leidos

July 22, 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 Unified Communications Manager 10.5.1 with Prime License Manager (the "Product") on July 8, 2014; has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1. Cisco FIPS Object Module v4.1 (FIPS 140-2 Cert. #2100)
2. RSA BSAFE Crypto-J JSAFE and JCE Software Module v5.0.1 (FIPS 140-2 Cert. #1502)
3. Red Hat Enterprise Linux 6.2 Openswan Cryptographic Module v2.0 (FIPS 140-2 Cert. #1859)
4. Red Hat Enterprise Linux 6.2 OpenSSH Server Cryptographic Module v2.1 (FIPS 140-2 Cert. #1792)

Specifically, Leidos' review confirmed that:

1. The integrated cryptographic modules (mentioned above) are initialized in a manner that is compliant with their individual security policies.

2. All cryptographic algorithms used for TLS used in Call Processing (ccm, cti manager), CA Service (CAPF), Certificate Trust List (CTL) Provider and Trust Verification Services (TVS) are offloaded to Cisco FIPS Object Module (FIPS 140-2 Cert. #2100).

3. All cryptographic algorithms used for Certificate Generation for CA Service (CAPF) are offloaded to Cisco FIPS Object Module (FIPS 140-2 Cert. #2100).

4. All cryptographic algorithms used for Cisco TFTP Data Protection (encryption and authentication) are offloaded to Cisco FIPS Object Module (FIPS 140-2 Cert. #2100).

5. All cryptographic algorithms used for COP File Authentication (digital signature verification) are offloaded to Cisco FIPS Object Module (FIPS 140-2 Cert. #2100).

6. All cryptographic algorithms used for TLS for HTTPs (via Tomcat), Disaster Recovery System (DRS), PLM Agent Interaction Client and PLM Swift Interaction Client are offloaded to RSA BSAFE Crypto-J JSAFE and JCE Software Module v5.0.1 (FIPS 140-2 Cert. #1502).

7. All cryptographic algorithms used for Tomcat based web application (LDAPS, SOAP AXL interface) are offloaded to RSA BSAFE Crypto-J JSAFE and JCE Software Module v5.0.1 (FIPS 140-2 Cert. #1502).

8. All cryptographic algorithms used for certificate management are offloaded to RSA BSAFE Crypto-J JSAFE and JCE Software Module v5.0.1 (FIPS 140-2 Cert. #1502).

9. All cryptographic algorithms used for J2SSH are offloaded to RSA BSAFE Crypto-J JSAFE and JCE Software Module v5.0.1 (FIPS 140-2 Cert. #1502).

10. All cryptographic algorithms used for IPSec are offloaded to Red Hat Enterprise Linux 6.2 Openswan Cryptographic Module v2.0 (FIPS 140-2 Cert. #1859).

11. All cryptographic algorithms used for SSH are offloaded to Red Hat Enterprise Linux 6.2 OpenSSH Server Cryptographic Module v2.1 (FIPS 140-2 Cert. #1792).

Leidos

6841 Benjamin Franklin Drive | Columbia, MD 21046 | tel: 443.367.7822 | fax: 443.367.7970 | leidos.com

12. The Product will not operate if any of the integrated modules (mentioned above) are missing or altered.

It is important to note that several of the above services support algorithms/key lengths that are no longer allowed by NIST Special Publication 800-131A. Using these non-approved key lengths will result in nonconformance to FIPS.

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