National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report for
Apple iOS 18: iPhone

Report Number:	CCEVS-VR-VID11623-2025
Dated:	December 15, 2025
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

Patrick Mallett, Ph.D.

Jerome Myers, Ph.D.

Seada Mohammed

The Aerospace Corporation

Common Criteria Testing Laboratory

Joachim Vandersmissen

Stephan Mueller

Alex Gong

Dick Sikkema

Evan Barnett

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 iOS 18: iPhone (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, atsec Germany CCTL (Munich, Germany), Apple Inc. (Cupertino, CA, USA), and Apple Inc. (Prague, Czech Republic). Evaluation was completed in December 2025. 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 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
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple iOS 18 executing on the following platforms: • iPhone 11, iPhone 11 Pro, iPhone 11 iPro Max (A13 Bionic processor)

	• iPhone 12 mini, Phone 12, iPhone 12 Pro, iPhone 12 Pro Max (A14 Bionic processor) • iPhone 13 mini, iPhone 13, iPhone 13 Pro, iPhone 13 Pro Max, iPhone SE (3rd gen), iPhone 14, iPhone 14 Plus (A15 Bionic processor) • iPhone 14 Pro, iPhone 14 Pro Max, iPhone 15, iPhone 15 Plus (A16 Bionic processor) • iPhone 15 Pro, iPhone 15 Pro Max (A17 Pro processor) • iPhone 16e, iPhone 16, iPhone 16 Plus (A18 processor) • iPhone 16 Pro, iPhone 16 Pro Max (A18 Pro)
Security Target	Apple iOS 18: iPhone Security Target, Version 1.1, 2025-09-17
Sponsor & Developer	Apple, Inc.
Completion Date	December 2025
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 Mobile Device Fundamentals, Biometric enrollment and verification for unlocking the device, Bluetooth, MDM Agents, Virtual Private Network (VPN) Clients, and WLAN Clients. Version 1.1, dated 2025-01-03, [CFG_MDF_BIO-BT-MDMA-VPNC-WLANC_V1.1] • [MDF]: Base-PP: Protection Profile for Mobile Device Fundamentals. Version 3.3 (PP_MDF_V3.3) as of 2022-09-12. • [BIO]: PP-Module: collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module]. Version 1.1 (MOD_CPP_BIO_V1.1) as of 2022-09-12. • [BT]: PP-Module for Bluetooth. Version 1.0 (MOD_BT_V1.0) as of 2021-04-15. • [Agent]: PP-Module for MDM Agents. Version 1.0 (MOD_MDM_AGENT_V1.0) as of 2019-04-25. • [VPNC]: PP-Module for Virtual Private Network (VPN) Clients. Version 2.5 (MOD_VPNC_V2.5) as of 2024-06-24. • [WLANC]: PP-Module for WLAN Clients. Version 1.0 (MOD_WLANC_V1.0) as of 2022-03-31. [TLSPKG]: Functional Package for Transport Layer Security (TLS). Version 1.1 (PKG_TLS_V1.1) as of 2019-03-01.
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
Evaluation Personnel	Joachim Vandersmissen, Stephan Mueller, Alex Gong, Dick Sikkema, Evan Barnett, James Reid, Parker Collier, Walker Riley

Validation Personnel	Patrick Mallett, Ph.D., Jerome Myers, Ph.D., Seada Mohammed

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The Target of Evaluation (TOE) is Apple iOS 18: iPhone, which is a series of Apple iPhone mobile devices running the iOS 18.3.1 operating system, a Mobile Device Management (MDM) Agent, VPN client, and WLAN client components, which are included on the mobile devices.

The TOE operating system manages the device hardware, provides MDM Agent functionality, and provides the technologies required to implement native applications. It provides a built-in MDM framework application programmer interface (API), giving management features that may be utilized by external MDM solutions, allowing enterprises to use profiles to control some of the device settings.

The TOE operating system provides a consistent set of capabilities allowing the supervision of enrolled devices. This includes the preparation of devices for deployment, the subsequent management of the devices, and the termination of management.

The operating system part of the TOE acts as an intermediary between the underlying hardware and the apps running on the TOE. Apps do not talk to the underlying hardware directly. Instead, they communicate with the hardware through a set of well-defined system interfaces. These interfaces make it easy to write apps that work consistently on devices having different hardware capabilities.

The implementation of the TOE OS can be viewed as a set of layers described below. Lower layers contain fundamental services and technologies. Higher-level layers build upon the lower layers and provide more sophisticated services and technologies.

The Cocoa Touch layer contains key frameworks for building apps. These frameworks define the appearance of apps. They also provide the basic app infrastructure and support for key technologies such as multitasking, touch-based input, push notifications, and many high-level system services. When designing apps, one should investigate the technologies in this layer first to see if they meet the needs of the developer.

The Media layer contains the graphics, audio, and video technologies you use to implement multimedia experiences in apps.

The Core Services layer contains fundamental system services for apps. Key among these services is the Core Foundation and Foundation frameworks, which define the basic types that all apps use. This layer also contains individual technologies to support features such as location, iCloud, social media, and networking. Moreover, this layer implements data protection functions that allow apps that work with sensitive user data to take advantage of the built-in encryption available on some devices.

The Core OS layer contains the low-level features that most other technologies are built upon. This layer provides the security-related frameworks: Generic Security Services Framework for services specified in RFC 2743 and RFC 4401; Local Authentication Framework, Network Extension Framework for support of VPN tunnels, Security Framework for providing the Common Crypto library and managing certificates, cryptographic keys and trust policies and System Framework for providing the kernel environment and low-level UNIX interfaces.

4 Environmental Strengths

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

4.1 Security Audit

The TOE provides the ability for responses to be sent from the MDM Device Agent to the MDM Server. These responses are configurable by the organization.

4.2 Cryptographic Support

The TOE provides cryptographic services via the following cryptographic modules for the encryption of data at rest, for secure communication channels, and for use by applications. In addition, the TOE implements a number of cryptographic protocols that can be used to establish a trusted channel to other IT entities:

- Apple corecrypto Module v18 [Apple silicon, User, Software, SL1] (User Space)
- Apple corecrypto Module v18 [Apple silicon, Kernel, Software, SL1] (Kernel Space)
- Apple corecrypto Module v18 [Apple silicon, Secure Key Store, Hardware, SL2] (SKS)

4.3 User Data Protection

The TOE protects user data in files using cryptographic functions, ensuring this data remains protected even if the device gets lost or is stolen. Critical data (like passcodes used by apps or application-defined cryptographic keys) can be stored in the keychain, which provides additional protection. Passcode protection and encryption ensure that data at rest remains protected even in the case of the device being lost or stolen.

The TOE includes the Secure Enclave Processor (SEP), a separate CPU that executes a stand-alone operating system and has separate memory, which provides protection for critical security data such as keys.

The TOE protects data such that only the app that owns the data can access it.

4.4 Identification and Authentication

The TOE provides user authentication using a passcode or biometric (fingerprint or face) except for accessing Medical ID information, answering calls, making emergency calls, using the cameras, flashlight, control center or notification center, viewing widgets in Today View and search.

The passcode can be configured for a minimum length, for dedicated passcode policies, and for a maximum lifetime. When entered, passcodes are obscured and the frequency of entering passcodes is limited as well as the number of consecutive failed attempts of entering the passcode.

The TOE also enters a locked state after a (configurable) time of user inactivity and the user is required to either enter their passcode or use biometric authentication (fingerprint or face) to unlock the TOE

External entities connecting to the TOE via a secure protocol (e.g., Transport Layer Security (TLS), Extensible Authentication Protocol Transport Layer Security (EAP-TLS), IPsec) can be authenticated using X.509 certificates. The TOE also supports the usage of Post-quantum Preshared Keys in the IKEv2 protocol.

4.5 Security Management

The security functions listed in the Security Target can be managed either by the user or by an authorized administrator through a Mobile Device Management (MDM) system. The Security Target identifies the functions that can be managed and indicates if the management can be performed by the user, by the authorized administrator, or both.

4.6 Protection of the TSF

The TOE implements the following to protect the TSF and TSF data:

- Protection of cryptographic keys—keys used for TOE internal key wrapping and for the protection of data at rest are not exportable. There are provisions for fast and secure wiping of key material.
- Use of memory protection and processor states to separate apps and protect the TSF from unauthorized access to TSF resources—in addition, each device includes a separate system called the SEP which is the only system that can use the Root Encryption Key (REK). The SEP is a separate CPU that executes a stand-alone operating system and has separate memory.
- Digital signature protection of the TSF image—all updates to the TSF need to be digitally signed.
- Software/firmware integrity self-test upon start-up—the TOE will not go operational when this test fails.
- Digital signature verification for apps.
- Access to defined TSF data and TSF services only when the TOE is unlocked.

4.7 TOE Access

The TSF provides functions to lock the TOE upon request and after an administrator-configurable time of inactivity. Access to the TOE via a wireless network is controlled by user/administrator defined policy.

4.8 Trusted Path/Channel

The TOE supports the use of the following cryptographic protocols that define a trusted channel between itself and another trusted IT product:

- IEEE 802.11-2012
- IEEE 802.11ac-2013 (a.k.a. Wi-Fi 5)
- IEEE 802.11ax (a.k.a. Wi-Fi 6)
- IEEE 802.11be (a.k.a. Wi-Fi 7)
- IEEE 802.1X
- EAP-TLS
- TLS
- IPsec
- Bluetooth
- HTTPS

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.

- The TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.
- Mobile device users are not willfully negligent or hostile and use the device within compliance of a reasonable Enterprise security policy.
- The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.

- TOE administrators are competent, trusted personnel who are not careless, willfully negligent, or hostile and abide by guidance documentation.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

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.

- 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 iOS 18: iPhone, September 17, 2025 ([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.
- The TOE does not include the user apps that run on top of the operating system but does include controls that limit the behavior of the apps and enforce data segregation and impermeability across apps by establishing containerization principles

6 Documentation

The vendor provides guidance documents describing the installation process for Apple iOS 18: iPhone, as well as guidance for subsequent administration and use of the applicable security features.

The following guidance documentation was examined during the evaluation:

Table 2: Guidance

Reference	Document	Location
[CCGUIDE]	Apple iOS 18: iPhone and Apple iPadOS 18: iPad Common Criteria Configuration Guide, Version 1.1, 2025-09-17.	https://www.niap-ccevs.org/products/11623

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 therefore should not be relied upon to configure or operate the TOE as evaluated.

7 IT Product Testing

A non-proprietary description of the tests performed, and their results is provided in the Assurance Activity Report ([AAR]).

The purpose of the testing activity was 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 iOS 18: iPhone running on platform in *Table 3*. 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, atsec Germany CCTL (Munich, Germany), Apple Inc. (Cupertino, CA, USA), and Apple Inc. (Prague, Czech Republic) from April 2025 to July 2025.

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. The evaluation covers the following devices running iOS 18 operating system as detailed in Table 3.

Table 3: Devices Covered by the Evaluation

Processor	Device Name	Model Number
A13 Bionic	iPhone 11	A2111
		A2221
		A2223
	iPhone 11 Pro	A2160
		A2215

		A2217
	iPhone 11 Pro Max	A2161
		A2218
		A2220
A14 Bionic	iPhone 12 mini	A2176
		A2398
		A2399
		A2400
	iPhone 12	A2172
		A2402
		A2403
		A2404
	iPhone 12 Pro	A2341
		A2406
		A2407
		A2408
	iPhone 12 Pro Max	A2342
		A2410
		A2411
		A2412
A15 Bionic	iPhone 13 mini	A2481
		A2626
		A2628
		A2629
		A2630
	iPhone 13	A2482
		A2631

		A2633
		A2634
	iPhone 13 Pro	A2483
		A2636
		A2638
		A2639
		A2640
	iPhone 13 Pro Max	A2484
		A2641
		A2643
		A2644
		A2645
	iPhone SE (3rd gen)	A2595
		A2782
		A2783
		A2785
	iPhone 14	A2649
		A2881
		A2882
		A2883
		A2884
	iPhone 14 Plus	A2632
		A2885
		A2886
		A2887
		A2888
A16 Bionic	iPhone 14 Pro	A2650

		A2889
		A2890
		A2891
		A2892
	iPhone 14 Pro Max	A2651
		A2893
		A2894
		A2895
		A2896
	iPhone 15	A2846
		A3089
		A3090
		A3092
	iPhone 15 Plus	A2847
		A3093
		A3094
		A3096
A17 Pro	iPhone 15 Pro	A2848
		A3101
		A3102
		A3104
	iPhone 15 Pro Max	A2849
		A3105
		A3106
		A3108
A18	iPhone 16e	A3212
		A3410

		A3409
		A3408
	iPhone 16	A3081
		A3288
		A3287
		A3286
	iPhone 16 Plus	A3082
		A3291
		A3290
		A3289
A18 Pro	iPhone 16 Pro	A3083
		A3294
		A3293
		A3292
	iPhone 16 Pro Max	A3084
		A3297
		A3296
		A3295

8.2 Excluded Functionality

The following security functionalities were not evaluated and are, therefore, excluded from the secure configuration of the mobile devices.

Apple iOS 18: iPhone additionally includes the following features that are not part of the evaluated TOE because they are outside the scope of the functionality described by the TOE's conformance claims:

- **Two-Factor Authentication**

  Two-factor authentication is an extra layer of security for an Apple ID used in the Apple store, iCloud, and other Apple services.

- **Bonjour**

  Bonjour is Apple's standards-based, zero configuration network protocol that lets devices find services on a network.

- **VPN Split Tunnel**

VPN split tunnel is not included in the evaluation and must be disabled in the Mobile Device configurations to meet the requirements of this CC evaluation.

- **Siri Interface**

  The Siri interface is capable of supporting commands related to configuration settings.

- **Third-party MDM Agents**

  Third-party applications are available that provide functionality as a Mobile Device MDM Agent. No third-party MDM Agent applications were included in the evaluation and are outside the scope of the evaluated configuration.

- **VPN Protocols and Authentication Methods**

  The following Virtual Private Network (VPN) protocols are not included in the evaluation and must be disabled in the Mobile Device configurations that meet the requirements of this CC evaluation.

  - Cisco IPsec
  - Layer Two Tunneling Protocol (L2TP) over IPsec
  - Secure Sockets Layer (SSL) VPN
  - Shared secret authentication

- **Face ID with a Mask**

  Face unlock with a face mask was not included in the evaluation. The Face ID with a Mask setting must be disabled in the evaluated configuration.

- **iCloud storage**

  Data storage or backup to iCloud is not supported in the evaluated configuration.

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 iOS 18: iPhone ([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 iOS 18: iPhone 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 was 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.1, ASE_REQ.1, 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.

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.

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 AGE_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.

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 and ALC_CMS.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.

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 Test Report, summarized in the AAR, section 2.3.4.

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 comprised a search of public vulnerability databases. Please refer to Section 2.3.5 of the [AAR] for more details.

The evaluator searched for publicly known vulnerabilities using 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 content disclosure statements for releases of iPadOS 18 related to this evaluation. **Note:** All releases of iPadOS contain security fixes for publicly known vulnerabilities.
  - https://support.apple.com/en-us/100100

As required by the vulnerability mitigation guidance, the following search terms were used during the vulnerability search:

- iPhone iOS 18
- curl
- libarchive
- libexpat
- libxml2
- libxslt
- Safari
- Apple Mail
- iMessage
- AirDrop
- AirPlay
- Secure Enclave Processor
- BCM4399
- BCM4388
- BCM4387
- BCM4378
- BCM4355
- corecrypto
- IEEE 802.11
- EAP-TLS
- TLS
- IPsec
- Bluetooth

The vulnerability search was repeated on the following dates, throughout the evaluation process (last search date: 2025-11-21):

- 2025-06-12
- 2025-06-30
- 2025-07-02
- 2025-07-03
- 2025-07-10
- 2025-07-11
- 2025-07-18
- 2025-07-23
- 2025-09-20
- 2025-10-28
- 2025-11-21

All “crucial” vulnerabilities (as defined by the NIAP Policy 17 Addendum) found during the vulnerability searches were mitigated. Any residual vulnerabilities are not considered crucial. Subsequently, the evaluator performed a generic port scan on the TOE to search for any undocumented open network ports. The evaluator found that no ports are unexpectedly open. In other words: all ports are associated with the TOE and publicly documented as such.

In addition to the lists of fixes published by the vendor, the evaluator performed manual searches throughout the evaluation process. The most recent searches did not identify any crucial vulnerabilities that were not addressed prior to product placement on the NIAP PCL. 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.

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 iOS 18: iPhone and Apple iPadOS 18: iPad Common Criteria Configuration Guide, Version 1.1, 2025-09-17.

No versions of the TOE and software, either earlier or later are covered by the scope of this evaluation. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The excluded functionality is specified in section 8.2 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Security Target

The ST for this product's evaluation is Apple iOS 18: iPhone Security Target, Version 1.1, dated 2025-09-17 ([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_MDF_BIO-BT-MDMA-VPNC-WLAN_V1.1]	PP-Configuration for Mobile Device Fundamentals, Biometric enrollment and verification for unlocking the device, Bluetooth, MDM Agents, Virtual Private Network (VPN) Clients, and WLAN Clients. Version 1.1, dated 2025-01-03.
[AAR]	Assurance Activity Report Apple iOS 18: iPhone, Version 1.3, 2025-12-12.
[BIO]	PP-Module for collaborative PP-Module for Biometric enrolment and verification – for unlocking the device, Version 1.1, 2022-09-12.
[BT]	PP-Module for Bluetooth, Version 1.0, 2021-04-15.
[CCGUIDE]	Apple iOS 18: iPhone and Apple iPadOS 18: iPad Common Criteria Configuration Guide, Version 1.1, 2025-09-17.
[ETR]	Evaluation Technical Report Apple iOS 18: iPhone, Version 1.5, 2025-12-12.
[MDF]	Protection Profile for Mobile Device Fundamentals. Version 3.3, 2022-09-12.
[ST]	Apple iOS 18: iPhone Security Target, Version 1.1, 2025-09-17.
[TLSPKG]	Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-03-01.
[VPNC]	PP-Module for Virtual Private Network (VPN) Clients. Version 2.5, 2024-06-24.
[WLANC]	PP-Module for WLAN Clients. Version 1.0, 2022-03-31.