August 15, 2024

To Whom It May Concern

A compliance review of Cisco Catalyst 9100, Wave 2, and IoT Series Access Points with software version 17.15 ("the Product") deployed in the following platforms:

1. C9115AXI/AXE Wireless LAN Access Points
2. C9120AXI/AXE/AXP Wireless LAN Access Points
3. C9130AXI/AXE Wireless LAN Access Points
4. C9105AXI/AXW Wireless LAN Access Points
5. C9124AXI/AXE/AXD Wireless LAN Access Points
6. C9136I Wireless LAN Access Points
7. CW9162I Wireless LAN Access Point
8. CW9164I Wireless LAN Access Point
9. CW9166I/D1 Wireless LAN Access Points
10. CW9163E Wireless LAN Access Point
11. Cisco Aironet 1562E/I/D/P Wireless LAN Access Points
12. Cisco Aironet 2802E/I Wireless LAN Access Points
13. Cisco Aironet 3802E/I/P Wireless LAN Access Points
14. Cisco Aironet 4800 Wireless LAN Access Point
15. Cisco Aironet IW6300H-AC/DC/DCW Wireless LAN Access Points
16. Cisco Aironet ESW6300 Wireless LAN Access Points
17. Cisco Catalyst IW9167IH/EH Wireless LAN Access Points
18. Cisco Catalyst IW9165E/DH Wireless LAN Access Points

was completed and found that the Product incorporates the following FIPS 140-3 compliant cryptographic module:

- Cisco FIPS Object Module version 7.3a (Certificate #4747)
  https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4747

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

- DTLS
- SSHv2
- WPA2/WPA3

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). 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.

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,

Edward D Paradise

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security