April 28, 2020

To Whom It May Concern

A conformance review of Cisco TelePresence Collaboration Endpoint Software CE9.12 ("the Product") was completed and found that the Product integrates the following FIPS 140-2 approved cryptographic modules:

1. Cisco FIPS Object Module (FIPS 140-2 Cert. #3341)
2. Cisco FIPS Object Module (FIPS 140-2 Cert. #2984)

The Software is known to run on the following platforms:

Cisco TelePresence MX200 G2
Cisco TelePresence MX300 G2
Cisco TelePresence MX700
Cisco TelePresence MX800
Cisco TelePresence MX800 Dual
Cisco TelePresence SX10 Quick Set
Cisco TelePresence SX20 Quick Set
Cisco TelePresence SX80 Codec
Cisco Webex Board 55
Cisco Webex Board 55S
Cisco Webex Board 70
Cisco Webex Board 70S
Cisco Webex Board 85S
Cisco Webex Desk Pro
Cisco Webex Desk Pro NR
Cisco Webex DX70
Cisco Webex DX70 NR
Cisco Webex DX80
Cisco Webex DX80 NR
Cisco Webex Room 55 Dual
Cisco Webex Room 55 Dual NR
Cisco Webex Room 55 Single
Cisco Webex Room 55 Single NR
Cisco Webex Room 70 Dual
Cisco Webex Room 70 Dual NR
Cisco Webex Room 70 G2 Dual
Cisco Webex Room 70 G2 Dual NR
Cisco Webex Room 70 G2 Single
Cisco Webex Room 70 G2 Single NR
Cisco Webex Room 70 Single
Cisco Webex Room 70 Single NR
Cisco Webex Room Kit
Cisco Webex Room Kit Mini
Cisco Webex Room Kit Mini NR
Cisco Webex Room Kit NR
Cisco Webex Room Kit Plus
Cisco Webex Room Kit Plus NR
Cisco Webex Room Kit Pro
Cisco Webex Room Kit Pro NR
Cisco Webex Room USB

Cisco confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for ***TLS***, ***SSHv2, H.323*** and ***sRTP (#3341) and 802.1x (WiFi, Authentication, and encryption)(#2984)***:

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