Wallet Application Security Audit Report

Table Of Contents

1 Executive Summary

On 2023.03.06, the SlowMist security team received the Sender Wallet team's security audit application for Sender Wallet Android, 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/grey box lead, white box assists" 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	Confirmed
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	Fixed
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	Confirmed
23	Paste copy detection	Confirmed
24	Keyboard keystroke cache detection	Confirmed
25	Background obfuscation detection	Confirmed
26	Suspend evoke security audit	Passed
27	AML anti-money laundering security policy detection	Confirmed
28	Others	Passed
29	User interaction security	Confirmed

3 Project Overview

3.1 Project Introduction

Audit Version

https://github.com/SenderWallet/sender-wallet-mobile/tree/slowmist-multi-chain

commit: 6ad3714c31fbae81c695ab846c42c50e2f92b21f

Android sender-mobile-multichain.apk V2.0.1

(sha256:3ec908fec7a121357575e29a9dd32b26f3d9521f9eee443f1c87f18ed9116e30)

Fixed Version

https://github.com/SenderWallet/sender-wallet-mobile/tree/slowmist-multi-chain

commit: 973e529554053c15ac660a996965dfe17d037233

Android sender-mobile-multichain.apk V2.0.1

(sha256:35de4faba5ba858d804507b27a7cea4b04943e9a19dbb4e7389e6e84c61586e0)

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	User interaction security suggestions	User interaction security	Suggestion	Confirmed
N2	Enhanced mnemonic verification	Business security audit	Suggestion	Confirmed
N3	Missing screenshot/screen recording detection	Screenshot/screen recording detection	Suggestion	Confirmed
N4	Lack of security reminders	Paste copy detection	Suggestion	Confirmed
N5	Lack of secure keyboard	Keyboard keystroke cache detection	Suggestion	Confirmed
N6	Background obfuscation issue	Background obfuscation detection	Suggestion	Confirmed
N7	Lack of AML security policy	AML anti-money laundering security policy detection	Suggestion	Confirmed
N8	The information leakage of developers	Code decompilation detection	Suggestion	Confirmed
N9	Defect in business logic	Business security audit	Suggestion	Fixed

3.3 Vulnerability Summary

[N1] [Suggestion] User interaction security suggestions

Category: User interaction security

Content

Functionality	Support	Notes
WYSIWYS	✓	The current version only allows signature transfers via WalletConnect.
AML	✗	AML strategy is not supported.
Anti-phishing	✗	Phishing detect warning is not supported.
Pre-execution	✗	Pre-execution result display is not supported.
Contact whitelisting	✗	The contact whitelisting is not supported, causing similar address attacks.
Password complexity requirements	✗	There is no password complexity limit.

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

Solution

It is recommended to add AML, Anti-phishing, Pre-execution and contact whitelisting functions to the application, and password complexity constraints need to be made.It is recommended to remind users to double-check the accuracy of the transfer destination address when it is not in their address book.

Status

Confirmed

[N2] [Suggestion] Enhanced mnemonic verification

Category: Business security audit

Content

When creating a wallet, the user is required to confirm whether the mnemonic phrase is backed up completely.The app only requires the user to verify 1 of the 12 mnemonic phrases, and this verification method needs to be strengthened. Because all mnemonics may not be fully backed up with.

Solution

It is recommended to scramble the 12 mnemonics and then let the user reorder the mnemonics, so as to guide the

user to verify the correctness of each mnemonic.

Status

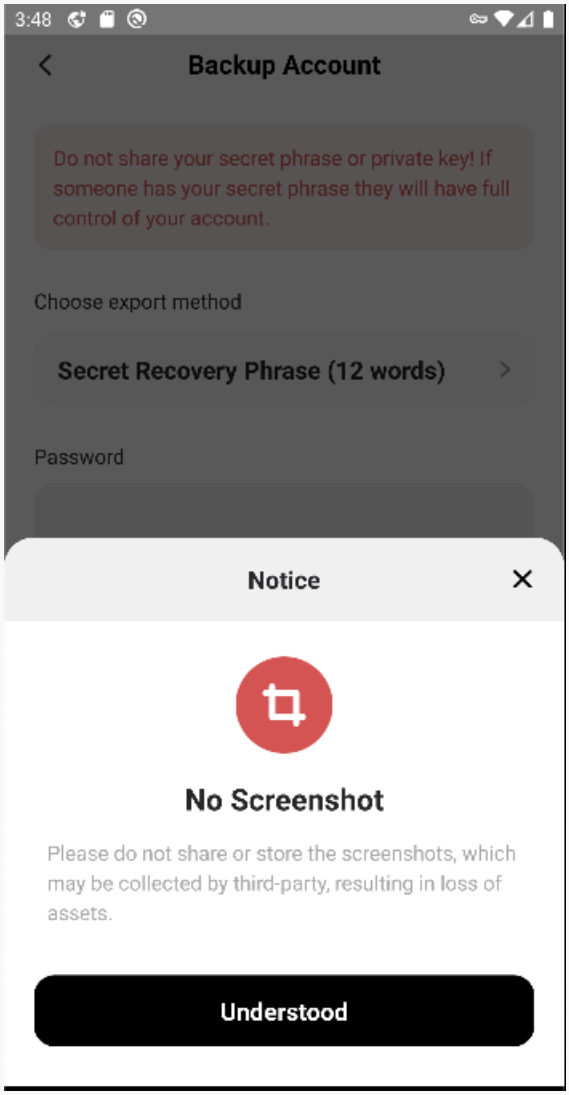
Confirmed

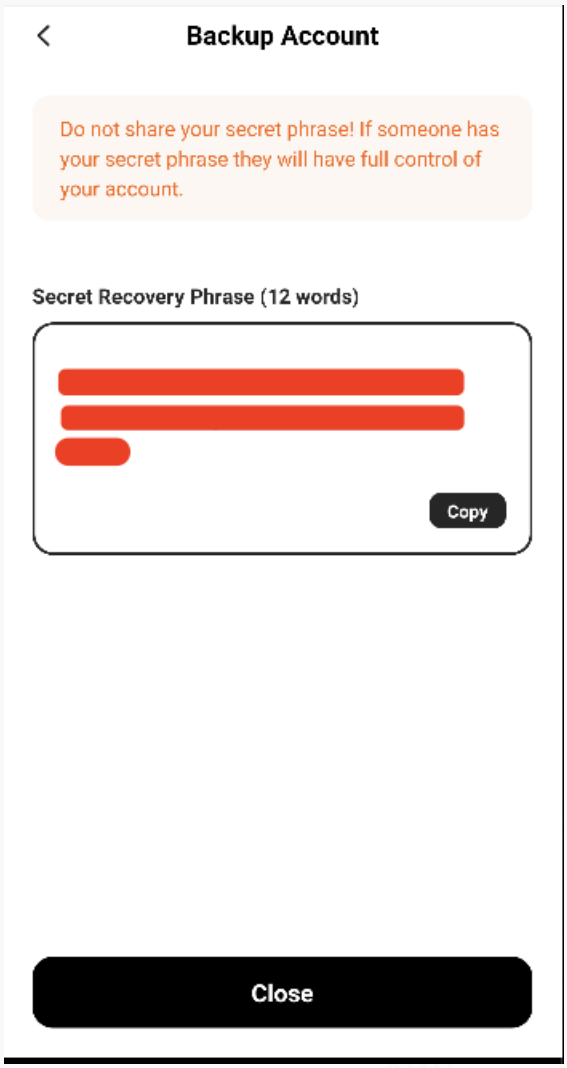
[N3] [Suggestion] Missing screenshot/screen recording detection

Category: Screenshot/screen recording detection

Content

The app has a reminder that screenshots are prohibited, but it does not restrict users from taking screenshots and missing screenshot detection and restrictions.





Solution

It is recommended to add screenshot/screen recording detection and prohibit screenshot/screen recording.

Status

Confirmed

[N4] [Suggestion] Lack of security reminders

Category: Paste copy detection

Content

When exporting wallets, users are allowed to copy mnemonic phrases and the app lacks security reminders, which may be subject to clipboard hijacking attacks.

Solution

It is recommended to remind users that they should record by transcribing instead of directly using the clipboard for copying.

Status

Confirmed

[N5] [Suggestion] Lack of secure keyboard

Category: Keyboard keystroke cache detection

Content

The app does not use a secure keyboard, mnemonics and passwords may be stolen by the keyboard when using the app.

Solution

It is recommended to add a secure keyboard and use the secure keyboard when entering mnemonics and passwords to avoid sensitive data being recorded.

Status

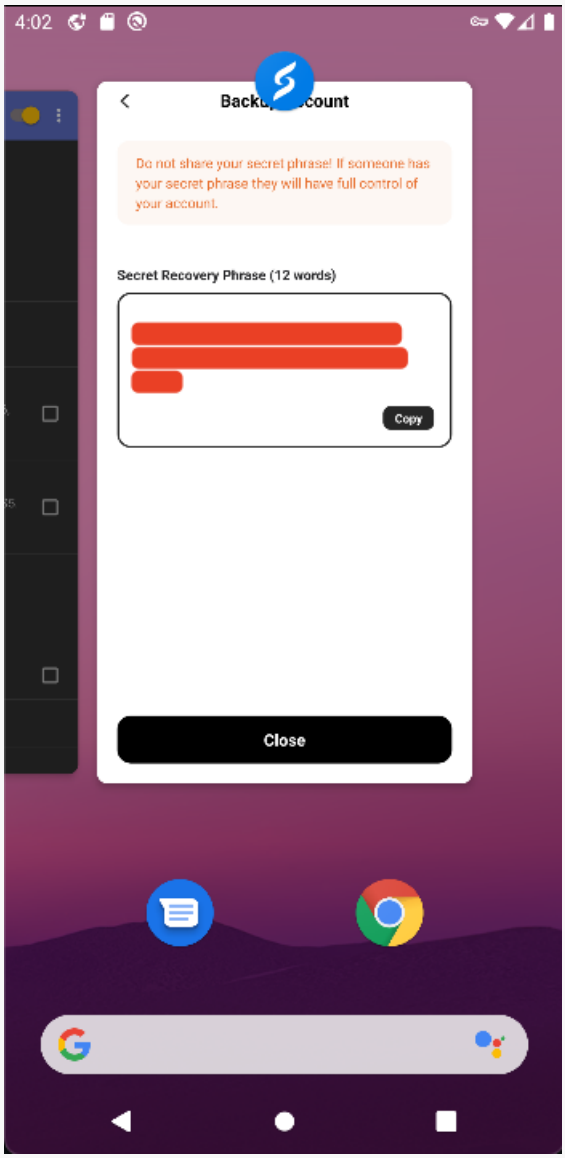
Confirmed

[N6] [Suggestion] Background obfuscation issue

Category: Background obfuscation detection

Content

App UI is not obfuscation when the app is in the background.If the wallet is being exported, the mnemonic phrase may be leaked.



Solution

It is recommended to add an obfuscation mechanism to avoid sensitive data leakage.

Status

Confirmed

[N7] [Suggestion] Lack of AML security policy

Category: AML anti-money laundering security policy detection

Content

The app does not have access to the AML security policy and cannot synchronize malicious addresses to users in a timely manner.

Solution

It is recommended to access the AML security policy to remind users to avoid interacting with malicious addresses.

Status

Confirmed

[N8] [Suggestion] The information leakage of developers

Category: Code decompilation detection

Content

The "index.android.bundle" file has leaked information about the developers.

```
phasedRegistrationNames:{bubbled:'onKeyPress',captured:'onKeyPressCapture'}},topPress:{phasedRegistrationNames:{bubbled:'onPress',captured:'onPressCa
essage'},topMomentumScrollBegin:{registrationName:'onMomentumScrollBegin'},topMomentumScrollEnd:{registrationName:'onMomentumScrollEnd'},topScroll:{r
andObjectDiff=f,e.stringifyViewConfig=function(t){return JSON.stringify(t,function(t,n){return'function'==typeof n?"\u0192 "+n.name:n},2)};var t=r(d[
structor!==u.constructor)return!0;if(Array.isArray(o)){var y=o.length;if(u.length!==y)return!0;for(var p=0;p<y;p++)if(t(o[p],u[p],l-1,c))return!0}els



ldYield=function(){return!1},r=_e.unstable_forceFrameRate=function(){}}else{var f=window.setTimeout,b=window.clearTimeout;if("undefined"!=typeof cons
])),c=["animating","color","hidesWhenStopped","onLayout","size","style"],f=this,p="/Users/shizhongwei/app/project/sender/sender_wallet_mobile/node_mo
/sender_wallet_mobile/node_modules/react-native/Libraries/Components/View/View.js";function c(t){if("function"!=typeof WeakMap)return null;var n=new
.hasOwnProperty.call(t,p)){var s=l?Object.getOwnPropertyDescriptor(t,p):null;s&&(s.get||s.set)?Object.defineProperty(u,p,s):u[p]=t[p]}return u.defaul

umber:91,columnNumber:5}}))});m.exports=f},179,[1,31,105,180,131]);

default)(l)};e.default=t},181,[1,182,45]);
```

Solution

It is recommended to check for information leaks in the code and remove them before publishing the sender wallet app.

Status

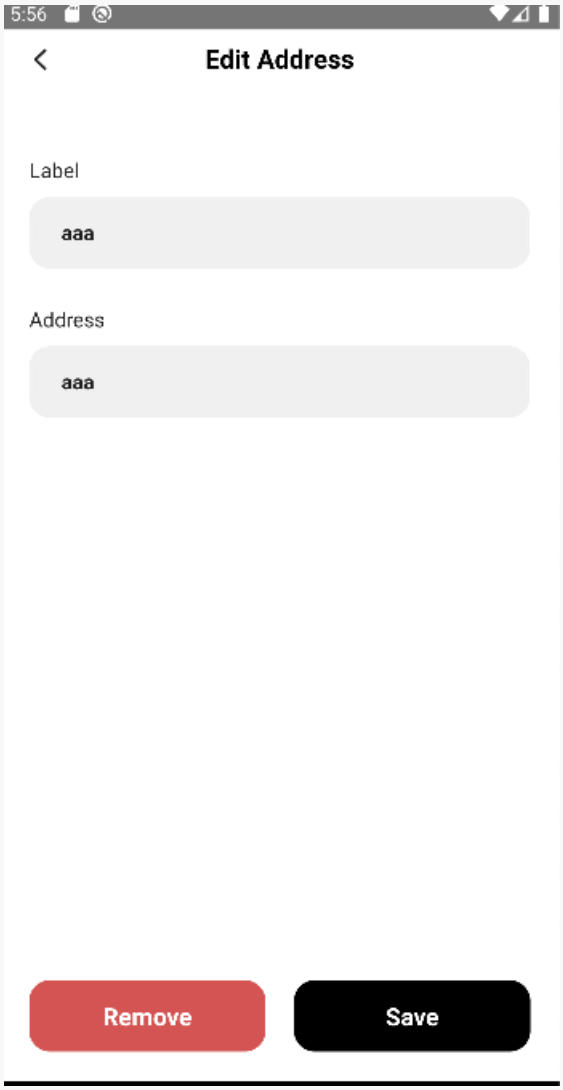
Confirmed

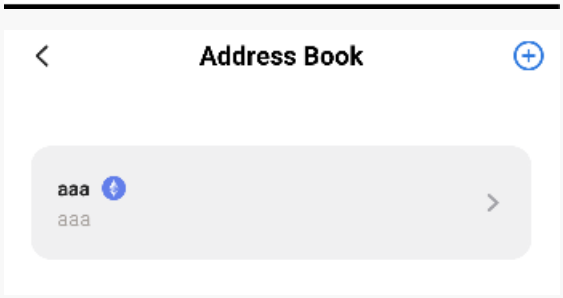
[N9] [Suggestion] Defect in business logic

Category: Business security audit

Content

Adding an address to the address book without checking its validity.





There is a bug in the address deletion feature where clicking the delete button does not remove the address.

Solution

1. It is recommended to check the validity of addresses before adding them to the address book;
2. It is recommended to fix the bug that the address cannot be deleted.

Status

Fixed

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002303170001	SlowMist Security Team	2023.03.06 - 2023.03.17	Passed

Summary conclusion: The SlowMist security team use a manual and SlowMist team's analysis tool to audit the project, during the audit work we found 9 suggestion vulnerabilities. And 1 suggestion risks vulnerabilities were confirmed and being fixed. All the findings have been confirmed. We extend our gratitude for Sender Wallet team recognition of SlowMist and hard work and support of relevant staff.

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