September 26, 2022

To Whom It May Concern

A conformance review of **Cisco** Application Policy Infrastructure Controller- Version 6.0, Application Centric Infrastructure (APIC-ACI) ("the Product") deployed on the following:

- Nexus 9000 APIC-ACI

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

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

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

- TLS v1.2 (HTTPS)
- TLS v1.3 (HTTPS)
- SSHv2
- SNMPv3

Users can communicate to the appliances using HTTPS and/or SSH. HTTPS is the primary protocol used, but SSH is available for those who desire/need it.

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 SNMPv3, SSHv2, TLS v1.2 and TLS v1.3 for sessions establishment, are handled within the Cisco FIPS Object Module, Certificate #4036
3. All underlying cryptographic algorithms supporting each services' key derivation functions,

Cisco Application Policy Infrastructure Controller (APIC), enters FIPS mode after the User enters "fips mode enable" command.

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 Application Policy Infrastructure Controller (APIC), version 6.0 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,

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security