



August 21, 2023

To Whom It May Concern

A conformance review of Cisco IOS-XE Release v17.12 in SDWAN mode (“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 incorporates the following FIPS 140-2 validated cryptographic module:

- Cisco IOS Common Cryptographic Module (IC2M) (FIPS 140-2 Cert. #4222)  
<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4222>
- FIPS Object Module (FOM) 7.2a (FIPS 140-2 Cert. #4036)  
<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4036>

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

- Security protocols – IPsec, TLS, SSHv2, SNMPv3
- Routing protocols– RADIUS, TACACS, BGP, OSPF, NTP, IS-IS (securely routed through an IPsec tunnel)

The review/testing confirmed that:

1. The cryptographic module (mentioned above) does initialize in a manner that is compliant with its Security Policy.
2. All cryptographic algorithms used for session establishment are handled within the cryptographic module.
3. All underlying cryptographic algorithms support each service’s key derivation function.

This letter has been generated in accordance with guidance provided by the Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules>).

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

Any questions regarding these statements may be directed via e-mail to the Cisco Global Certification Team (GCT) at [certteam@cisco.com](mailto:certteam@cisco.com).

Sincerely,

Ed Paradise  
Cisco Senior Vice President  
Foundational & Government Security



August 21, 2023

To Whom It May Concern

A conformance review of Cisco IOS-XE Release v17.12 in XE mode ("the Product") deployed on the following devices:

- Cisco C8500, C8500L Series Edge Platforms
- Cisco C8300, C8200, C8200L 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 Aggregation Services Router (ASR) 920
- Cisco VG400 Series Voice Gateways
- Cisco Unified Border Element (CUBE)

was completed and found that the Product incorporates the following FIPS 140-2 validated cryptographic module:

- Cisco IOS Common Cryptographic Module (IC2M) (FIPS 140-2 Cert. #4222)  
<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4222>
- FIPS Object Module (FOM) 7.2a (FIPS 140-2 Cert. #4036 [CUBE only])  
<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4036>

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

- Security protocols – IPsec, TLS, SSHv2, SNMPv3, SRTP[CUBE]
- Routing protocols – RADIUS, TACACS, BGP, OSPF, NTP, IS-IS (securely routed through an IPsec tunnel)

This letter has been generated in accordance with guidance provided by the Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules>).

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

Any questions regarding these statements may be directed via e-mail to the Cisco Global Certification Team (GCT) at [certteam@cisco.com](mailto:certteam@cisco.com).

Sincerely,

A handwritten signature in black ink that reads "Edward D Paradise".

Ed Paradise  
Cisco Senior Vice President  
Foundational & Government Security