September 23, 2022

To Whom It May Concern

Cisco Systems, Inc performed a conformance review of the following devices (the "Product") running IOS XR 7.5.2:

- Cisco ASR 9000 Aggregation Services Series Routers
- Cisco 8000 Series Routers

The Product integrates the following FIPS 140-2 approved cryptographic module:

- FIPS Object Module (FOM) version 7.2a (FIPS 140-2 Cert. #4036)

Cisco confirmed that the following features leverage the embedded cryptographic modules to provide cryptographic services:

1. Session establishment supporting the following service:
   - SSHv2

2. All underlying cryptographic algorithms supporting the following service key derivation function:
   - SSHv2

3. Hashing for the following services:
   - SSHv2
   - SNMPv3

4. Asymmetric key based encryption/authentication for the following services:
   - SSHv2
   - RSA Key Generation

5. Symmetric encryption/decryption for the following services:
   - SSHv2
   - SNMPv3

Details of Cisco's review, which consisted of source code review and operational testing, are available 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 within the scope of the claims indicated above. The Cryptographic Module Validation Program (CMVP) has not independently reviewed this analysis, testing, or the results.

Direct questions regarding these statements to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Ed Paradise
SVP Engineering
Cisco S&TO