April 26, 2022

To Whom It May Concern

A conformance review of Cisco Digital Network Architecture – Center (Cisco DNA-C), version 2.3.3 deployed within Ubuntu 18.04.

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

- Cisco FIPS Object Module version 7.2a (Certificate #4036)
- BC-FJA Bouncy Castle FIPS 1.0.2 Java (Certificate #3514)

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

- TLS v1.2 (HTTPS management) inbound using FOM 7.2a
- SSHv2 (management between PC and Sensor) outbound using Bouncy Castle
- SNMPv3 (Secure logging) outbound using Bouncy Castle
- TLS 1.2 (HTTPS) outbound using Bouncy Castle

The review/testing confirmed that:

1. The FIPS Object Module version 7.2a cryptographic module (referenced above) is initialized in a manner that is compliant with its security policy.
2. The BC-FJA Bouncy Castle FIPS 1.0.2 Java cryptographic module (referenced above) is initialized in a manner that is compliant with its security policy.
3. All cryptographic algorithms used in SNMPv3, SSHv2 and TLS v1.2 for sessions establishment, are handled within the BC-FJA Bouncy Castle FIPS 1.0.2 Java, Certificate #3514
4. All cryptographic algorithms used in TLS v1.2 (HTTPS Management) for sessions establishment, are handled within the Cisco FIPS Object Module, Certificate #4036

Cisco Digital Network Architecture – Center (Cisco DNA-C), enables FIPS mode at install-time using the first time configuration wizard. Once set a factory reset must be run to disable FIPS.

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 and BC-FJA Bouncy Castle FIPS 1.0.2 Java, both 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