December 23, 2024

To Whom It May Concern

A compliance review of Cisco customized Linux OS Release v4.1.6 ("the Product") deployed in the following platforms:

- Catalyst 1200 Series Switches
- Catalyst 1300 Series Switches

was completed and found that the Product incorporates the following FIPS 140-2 validated cryptographic module:

- OpenSSL FIPS Provider v3.0.9 (FIPS 140-2 Cert. #4282)

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

- TLSv1.2 and TLSv1.3
- SSHv2
- SNMPv3

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 applicable cryptographic algorithms used for session establishment are handled within the cryptographic module.
3. All applicable underlying cryptographic algorithms support each service's key derivation function.

This letter has been generated in accordance with guidance provided by the Cryptographic Module Validation Program (CMVP). The CMVP has not independently reviewed this analysis, testing or the results.

In general, 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.

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