward D Paradise

Ed Paradise
SVP Engineering
Cisco S&TO