December 20, 2022

To Whom It May Concern,

A conformance review of Cisco SD-WAN v20.9 [vManage, vBond, vSmart, vEdge] (the "Product") was completed and confirmed that the Product does incorporate the following FIPS 140-2 approved cryptographic module:

- FIPS Object Module (FOM) 7.2a (Certificate #4036)

The review/testing confirmed that:

1. The cryptographic module (mentioned above) is initialized in a manner that is compliant with its Security Policy.
2. All cryptographic algorithms used in TLS v1.2, DTLSv1.2, SSHv2 and SNMPv3 for sessions establishment, are handled within the Cisco FIPS Object Module, Certificate #4036
3. All underlying cryptographic algorithms key derivation functions supporting each services listed above

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 SD-WAN v20.9 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
SVP Engineering
Cisco S&TO