Wallet Application Security Audit Report

Table Of Contents

1 Executive Summary

On 2023.05.16, the SlowMist security team received the OKX team's security audit application for OKX MPC 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	Some Risks
3	App permissions detection	Some Risks
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

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

3 Project Overview

3.1 Project Introduction

Audit Version

App Name: okx-android.apk

App Link:https://static.febjify.cn/upgradeapp/okx-android.apk

App Version: 6.14.0

Sha256: 5f3c3ea7eba6c5d69fca01e2fb207bec06c74d32e98beb3f104956a1c0bf5618

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Code decompilation issue	Code decompilation detection	Low	Confirmed
N2	Access control issue	App permissions detection	Suggestion	Confirmed
N3	Suspend and invoke security issue	Suspend evoke security audit	Suggestion	Confirmed
N4	Missing screenshot/screen recording detection	Screenshot/screen recording detection	Suggestion	Confirmed
N5	Built-in security keyboard not used	Keyboard keystroke cache detection	Suggestion	Confirmed
N6	User interaction security suggestions	User interaction security	Suggestion	Confirmed
N7	Secret key storage security issue	Secret key storage security audit	Suggestion	Confirmed
N8	Secret key storage security issue	Secret key storage security audit	Suggestion	Confirmed
N9	The signature information display is incomplete	User interaction security	Suggestion	Confirmed
N10	Insufficient backup and recovery authentication	Secret key backup security audit	Suggestion	Confirmed

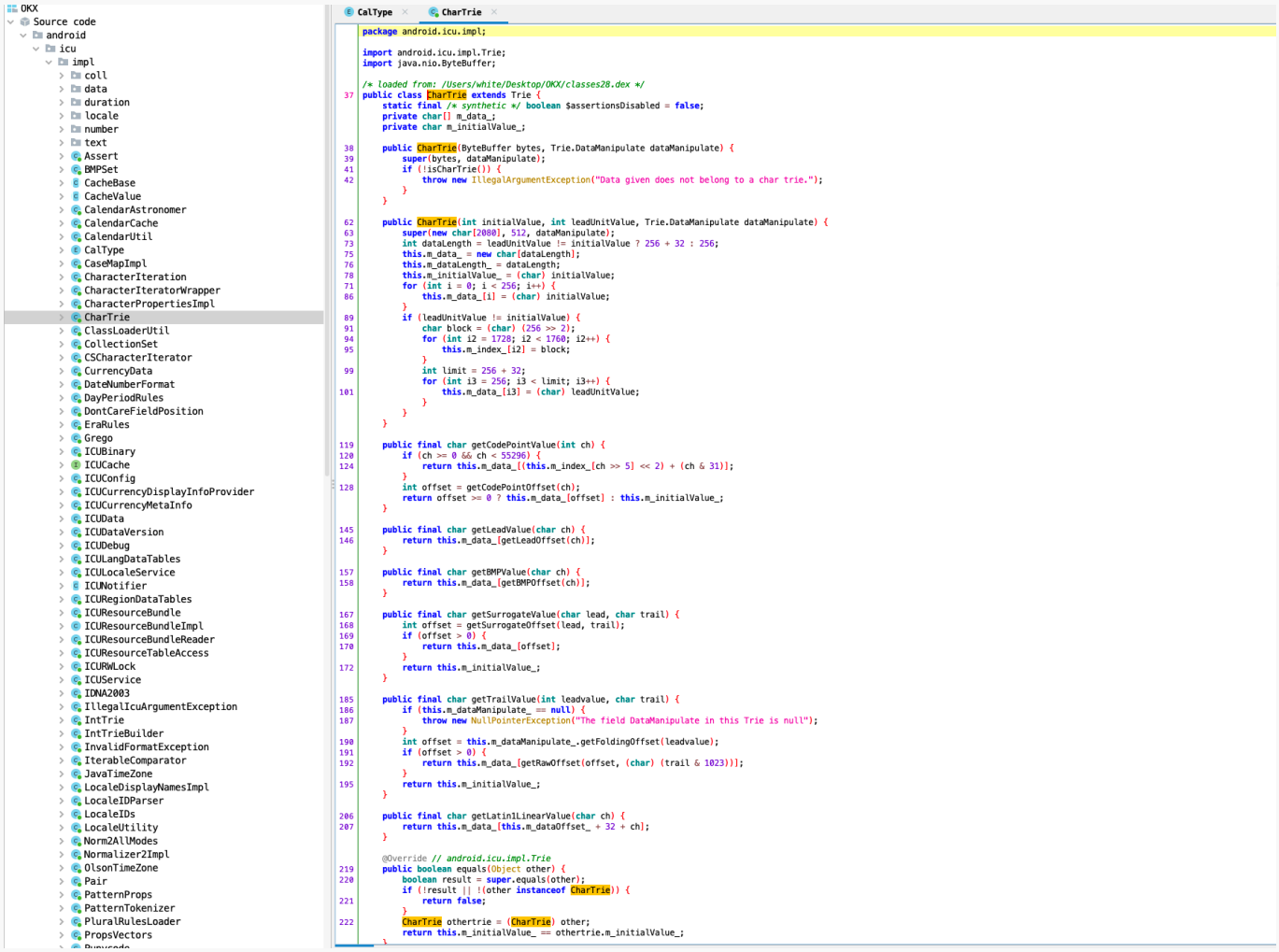
3.3 Vulnerability Summary

[N1] [Low] Code decompilation issue

Category: Code decompilation detection

Content

The unobfuscated code can be seen by decompiling.



Solution

1. Use code obfuscation techniques: Code obfuscation can convert critical information, variables, and function names in the application code into meaningless characters, thereby increasing the difficulty of decompiling the application.
2. Encrypt sensitive data: For sensitive information and data, encryption techniques can be used to protect them, thereby increasing the difficulty for attackers to obtain the information.
3. Use anti-debugging techniques: The application can use anti-debugging techniques to prevent attackers from using debuggers to decompile and analyze it. For example, open-source tools or custom code can be used for anti-debugging.

4. Use digital signatures and certificates: Digital signatures and certificates can be used to verify the authenticity of the application and prevent attackers from decompiling and analyzing it by tampering with it.
5. Protect sensitive code and critical algorithms: Hardware protection, secure storage, and encryption techniques can be used to protect sensitive code and critical algorithms, thereby increasing the difficulty for attackers to obtain information.

Status

Confirmed

[N2] [Suggestion] Access control issue

Category: App permissions detection

Content

The app obtains many permissions, some of which are relatively dangerous, and the project party needs to confirm whether these permissions are required by the business.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.QUERY_ALL_PACKAGES	normal		Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_SCAN	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_ADVERTISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
MediaStore.Images.Media.INTERNAL_CONTENT_URI	unknown	Unknown permission	Unknown permission from android reference
MediaStore.Images.Media.EXTERNAL_CONTENT_URI	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
com.okinc.okex.gp.permission.MIPUSH_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.okinc.okex.gp.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.okinc.okex.gp.push.permission.MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	unknown	Unknown permission	Unknown permission from android reference
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.okinc.okex.gp.permission.PROCESS_PUSH_MSG	unknown	Unknown permission	Unknown permission from android reference
com.okinc.okex.gp.permission.PUSH_PROVIDER	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	Show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
com.okinc.okex.gp.permission.RONG_ACCESS_RECEIVER	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference

Solution

It is recommended to remove unnecessary permission acquisition.

Status

Confirmed

[N3] [Suggestion] Suspend and invoke security issue

Category: Suspend evoke security audit

Content

1. No timeout mechanism was found in the wallet app, and the test was suspended for quite a while without re-verification of the password.
2. After the background is suspended, you can continue to use it without verifying the wallet password.

Solution

It is recommended to re-awaken the App after a period of suspension in the background to verify the password.

Status

Confirmed; 1. It is recommended to automatically log out when the wallet has not been operated for a long time, and to wake up again requires verification of the password.

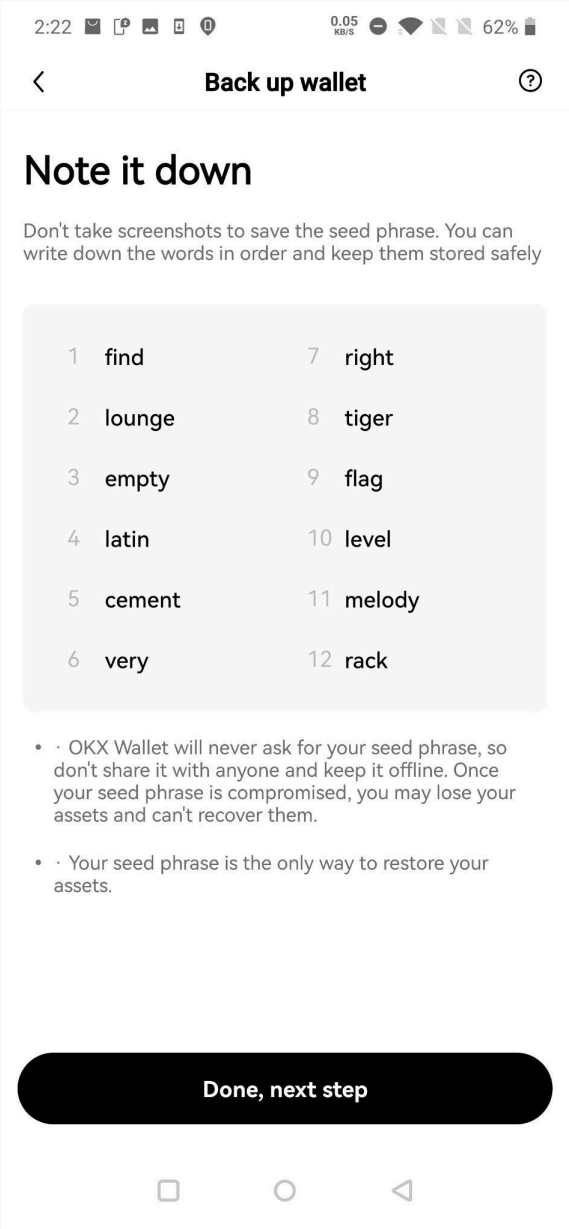
2. It is recommended to verify the password when the wallet wakes up again from the background.

[N4] [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

[N5] [Suggestion] Built-in security keyboard not used

Category: Keyboard keystroke cache detection

Content

The wallet app does not have a built-in secure keyboard, allowing the use of third-party keyboards. If the user uses an unsafe third-party keyboard mnemonic and other important information may be collected by the third-party keyboard, resulting in information leakage.

Solution

The third-party input method will collect the input content of the user, so it may lead to the leakage of the mnemonic phrase. It is recommended to use a secure keyboard.

Status

Confirmed

[N6] [Suggestion] User interaction security suggestions

Category: User interaction security

Content

Functionality	Support	Notes
WYSIWYS	•	There is no friendly parsing of the data.
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 are no password complexity requirements.

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

[N7] [Suggestion] Secret key storage security issue

Category: Secret key storage security audit

Content

The wallet mnemonic, private keys, and MPC private key shard information are stored using AES encryption. However, AES encryption algorithm is not the optimal solution as it may be vulnerable to brute-force enumeration.

- MPC-iOS/OKWalletCore/Bridge/OKWBridge.m#line215-217

```
+ (OKWBridgeResult<NSString *> *)encodeData:(NSString *)pwd pwdHash:(NSString
*)pwdHash data:(NSString *)data {
    return [self dispatch:@"encrypt_data" data:@{@"passWord": pwd ? : @"",
@"passWordHash": pwdHash ? : @"", @"data": data ? : @""}];
}
```

- wallet-core/core/core.go#line36-46

```
func EncryptData(pass, hash, data string) (string, int) {
        if !ValidatePass(pass, hash) {
                return "", storage.PASS_ERROR
        }
        aesPass := getAesPass(pass, hash)
        d, err := crypto.Encrypt([]byte(data), aesPass)
        if err != nil {
                return "", storage.DATA_ERROR
        }
        return d, storage.SUCCESS
}
```

- wallet-core/thirdparty/crypto/aes.go#line82-88

```
func Encrypt(rawData, key []byte) (string, error) {
        data, err := AesCBCEncrypt(rawData, key)
        if err != nil {
                return "", err
        }
        return base64.StdEncoding.EncodeToString(data), nil
}
```

Solution

It is recommended to use RSA encryption algorithm for secure storage.

Status

Confirmed

[N8] [Suggestion] Secret key storage security issue

Category: Secret key storage security audit

Content

The getAesPass function invokes MoreHash with an input parameter of 1, indicating the intention to perform multiple hash calculations. However, it seems that the number of calculations in this context is insufficient.

- wallet-core/core/core.go#line71-78

```
func getAesPass(pass string, hash string) []byte {
        h, _ := getHash(pass, hash)
        hb := MoreHash(1, []byte(pass), sha3.NewKeccak256())
        aesPass, _ := hex.DecodeString(h)
        copy(aesPass[:8], hb[:8])
        copy(aesPass[len(aesPass)-8:], hb[len(hb)-8:])
        return aesPass
}
```

- wallet-core/core/core.go#line96-103

```
func MoreHash(count int, value []byte, h hash.Hash) []byte {
        for i := 0; i < count; i++ {
                h.Reset()
                h.Write(value)
                value = h.Sum(nil)
        }
        return value[:32]
}
```

Solution

It is recommended to have an adequate number of iterations for hash computations.

Status

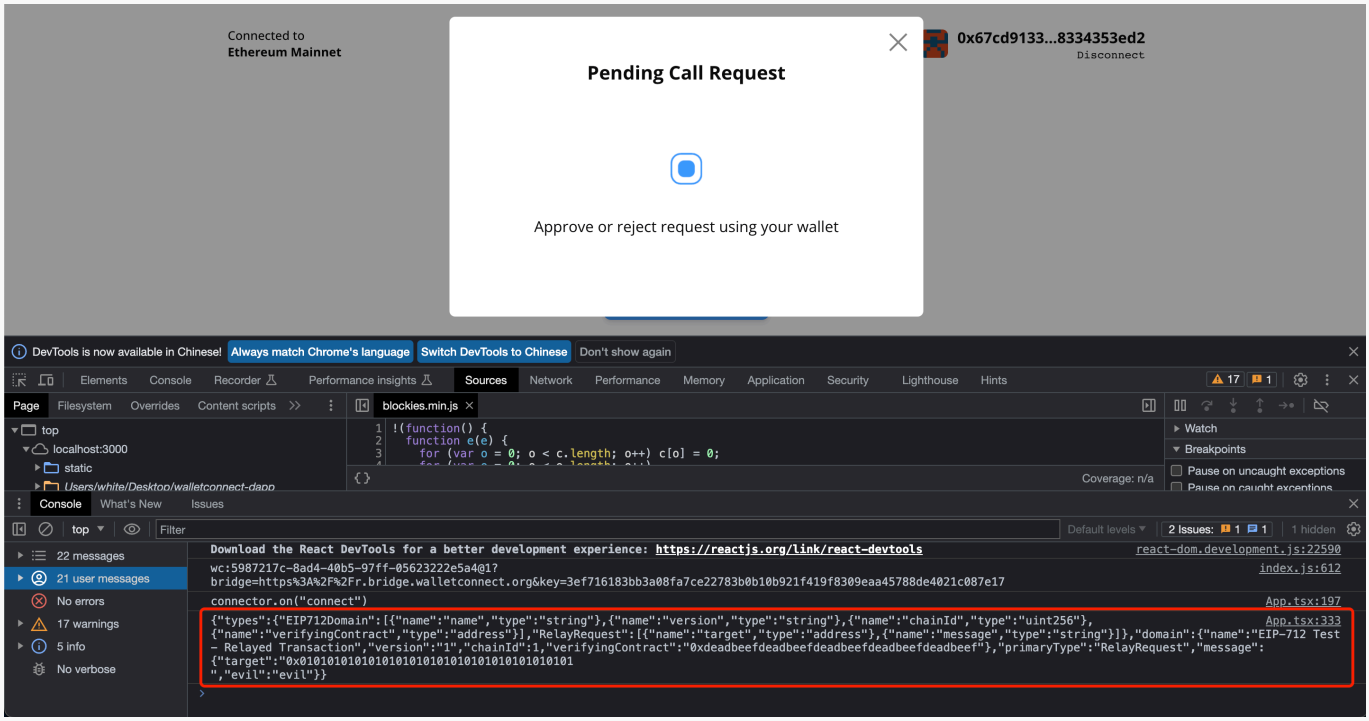
Confirmed

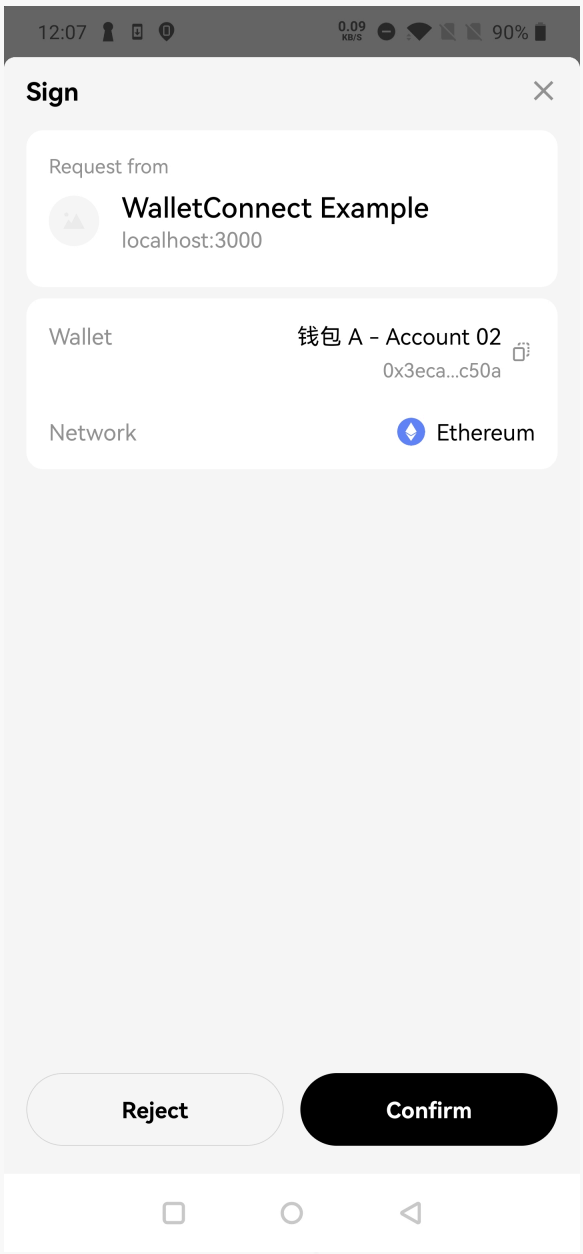
[N9] [Suggestion] The signature information display is incomplete

Category: User interaction security

Content

Signed via Wallet Connect, full, readable signature information not shown.





Solution

It is recommended to display complete and readable signature information when signing.

Status

Confirmed

[N10] [Suggestion] Insufficient backup and recovery authentication

Category: Secret key backup security audit

Content

When a user loses their old device and attempts to recover their MPC wallet account on a new device, the current authentication relies on OKX exchange account verification and cloud-based account authentication. However, this method cannot guarantee that the recovery process is performed by the wallet owner themselves.

Solution

It is recommended to incorporate biometric authentication, such as facial recognition, to ensure that the recovery is done by the wallet creator.

Status

Confirmed

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002306060002	SlowMist Security Team	2023.05.16 - 2023.06.06	Low Risk

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 suggestions and 1 low risk. All the findings have been confirmed.

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