May 6, 2022

To Whom It May Concern

A conformance review of Cisco Istio Service Mesh version 1.12 running on Ubuntu was completed and found to properly incorporate the following FIPS 140-2 validated cryptographic module:

- BoringCrypto version ae223d6138807a13006342edfeef32e813246b39 (Cert # 3678)

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

- TLS v1.2 (HTTPS) (Management).

Users communicate to appliances using HTTPS

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 TLS v1.2 for sessions establishment, are handled within the BoringCrypto Module, Certificate #3678

Cisco Istio Service Mesh enters FIPS mode at build time through crypto/tls/fipsonly

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 modules 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
SVP Engineering
Cisco S&TO