CISCO

May 5, 2023

To Whom It May Concern:

A conformance review of Cisco Email Security Appliance (ESA) running AsyncOS v15.0 ("the Product") deployed in the following platforms:

- ESA hardware models: C190, C195, C390, C395, C690, C690X, C695, C695F
- ESA virtual models: C100v, C300v, C600v hosted on UCS C-series servers running ESXi 6.7 or 7.0

was completed and found that the Product incorporates the following FIPS 140-2 validated cryptographic module:

- Cisco FIPS Object Module version 7.2a (Certificate #4036)
  https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4036

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

- TLS v1.2
- SSHv2
- SCP

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 cryptographic algorithms used for session establishment are handled within the cryptographic module.
3. All 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).

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,

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security