October 21, 2022

To Whom It May Concern

A conformance review of Cisco IOS-XE SDWAN Release v17.9 ("the Product") deployed on the following devices:

- Cisco C8500, C8500L Series Edge Platforms
- Cisco C8200, C8200L, C8300 Series Edge Platforms
- 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, 8300 Series Industrial Routers

was completed and found that the Product integrates the following FIPS 140-2 approved cryptographic module:

- Cisco IOS Common Cryptographic Module (IC2M) (FIPS 140-2 Cert. #4222)
- FIPS Object Module (FOM) 7.2a (FIPS 140-2 Cert. #4036) .

Cisco confirms that the embedded cryptographic module listed above provides all cryptographic services for the following:

- 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
    - 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

In keeping with the last paragraph of the Cryptographic Module Validation Program (CMVP) requirements for validated modules (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules), this signed letter serves as confirmation that the product, with the embedded cryptographic module, provides the cryptographic services listed above. The information within this letter can be verified against the CMVP validation entries found on the CMVP website:

IC2M: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4222
FOM: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4036

The CMVP has not independently reviewed this analysis, testing, or results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security

October 21, 2022

To Whom It May Concern

A conformance review of Cisco IOS-XE Release v17.9 ("the Product") deployed on the following devices:

- Cisco C8500, C8500L Series Edge Platforms
- Cisco C8200, C8200L, C8300 Series Edge Platforms
- 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, 8300 Series Industrial Routers
- Cisco ESR 6300 Series Embedded Services Routers
- Cisco VG400 Series Voice Gateways

was completed and found that the Product integrates the following FIPS 140-2 approved cryptographic module:

- Cisco IOS Common Cryptographic Module (IC2M) (FIPS 140-2 Cert. #4222)

Cisco confirms that the embedded cryptographic module listed above provides all cryptographic services for the following:

- 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

In keeping with the last paragraph of the Cryptographic Module Validation Program (CMVP) requirements for validated modules (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules), this signed letter serves as confirmation that the product, with the embedded cryptographic module, provides the cryptographic services listed above. The information within this letter can be verified against the CMVP validation entries found on the CMVP website:

IC2M: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4222

The CMVP has not independently reviewed this analysis, testing, or results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security