National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

for

Apple macOS 15 Sequoia

Report Number:	CCEVS-VR-VID11648-2026
Dated:	February 20, 2026
Version:	1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Sheldon Durrant

Randy Heimann

Lisa Mitchell

Jaemond Reyes

Lori Sarem

The MITRE Corporation (FFRDC)

Common Criteria Testing Laboratory

Joachim Vandersmissen

James Reid

Parker Collier

Walker Riley

atsec information security corporation

Austin, TX

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Apple macOS 15 Sequoia (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government, and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target ([ST]), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the validator comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by atsec Common Criteria Testing Laboratory (CCTL) in Austin, TX, USA, and was completed in February 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by atsec. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the *Protection Profiles* and *Functional Packages* identified in Table 1.

2 Identification

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The *PPs/PP-Modules/Packages* to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Validation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple macOS 15 Sequoia
Security Target	Apple macOS 15 Sequoia Security Target, Version 1.2, 2026-02-10

Sponsor & Developer	Apple Inc.
Completion Date	February 20, 2026
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017

PP	• PP-Configuration for General Purpose Operating System, Bluetooth, and Wireless Local Area Network Clients, Version 1.0 (CFG_GPOS_BT_WLANC_V1.0).
	  ○ Base-PP: Protection Profile for General Purpose Operating Systems, Version 4.3 (PP_OS_V4.3);
	  ○ PP-Module: PP-Module for Bluetooth, Version 1.0 (MOD_BT_V1.0); and
	  ○ PP-Module: PP-Module for WLAN Clients, Version 1.0 (MOD_WLANC_V1.0).
	• Functional Package for Transport Layer Security (TLS), Version 1.1 (PKG_TLS_V1.1)

Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
CCTL	atsec information security corporation 4516 Seton Center Parkway Suite 250 Austin, TX 78759
Validation Personnel	Sheldon Durrant, Randy Heimann, Lisa Mitchell, Jaemond Reyes, Lori Sarem
Evaluation Personnel	Joachim Vandersmissen, James Reid, Parker Collier, Walker Riley

3 TOE Architecture

The Target of Evaluation (TOE) is Apple macOS 15 Sequoia, which is a general purpose operating system running on the Apple Mac computers with Apple silicon and providing wireless LAN and Bluetooth functionality.

The TOE is a Unix-based operating system built on top of the XNU kernel. The TOE implements standard Unix facilities, provides both command-line and graphical user interfaces, supports Bluetooth communication, and includes Wireless Local Area Network (WLAN) client functionality. A portion of the Bluetooth and WLAN functionalities is implemented in hardware (Broadcom chip).

The Mac computers covered in this evaluation contain the Secure Enclave, a dedicated secure subsystem integrated into the Apple silicon. Utilizing a dedicated processor (Secure Enclave Processor or SEP), the Secure Enclave is isolated from the main processor to provide an extra layer of security designed to keep sensitive data secure. The SEP executes the SEP Operating System (sepOS), which is based on a customized version of the L4 microkernel. The sepOS is included with macOS and is within the TOE boundary. The Secure Enclave supports the TOE for secure boot, and the generation of secure random data used in cryptographic key generation.

The executing TOE is divided into user space and kernel space. User space contains processes that execute in their own protected memory space and access services provided by the kernel. Kernel space contains the macOS kernel

(including device drivers and kernel extensions) that also executes in its own protected memory space. The kernel enforces process separation, provides processes with controlled access to hardware devices, and implements many other OS features.

3.1 Physical Boundaries

The physical boundary of the TOE is the installation image which includes both macOS and sepOS.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration and any excluded functionality is provided in Section 8.

4 Environmental Strengths

The TOE provides the following security functions as described in the ST.

4.1 Security Audit

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified by the conformance claims defined by the PPs. Audit events are generated for the following audit functions:

- Authentication events (Success/Failure)
- Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes)
- Privilege or role escalation events (Success/Failure)
- Administrator or root-level access events (Success/Failure)

Each audit record contains the date and time of the event, type of event, subject identity (if applicable), and outcome (success or failure) of the event.

4.2 Cryptographic Support

The TOE includes the Apple corecrypto v18.3 cryptographic libraries and is supported by the onboard Apple Secure Enclave hardware for performing user space, kernel space, and Secure Enclave cryptographic operations. In addition, it uses software and hardware noise sources for entropy generation.

The TOE implements Transport Layer Security version 1.2 (TLS 1.2) for secure communications with remote servers. The Bluetooth hardware implements the AES-CCM-128 cryptographic functionality used when connecting to remote Bluetooth devices. The TOE implements Wi-Fi Protected Access (WPA2 and WPA3) to secure 802.11 wireless traffic protected using AES-CCMP-256 and AES-GCMP-256 cryptographic algorithms.

4.3 User Data Protection

The TOE implements access controls that prevent unprivileged users from accessing files and directories owned by other users.

4.4 Identification and Authentication

All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports:

- password-based authentication,
- authentication based on username and a PIN that releases the asymmetric key stored in OE-protected storage.

The TOE will deny further user authentication once a defined number of unsuccessful authentication attempts have been reached.

For Bluetooth, the TOE supports Secure Simple Pairing (SSP). It requires user authorization and mutual authentication during pairing. It also discards pairing attempts and session initialization from Bluetooth devices to which an active session already exists. The TOE requires explicit user authorization when pairing with an untrusted device.

External entities connecting to the TOE via a secure protocol (e.g., TLS, Extensible Authentication Protocol TLS (EAP-TLS)) can be authenticated using X.509 certificates.

4.5 Security Management

The TOE can perform management functions. The administrator has full access to carry out all management functions, whereas the user has limited privileges.

4.6 Protection of the TSF

The TOE implements the following protection of TOE Security Functionality:

- Access controls for critical components.
- Address space layout randomization (ASLR) with 16 bits of entropy.
- Stack buffer overflow protection.
- Verification of integrity of the bootchain and operating system executable code.
- Trusted software updates using digital signatures.

4.7 TOE Access

Before establishing a user session, the TOE can display an advisory warning message regarding unauthorized use of the OS. Access to the TOE via a wireless network is controlled by administrator defined policy.

4.8 Trusted Path/Channel

The TOE supports TLS 1.2 for trusted channel communications. The TOE uses TLS to securely communicate with the Apple Update Server. Applications may invoke the TOE-provided TLS to securely communicate with remote servers. The TOE enforces encryption when transmitting data over Bluetooth and terminates the connection if the connected device stops encrypting. The TOE uses EAP-TLS for authentication and WPA for data encryption when connecting to a wireless access point as the WLAN client.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the *PPs, PP-Modules,* and *Packages* to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed *PPs, PP-Modules,* and *Packages*, as listed in Table 1.

5.2 Clarification of Scope

As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified by the *PPs*, *PP-Modules*, and *Packages* specified in Table 1. Other functionality included in the product was not assessed as part of this evaluation. All other functionality

provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in *Apple macOS 15 Sequoia Security Target*, Version 1.2, 2026-02-10 ([ST]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor provides guidance documents describing the installation process for Apple macOS 15 Sequoia, as well as guidance for subsequent administration and use of the applicable security features.

The following guidance documentation was examined during the evaluation:

- *Apple macOS 15 Sequoia Common Criteria Guide*, Version 1.1, 2026-02-10

To use the TOE in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above. Consumers are encouraged to download this documentation from the NIAP website. Only the guidance documentation listed above, and the specified sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of the TOE in its evaluated configuration. Any other documentation (e.g., published on the vendor's website) was not covered by the evaluation and should not be relied upon to configure or operate the TOE as evaluated.

7 IT Product Testing

Test plan, procedures, and evidence are documented in the proprietary *Detailed Test Report Apple macOS 15 Sequoia v1.1*, 2026-02-17 ([DTR]). A non-proprietary description of the tests performed, and their results is provided in the *Assurance Activity Report Apple macOS 15 Sequoia* Assurance Activity Report ([AAR]).

The purpose of the testing activity is to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the *PPs*, *PP-Modules*, and *Packages* listed in Table 1.

7.1 Developer Testing

No evidence of developer testing is required by the assurance activities for this TOE.

7.2 Evaluation Team Testing

The evaluation team established a test configuration comprising Apple macOS 15 Sequoia running on Apple devices listed in Section 8.1 of this document. Section 2.3.4 of the Assurance Activity Report ([AAR]) provides a detailed description of the test configuration the CCTL used to test the TOE, including a description of the test environment and a list of tools used.

The evaluation team devised a Test Plan based on the Test Activities specified in the above *PP* and *Functional Package*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the atsec CCTL facility in Austin, TX, between July 2025 and February 2026.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements were fulfilled.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of the following hardware and software when configured in accordance with the documentation specified in Section 6:

Table 2: Hardware Platforms

Marketing Name	Model	Model Identifier	Processor (Micro Architecture)	Security Chip	BT Version (BT/Wi-Fi Chip)
2025					
MacBook Air (15-inch, M4, 2025)	A3241	Mac16,13	M4 (ARMv9.2-A)	SEP v2.0	5.3 (4388)
MacBook Air (13-inch, M4, 2025)	A3240	Mac16,12	M4 (ARMv9.2-A)	SEP v2.0	5.3 (4388)
Mac Studio (2025)	A3143	Mac16,9	M4 Max (ARMv9.2-A)	SEP v2.0	5.3 (4388)
2024					
MacBook Pro (14-inch, 2024)	A3401	Mac16,8	M4 Pro (ARMv9.2-A)	SEP v2.0	5.3 (4388)
	A3185	Mac16,6	M4 Max (ARMv9.2-A)	SEP v2.0	5.3 (4388)
	A3112	Mac16,1	M4 (ARMv9.2-A)	SEP v2.0	5.3 (4388)
MacBook Pro (16-inch, 2024)	A3403	Mac16,7	M4 Pro (ARMv9.2-A)	SEP v2.0	5.3 (4388)
	A3186	Mac16,5	M4 Max (ARMv9.2-A)	SEP v2.0	5.3 (4388)
iMac (24-inch, 2024, Four ports)	A3137	Mac16,3	M4 (ARMv9.2-A)	SEP v2.0	5.3 (4388)
	A3247	Mac16,2	M4 (ARMv9.2-A)	SEP v2.0	5.3 (4388)
Mac mini (2024)	A3239	Mac16,11	M4 Pro (ARMv9.2-A)	SEP v2.0	5.3 (4388)
	A3238	Mac16,10	M4 (ARMv9.2-A)	SEP v2.0	5.3 (4388)

MacBook Air (15-inch, M3, 2024)	A3114	Mac15,13	M3 (ARMv8.6-A)	SEP v2.0	5.3 (4388)
MacBook Air (13-inch, M3, 2024)	A3113	Mac15,12	M3 (ARMv8.6-A)	SEP v2.0	5.3 (4388)
2023					
MacBook Pro (14-inch, Nov 2023)	A2992	Mac15,10	M3 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac15,8	M3 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac15,6	M3 Pro (ARMv8.6-A)	SEP v2.0	5.3 (4388)
	A2918	Mac15,3	M3 (ARMv8.6-A)	SEP v2.0	5.3 (4388)
MacBook Pro (16-inch, Nov 2023)	A2991	Mac15,11	M3 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac15,9	M3 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac15,7	M3 Pro (ARMv8.6-A)	SEP v2.0	5.3 (4388)
iMac (24-inch, 2023)	A2873	Mac15,5	M3 (ARMv8.6-A)	SEP v2.0	5.3 (4388)
	A2874	Mac15,4	M3 (ARMv8.6-A)	SEP v2.0	5.3 (4388)
Mac Pro (-/Rack 2023)	A2786	Mac14,8	M2 Ultra (ARMv8.6-A)	SEP v2.0	5.3 (4388)
MacBook Air (15-inch, 2023)	A2941	Mac14,15	M2 (ARMv8.6-A)	SEP v2.0	5.3 (4387)
Mac Studio (2023)	A2901	Mac14,14	M2 Ultra (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac14,13	M2 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
MacBook Pro (16-inch, 2023)	A2780	Mac14,6	M2 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac14,10	M2 Pro (ARMv8.6-A)	SEP v2.0	5.3 (4388)
MacBook Pro (14-inch, 2023)	A2779	Mac14,5	M2 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac14,9	M2 Pro (ARMv8.6-A)	SEP v2.0	5.3 (4388)
Mac mini (M2 Pro, 2023)	A2816	Mac14,12	M2 Pro (ARMv8.6-A)	SEP v2.0	5.3 (4388)
Mac mini (M2, 2023)	A2686	Mac14,3	M2 (ARMv8.6-A)	SEP v2.0	5.3 (4388)
2022					
MacBook Pro (13-inch, M2, 2022)	A2338	Mac14,7	M2 (ARMv8.6-A)	SEP v2.0	5.0 (4378)
MacBook Air (M2, 2022)	A2681	Mac14,2	M2 (ARMv8.6-A)	SEP v2.0	5.3 (4387)
Mac Studio (2022)	A2615	Mac13,2	M1 Ultra (ARMv8.5-A)	SEP v2.0	5.0 (4387)

		Mac13,1	M1 Max (ARMv8.5-A)	SEP v2.0	5.0 (4387)
2021					
MacBook Pro (16-inch, 2021)	A2485	MacBookPro 18,2	M1 Max (ARMv8.5-A)	SEP v2.0	5.0 (4387)
		MacBookPro 18,1	M1 Pro (ARMv8.5-A)	SEP v2.0	5.0 (4387)
MacBook Pro (14-inch, 2021)	A2442	MacBookPro 18,4	M1 Max (ARMv8.5-A)	SEP v2.0	5.0 (4387)
		MacBookPro 18,3	M1 Pro (ARMv8.5-A)	SEP v2.0	5.0 (4387)
iMac (24-inch, M1, 2021)	A2438	iMac21,1	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)
	A2439	iMac21,2	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)
2020					
Mac mini (M1, 2020)	A2348	Macmini9,1	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)
MacBook Air (M1, 2020)	A2337	MacBookAir 10,1	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)
MacBook Pro (13-inch, M1, 2020)	A2338	MacBookPro 17,1	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)

8.2 Excluded Functionality

The following functionality is specifically excluded from the evaluated configuration.

- Protection of traffic using a VPN
- Siri
- Any cryptographic functions and protocol versions outside the scope of the claimed Protection Profiles and Modules.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Apple macOS 15 Sequoia ([*ETR*]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([CCPART1], [CCPART2], [CCPART3]) and CEM version 3.1, revision 5 ([CEM]), and the specific evaluation activities specified in the *PPs*, *PP-Modules*, and *Packages* listed in Table 1

The evaluation determined the TOE satisfies the conformance claims made in the Apple macOS 15 Sequoia Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the *PPs*, *PP-Modules*, and *Packages* listed in Table 1.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification were provided to confirm that the evaluation was conducted in accordance with requirements, and that the conclusions reached by the evaluation team were justified.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and each CEM work unit from ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, and ASE_TSS.1. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed *PPs*, *PP-Modules*, and *Packages*, and security function descriptions that satisfy the requirements.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development Activities (ADV)

The evaluation team performed each ADV assurance activity and applied each CEM work unit from ADV_FSP.1. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed *PPs, PP-Modules*, and *Packages* for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Activities (AGD)

The evaluation team performed each AGD assurance activity and applied each CEM work unit from AGD_OPE.1 and AGD_PRE.1. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each CEM work unit from ALC_CMC.1, ALC_CMS.1, and ALC_TSU_EXT.1 to the extent possible given the evaluation evidence required by the claimed *PPs*, *PP-Modules*, and *Packages.* The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activities (ATE)

The evaluation team performed each ATE assurance activity and applied each CEM work unit from ATE_IND.1. The evaluation team ran the set of tests specified by the claimed *PPs*, *PP-Modules*, and *Packages* and recorded the results in the [DTR], summarized in section 2.3.4 of the [AAR].

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Evaluation of the Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each CEM work unit from AVA_VAN.1. The evaluation team performed a vulnerability analysis following the processes described in the claimed *PPs*, *PP-Modules*, and *Packages*. This is comprised of a search of public vulnerability databases to ensure there are no publicly known and exploitable vulnerabilities in the TOE. The vulnerability search was repeated throughout the evaluation process. The most recent searches (2026-02-17) did not identify any crucial vulnerabilities that were not addressed prior to product placement on the NIAP PCL.

The evaluation team performed a public search against the following sources:

- MITRE Common Vulnerabilities and Exposures (CVE) List: https://cve.mitre.org/cve/
- National Vulnerability Database (NVD): https://nvd.nist.gov/
- CISA Known Exploited Vulnerabilities (KEV) Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Apple security releases: https://support.apple.com/en-us/100100
- curl vulnerabilities: https://curl.se/docs/security.html

The following search terms were used during the vulnerability search:

- macOS 15
- XNU
- curl
- libarchive
- libexpat
- libxml2
- libxslt
- WebKit
- Safari
- Apple Mail
- AirDrop
- AirPlay
- Secure Enclave Processor
- BCM4388
- BCM4387
- BCM4378
- Corecrypto
- IEEE 802.11
- EAP-TLS
- TLS
- Bluetooth

The conclusion drawn from the vulnerability analysis is that no crucial residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed *PP*. Furthermore, the evaluation team's testing demonstrates the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Apple macOS 15 Sequoia Common Criteria Guide*, Version 1.0, 2025-12-19. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled or otherwise not utilized when the TOE is in the evaluated configuration.

Evaluation activities are strictly bound by the assurance activities described in the PP_OS_V4.3, MOD_BT_V1.0, MOD_WLANC_V1.0, and PKG_TLS_V1,1 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Security Target

The ST for this product's evaluation is Apple macOS 15 Sequoia Security Target, Version 1.2, 2026-02-10 ([ST]).

A Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

B Bibliography

The validation team used the following documents to produce this VR:

[CCPART1]	*Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1*: Introduction and general model, Version 3.1, Revision 5, April 2017.
[CCPART2]	*Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.
[CCPART3]	*Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements*, Version 3.1, Revision 5, April 2017.
[CEM]	*Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, April 2017.
CFG_GPOS_BT_ WLANC_V1.0	*PP-Configuration for General Purpose Operating System, Bluetooth, and Wireless Local Area Network Clients,* Version 1.0, 2025-05-12
PP_OS_V4.3	*Protection Profile for General Purpose Operating Systems,* Version 4.3, 2022-09-27
MOD_BT_V1.0	*PP-Module for Bluetooth*, Version 1.0, 2021-04-15
MOD_WLANC_V1.0	*PP-Module for Local Area Network (WLAN) Clients*, Version 1.0, 2022-03-31
PKG_TLS_V1.1	*Functional Package for Transport Layer Security (TLS),* Version 1.1, 2019-03-01
[ST]	*Apple macOS 15 Sequoia Security Target*, Version 1.2, 2026-02-10
[CCGUIDE]	*Apple macOS 15 Sequoia Common Criteria Guide*, Version 1.1, 2026-02-10
[ETR]	*Evaluation Technical Report Apple macOS 15 Sequoia*, Version 1.1, 2026-02-15
[DTR]	*Detailed Test Report Apple macOS 15 Sequoia v1.1*, 2026-02-17
[AAR]	*Assurance Activity Report Apple macOS 15 Sequoia*, Version 1.1, 2026-01-02-17
[MTPLN]	*Mitigation Plan Apple macOS 15 Sequoia,* Version 1.1, 2026-02-17