Wallet Application Security Audit Report

Table Of Contents

1 Executive Summary

On 2025.08.04, the SlowMist security team received the Rabby team's security audit application for Rabby mobile wallet iOS, developed the audit plan according to the agreement of both parties and the characteristics of the project, and finally issued the security audit report.

The SlowMist security team adopts the strategy of "black-box and grey-box" to conduct a complete security test on the project in the way closest to the real attack.

The test method information:

Test method	Description
Black box testing	Conduct security tests from an attacker's perspective externally.
Grey box testing	Conduct security testing on code modules through the scripting tool, observing the internal running status, mining weaknesses.
White box testing	Based on the open source code, non-open source code, to detect whether there are vulnerabilities in programs such as nodes, SDK, etc.

The vulnerability severity level information:

Level	Description
Critical	Critical severity vulnerabilities will have a significant impact on the security of the project, and it is strongly recommended to fix the critical vulnerabilities.
High	High severity vulnerabilities will affect the normal operation of the project. It is strongly recommended to fix high-risk vulnerabilities.
Medium	Medium severity vulnerability will affect the operation of the project. It is recommended to fix medium-risk vulnerabilities.
Low	Low severity vulnerabilities may affect the operation of the project in certain scenarios. It is suggested that the project team should evaluate and consider whether these vulnerabilities need to be fixed.
Weakness	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.
Suggestion	There are better practices for coding or architecture.

2 Audit Methodology

The security audit process of SlowMist security team for wallet application includes two steps:

The codes are scanned/tested for commonly known and more specific vulnerabilities using automated analysis tools.

Manual audit of the codes for security issues. The wallet application is manually analyzed to look for any potential issues.

The following is a list of security audit items considered during an audit:

NO.	Audit Items	Result
1	App runtime environment detection	Passed
2	Code decompilation detection	Passed
3	App permissions detection	Passed
4	File storage security audit	Passed
5	Communication encryption security audit	Passed
6	Interface security audit	Passed
7	Business security audit	Passed
8	WebKit security audit	Passed
9	App cache security audit	Passed
10	WebView DOM security audit	Passed
11	SQLite storage security audit	Passed
12	Deeplinks security audit	Passed
13	Client-Based Authentication Security audit	Passed
14	Signature security audit	Passed
15	Deposit/Transfer security audit	Passed
16	Transaction broadcast security audit	Passed

NO.	Audit Items	Result
17	Secret key generation security audit	Passed
18	Secret key storage security audit	Passed
19	Secret key usage security audit	Passed
20	Secret key backup security audit	Passed
21	Secret key destruction security audit	Passed
22	Screenshot/screen recording detection	Passed
23	Paste copy detection	Passed
24	Keyboard keystroke cache detection	Passed
25	Insecure entropy source security audit	Passed
26	Background obfuscation detection	Passed
27	Suspend evoke security audit	Passed
28	AML anti-money laundering security policy detection	Passed
29	Others	Passed
30	User interaction security	Passed
31	Cryptography security audit	Passed

3 Project Overview

3.1 Project Introduction

Audit Version

Source Code

Link: https://github.com/RabbyHub/rabby-mobile

Commit hash: f4aaa2a72a4075df655387961c193d3d2fc1bdf7

iOS

App Link: https://apps.apple.com/us/app/rabby-wallet-crypto-evm/id6474381673

App Version: 0.6.31

Sha256: deab7866986f1940b8cd5eba86a615ade669396d45151bf70203d530f4054b26

Fixed Version

Source Code

Link: https://github.com/RabbyHub/rabby-mobile

Commit hash: 979aa26760c5dc72874899863d051ce9abb30167

iOS

App Link: https://download.rabby.io/downloads/wallet-mobile-pretest/ios-0.6.32.1-20250819_174404/rabbymobile.ipa

App Version: 0.6.32

Sha256: 12f969dba5a844a7b1123eaee5c5c789d0b334215625dc63ac9b70b1320bb5df

3.2 Vulnerability Information

The following is the status of the vulnerabilities found in this audit:

NO	Title	Category	Level	Status
N1	Insufficient App Runtime Environment Detection	App runtime environment detection	Suggestion	Acknowledged
N2	Weaknesses in Communication Encryption	Communication encryption security audit	Suggestion	Acknowledged
N3	User Interaction Issue	User interaction security	Suggestion	Acknowledged
N4	"Unknown Signature Type" lacks security reminder	User interaction security	Suggestion	Fixed

3.3 Vulnerability Summary

[N1] [Suggestion] Insufficient App Runtime Environment Detection

Category: App runtime environment detection

Content

The Rabby Mobile App lacks detection mechanisms for jailbroken devices and Frida hooks.

Solution

It is recommended to add a detection and alert mechanism for jailbroken iOS devices.

Status

Acknowledged

[N2] [Suggestion] Weaknesses in Communication Encryption

Category: Communication encryption security audit

Content

1. Communication encryption is carried out using the HTTPS protocol for transmission.
2. Communication encryption performs certificate verification on the client-side and does not employ mutual authentication.

Solution

It is recommended to use two-way certificate binding or certificate whitelist for communication encryption.

Status

Acknowledged

[N3] [Suggestion] User Interaction Issue

Category: User interaction security

Content

Functionality	Support	Notes
WYSIWYS	✓	There is friendly parsing of the data.
AML	✓	AML strategy is supported.

Functionality	Support	Notes
Anti-phishing	✓	Phishing detect warning is supported.
Pre-execution	✓	Pre-execution result display is supported.
Contact whitelisting	✓	The contact whitelisting is supported.
Password complexity requirements	✗	The password complexity is not supported.

Tip: ✓ Full support, ● Partial support, ✗ No support

Solution

It is recommended to enhance security by integrating password complexity requirements.

Status

Acknowledged

[N4] [Suggestion] "Unknown Signature Type" lacks security reminder

Category: User interaction security

Content

Rabby mobile wallet will mark transactions with unrecognized signature types as "Unknown Signature Type" and

there will be no reminder of security risks. However, these transactions can be normally parsed on the blockchain.

Solution

It is recommended to remind users of the security risks associated with these unrecognizable signature information, and to allow users to confirm the signature information carefully before proceeding with the signature.

Status

Fixed

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002508150003	SlowMist Security Team	2025.08.04 - 2025.08.15	Passed

Summary conclusion: The SlowMist security team conducted the audit using manual methods along with SlowMist's proprietary analysis tools. During the audit, we identified four issues, all categorized as "Suggestion" level. One of these issues has been fixed, while the remaining findings have been acknowledged.

5 Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility based on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.

Official Website

www.slowmist.com

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist