February 22, 2022

To Whom It May Concern

A conformance review of Cisco Application Policy Infrastructure Controller (APIC), version 5.2.4 deployed in the following:

- Nexus 9000 APIC-ACI

was completed and found to properly incorporate the following FIPS 140-2 validated cryptographic module:

- 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)
- SSHv2
- SNMPv3

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 and TLS v1.2 for sessions establishment, are handled within the Cisco FIPS Object Module, Certificate #4036

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

Details of Cisco’s review, which consisted of build process, source code review and operational testing (both positive and negative), can be provided upon request.

The intention of this letter is to provide an assessment and assurance that the Product correctly integrates and uses the validated cryptographic module Cisco FIPS Object Module Version 7.2a, listed above within the scope of the claims indicated above. 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
VP Engineering
Cisco S&TO