December 19, 2023

To Whom It May Concern

A compliance review of Cisco Unified Communications Manager (CUCM) and Unified Communications Manager Session Management Edition (SME) version 15 ("the Product") was completed and found that the Product incorporates the following FIPS 140 compliant cryptographic module:

- CiscoSSL FIPS Object Module (version 7.2a), cert #4036
- BC-FJA (Bouncy Castle FIPS Java API), cert #3514
- Ubuntu 20.04 Strongswan Cryptographic Module, cert #4046
- Linux Kernel FIPS Object Module (KFOM) Cryptographic Module, cert #TBD ('in Coordination' as of 3/17/2023) https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List

Cisco confirms that the cryptographic module listed above provides cryptographic services for the following:

- Call processing, CA services, HTTPs, SSH, IKE, IPSec (#4036)
- LDAP over SSL, SOAP AXL, Disaster Recovery, Certificate Management (#3514)
- IKEv1 #4046
- IPSec Control plane (#TBD)

The review/testing confirmed that:

1. The cryptographic module (mentioned above) does initialize in a manner that is compliant with its Security Policy.
2. All cryptographic algorithms used for session establishment are handled within the cryptographic module.
3. All underlying cryptographic algorithms support each service's key derivation function.

This letter has been generated, with caveats, in accordance with guidance provided by the Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules). A letter will not be generated for subsequent software releases unless a change has been made to the cryptographic module(s) noted in this letter.

Due to known delays with the CMVP review process, this temporary letter will serve in the interim between completed laboratory evaluation and formal review finalization (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-flow). A temporary letter will be released after a submission has been at the 'Review Pending' or later milestone for more than thirty days. Upon formal review finalization and certificate posting, this temporary letter will be replaced with a standard compliance review letter.

The 'Review Pending' and later milestones mean that NIST has received both a complete set of testing documents and a signed recommendation letter for validation from an accredited laboratory, however, CMVP review has not completed (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process).

This letter is also intended to act as an authorization package artifact that can augment a Plan of Action and Milestones (POA&M) similar to guidance provided by the FedRAMP Program Management Office (PMO) (https://www.fedramp.gov/blog/2022-12-22-crypto-modules-historical-status/). It is expected that this POA&M

would be used to facilitate tracking of the module's formal listing and subsequent updating of an authorization package.

The CMVP has not independently reviewed this analysis, testing, or the results.

Any questions regarding these statements may be directed via e-mail to the Cisco Global Certification Team (GCT) at certteam@cisco.com.

Sincerely,

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security