leidos

May 19th, 2014

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

To Whom It May Concern:

Leidos completed its conformance review of the Cisco Systems, Inc.'s Cisco Telepresence TC7.1.3 (the "Product") on April 22, 2014 and May 14, 2014; has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic module:

1. Cisco FIPS Object Module (FIPS 140-2 Cert. #2100)
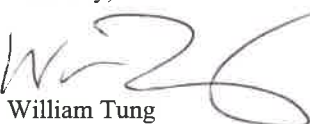
Specifically, Leidos' review confirmed that:

1. The integrated cryptographic module (mentioned above) is initialized in a manner that is compliant with its individual security policy.

2. All cryptographic algorithms used for TLS used in HTTPS and SIP for session establishment, traffic encryption and traffic authentication are offloaded to Cisco FIPS Object Module (FIPS 140-2 Cert. #2100). The product is able to load certificates that have a key size less than 2048 bits, however this is not allowed while the product is operating in compliance with FIPS mode.

3. All cryptographic algorithms used for SSHv2 for session establishment, traffic encryption and traffic authentication are offloaded to Cisco FIPS Object Module (FIPS 140-2 Cert. #2100).

4. All cryptographic algorithms used for H.325 Media Stream Security for traffic encryption are offloaded to Cisco FIPS Object Module (FIPS 140-2 Cert. #2100). The product also supports the use of 1024-bit Diffie-Hellman, however any key sizes less than 2048 bits shall not be used with the product in a FIPS conformant manner.

5. All cryptographic algorithms used for sRTP for session establishment, traffic encryption and traffic authentication are offloaded to Cisco FIPS Object Module (FIPS 140-2 Cert. #2100).

6. The Product will not operate if either of the integrated modules (mentioned above) is missing or altered.

Details of Leidos' review, which consisted of source code review and operational testing, are obtainable by special request.

Please note that for this review, Leidos only examined the Product features referenced above and while the Product may contain other features or functionality, Leidos did not examine these during its review and makes no claims or representations regarding them. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed Leidos' analysis, testing, or results.

The intention of this letter is to provide independent opinion that the Product correctly integrates and uses validated cryptographic modules within the scope of claims indicated above. Leidos offers no warranties or guarantees with respect to the above described compliance review. This letter does not imply a Leidos certification or product endorsement.
Please let us know if you have any questions.

Sincerely,

William Tung
Laboratory Manager

Leidos