March 17, 2023

To Whom It May Concern

A conformance review of Cisco Cyber Vision, version 4.1 ("the Product") deployed on the following:

- Cisco IC3000 Industrial Compute Gateway
- Cisco Catalyst IE3300 Rugged Series switch
- Cisco Catalyst IE3400 Rugged Series switch
- Cisco Catalyst IE3400 Heavy Duty Series switch
- Cisco Catalyst IR1100 Rugged Series Routers
- Cisco Catalyst IR8300 Rugged Series Router
- Cisco Catalyst 9300 Series switch
- Cisco Catalyst 9400 Series switch

was completed and confirmed that the Product does incorporates the following FIPS 140-2 approved cryptographic module:

1. Cisco FIPS Object Module version 7.2a (Certificate #4036)

The review/testing confirmed that:

1. The cryptographic module (mentioned above) is built and initialized in a manner that is compliant with its Security Policy.
2. All cryptographic algorithms used in TLS v1.2 for session establishment, are handled within the Cisco FIPS Object Module, Certificate #4036
3. All underlying cryptographic algorithms supporting the TLS key derivation functions,

In keeping with CMVP (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules) requirements, last paragraph. This signed letter serves as confirmation that Cisco Cyber Vision, version 4.1 with embedded cryptographic module cert #4036 which is a validated module found on the CMVP website https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4036 and provides the cryptographic services listed above in this product. The information within this letter can be verified against the CMVP validation entry for certificate #4036.

The Cryptographic Module Validation Program (CMVP) has not independently reviewed this analysis, testing or the results.

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

Thank you,

Edward D Paradise

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security