November 28, 2023

To Whom It May Concern

An updated conformance review was conducted on what is now named Cisco Catalyst Center version 2.3 (previously named Cisco DNA Center) deployed within Ubuntu 18.04 was completed and found to properly incorporate the following FIPS 140-2 validated cryptographic modules:

- Cisco FIPS Object Module (FOM) version 7.2a (Certificate #4036)
- BC-FJA (Bouncy Castle FIPS Java API) version 1.0.2 (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 BC-FJA (Bouncy Castle FIPS Java API)
- SNMPv3 (Secure logging) outbound using BC-FJA (Bouncy Castle FIPS Java API)
- TLS 1.2 (HTTPS) outbound using BC-FJA (Bouncy Castle FIPS Java API)

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 (BC-FJA (Bouncy Castle FIPS Java API) version 1.0.2, Certificate #3514.
4. All cryptographic algorithms used in TLS v1.2 (HTTPS Management) for sessions establishment, are handled within the Cisco FIPS Object Module, version 7.2a, Certificate #4036

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 Cisco Catalyst Center version 2.3 correctly integrates and uses the validated cryptographic module Cisco FIPS Object Module (FOM) Version 7.2a and BC-FJA (Bouncy Castle FIPS Java API) version 1.0.2, both listed above within the scope of the claims indicated above and used on either a physical or virtual appliance. 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