Cisco Systems, Inc.
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park
NC 27709
Phone: 919 392-2000
http://www.cisco.com

29, May 2014

To Whom It May Concern

Cisco completed its conformance review of Cisco Systems Inc.'s Cisco TelePresence Video Communication Server (VCS) software version 8.1.1 on May 29, 2014, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1. Cisco FIPS Object Module (FOM) (FIPS 140-2 Cert. #2034)

Specifically, Cisco's review confirmed that:

1. The integrated cryptographic module (mentioned above) is initialized in a manner that is compliant with its individual security policy. Note: the cryptographic module supports pre-SP 800-131a key strengths (less than 112 bits). In order to operate in an approved mode of operation, applications must only use cryptographic services with key strengths of 112 bits or greater
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 (FOM) (FIPS 140-2 Cert. #2034)
3. All cryptographic algorithms used for SSHv2 for session establishment, traffic encryption, and traffic authentication are offloaded to Cisco FIPS Object Module (FOM) (FIPS 140-2 Cert. #2034)
4. All cryptographic algorithms used for H.323 Media Stream Security for traffic encryption are offloaded to Cisco FIPS Object Module (FOM) (FIPS 140-2 Cert. #2034)
5. All cryptographic algorithms used for sRTP for session establishment, traffic encryption, and traffic authentication are offloaded to Cisco FIPS Object Module (FOM) (FIPS 140-2 Cert. #2034)
6. All cryptographic algorithms used for SNMPv3 for privacy and authentication are offloaded to Cisco FIPS Object Module (FOM) (FIPS 140-2 Cert. #2034)
7. OpenSSL CVE-2014-0160.patch was applied and as a result, the product is not susceptible to the Heartbleed Vulnerability.
8. The product will not operate if the integrated module (listed above) is missing or altered.

Details of Cisco's review, which consisted of source code review and operational testing, can be provided upon request.

Moreover, the FIPS conformance claims made for Cisco TelePresence Video Communication Server (VCS) software version 8.1, verified by Leidos, hold true for Cisco TelePresence Video Communication Server (VCS) software version 8.1.1 with no additions or removal of cryptographic services or cryptographic implementations.

The intention of this letter is to provide our assessment that the Product correctly integrates and uses validated cryptographic modules within the scope of the claims indicated above. Cisco offers no warranties or guarantees with respect to the above described conformance review. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed Cisco's analysis, testing or results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Ed Paradise
VP Engineering
Cisco TRIAD