March 6, 2024

To Whom It May Concern

A compliance review of Cisco Catalyst 9100, Wave 2, and IoT Series Access Points with software version 17.12 ("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 Point
10. Cisco Aironet 1562E/I/D/P Wireless LAN Access Points
11. Cisco Aironet 2802E/I Wireless LAN Access Points
12. Cisco Aironet 3802E/I/P Wireless LAN Access Points
13. Cisco Aironet 4800 Wireless LAN Access Point
14. Cisco Aironet IW6300H-AC/DC/DCW Wireless LAN Access Points
15. Cisco Aironet ESW6300 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 ('Review Pending' as of 8/30/2022) 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:

- 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.

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,

Edward D Paradise

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security