July 29, 2024

To Whom It May Concern,

A compliance review of Emergency Responder (CER) version 15 ("the Product") was completed and found that the Product integrates the following FIPS 140 approved cryptographic module:

1. Cisco FIPS Object Module 7.2a (FIPS 140-2 Cert. #4036
2. BC-FJA (Bouncy Castle FIPS Java API), cert #3514
3. Ubuntu 20.04 Strongswan Cryptographic Module, cert #4046
4. Linux Kernel FIPS Object Module (KFOM) Cryptographic Module, cert #4744

Cisco confirms that the cryptographic module listed above provides cryptographic services for the following as applicable:

- Certificate Management for Self-Signed Certificate (#4036)
- TLS for HTTPs (via Tomcat), Tomcat-based web applications, SOAP AXL interface, TLS for Disaster Recovery System (DRS), Certificate Management (CA Signing), SSH (#3514)
- IKEv1 #4046
- IPSec Control plane (#4744)

The review/testing confirmed that:

1. The cryptographic module (mentioned above) does initialize in a manner that is compliant with its Security Policy.
2. All applicable cryptographic algorithms used for session establishment are handled within the cryptographic module.
3. All applicable underlying cryptographic algorithms support each service's key derivation function.

This letter has been generated in accordance with guidance provided by the Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules). In general, a letter will not be generated for subsequent software releases unless a change has been made to the cryptographic module(s) noted in this letter.

The CMVP has not independently reviewed this analysis, testing or the results.

Any questions regarding these statements may be directed via e-mail to the Cisco Global Certification Team (GCT) at certteam@cisco.com.

Sincerely,

Edward D Paradise

Ed Paradise,
SVP Engineering S&TO