March 26, 2021

To Whom It May Concern

A conformance review of Cisco Unified Communications Manager (CUCM) and Unified Communications Manager Session Management Edition (SME) version 14 ("the Product") was completed and found that the Product integrates the following FIPS 140-2 approved cryptographic modules:

1. Cisco FIPS Object Module (version 6.2), cert #2984
2. Cisco CentOS Libreswan Cryptographic Module cert #3534

Cisco confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for ***Call processing, CA services, HTTPs, CTLs, SSH, CiscoJ (LDAP over SSL, SOAP AXL, Disaster Recovery, Certificate Management) (#2984), IKE/IPsec Key Derivation (#3534) :***

1. Session establishment supporting each service,
2. All underlying cryptographic algorithms supporting each services' key derivation functions,
3. Hashing for each service,
4. Symmetric encryption for each service.

Details of Cisco's review, which consisted of source code review and operational testing, 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 module 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
VP Engineering
Cisco S&TO