Wallet Application Security Audit Report

Table Of Contents

1 Executive Summary

On 2025.01.08, the SlowMist security team received the Safeheron team's security audit application for Safeheron App (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 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

3 Project Overview

3.1 Project Introduction

Audit Version

iOS

DownLink: https://apps.apple.com/us/app/safeheron-crypto-mpc-wallet/id1627480889

Version: 1.5.1

Sha256 Sum: ddebafdab1397b98dfffb12f425ca6928904c4ed133d4036a157eef17e98901c

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	App Runtime Environment issue	App runtime environment detection	Suggestion	Acknowledged
N2	Code Decompilation issue	Code decompilation detection	Suggestion	Acknowledged
N3	Missing Signature Verification for File Upload Requests	Business security audit	Suggestion	Acknowledged
N4	Missing Signature Verification for AML Query Requests	Business security audit	Suggestion	Fixed
N5	Secret Key Destruction issue	Secret key destruction security audit	Suggestion	Acknowledged
N6	Screenshot/screen recording issue	Screenshot/screen recording detection	Suggestion	Acknowledged
N7	Paste copy issue	Paste copy detection	Suggestion	Acknowledged
N8	Keyboard Keystroke Cache issue	Keyboard keystroke cache detection	Suggestion	Acknowledged
N9	Background obfuscation issue	Background obfuscation detection	Suggestion	Acknowledged
N10	User interaction issue	User interaction security	Suggestion	Acknowledged

3.3 Vulnerability Summary

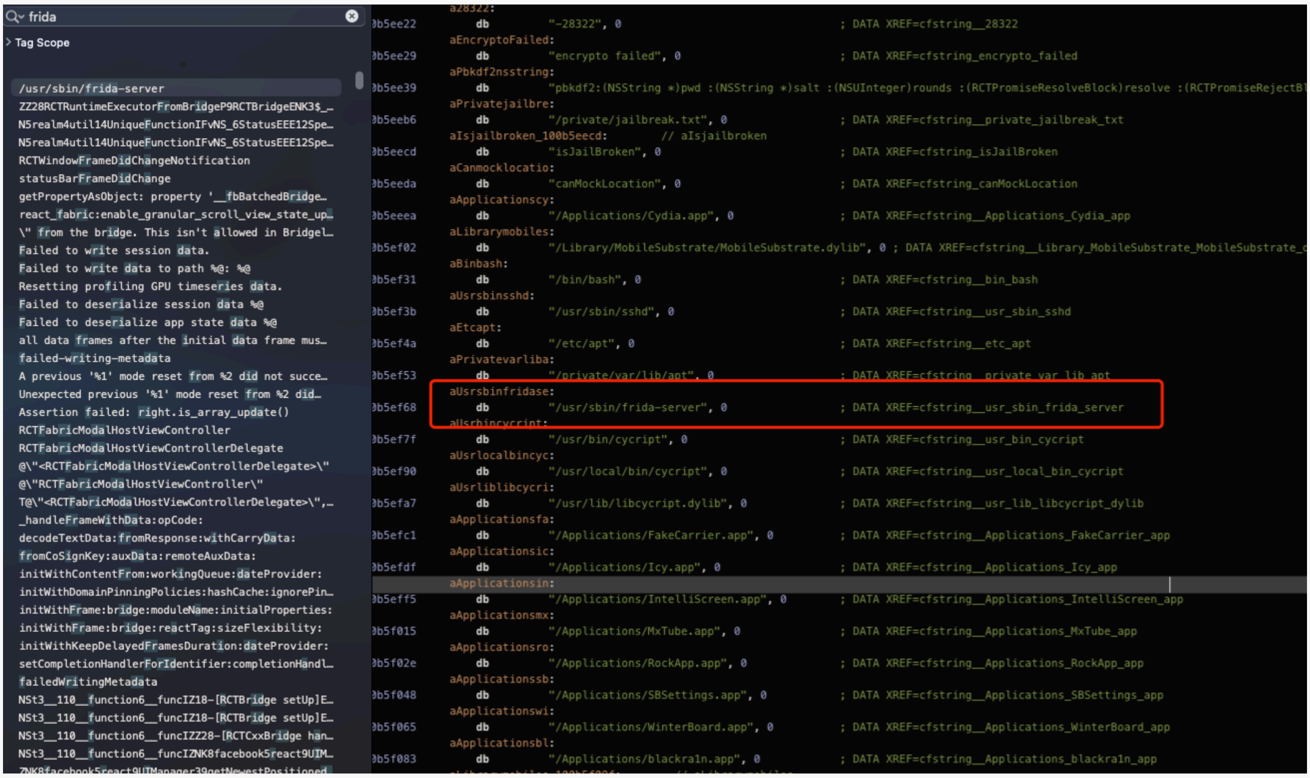
[N1] [Suggestion] App Runtime Environment issue

Category: App runtime environment detection

Content

About Hook Detection

In the decompiled code, we found checks for the existence of the @"/usr/sbin/frida-server" path. Beyond Frida, it also checks for dynamic libraries and performs Fork detection, which to some extent covers Hook detection. However, this logic is part of the user's jailbreak detection mechanism, and there isn't actually any separate real-time detection of Hooks during runtime.



```
/usr/sbin/frida-server
ZZ28RCTRuntimeExecutorFromBridgeP9RCTBridgeENK3$_…
N5realm4util14UniqueFunctionIFvNS_6StatusEEE12Spe…
N5realm4util14UniqueFunctionIFvNS_6StatusEEE12Spe…
RCTWindowFrameDidChangeNotification
statusBarFrameDidChange
getPropertyAsObject: property '__fbBatchedBridge…
react_fabric:enable_granular_scroll_view_state_up…
\" from the bridge. This isn't allowed in Bridgel…
Failed to write session data.
Failed to write data to path %@: %@
Resetting profiling GPU timeseries data.
Failed to deserialize session data %@
Failed to deserialize app state data %@
all data frames after the initial data frame mus…
failed-writing-metadata
A previous '%1' mode reset from %2 did not succe…
Unexpected previous '%1' mode reset from %2 did…
Assertion failed: right.is_array_update()
RCTFabricModalHostViewController
RCTFabricModalHostViewControllerDelegate
@\"<RCTFabricModalHostViewControllerDelegate>\"
@\"RCTFabricModalHostViewController\"
T@\"<RCTFabricModalHostViewControllerDelegate>\",…
_handleFrameWithData:opCode:
decodeTextData:fromResponse:withCarryData:
fromCoSignKey:auxData:remoteAuxData:
initWithContentFrom:workingQueue:dateProvider:
initWithDomainPinningPolicies:hashCache:ignorePin…
initWithFrame:bridge:moduleName:initialProperties:
initWithFrame:bridge:reactTag:sizeFlexibility:
initWithKeepDelayedFramesDuration:dateProvider:
setCompletionHandlerForIdentifier:completionHandl…
failedWritingMetadata
NSt3__110__function6__funcIZ18-[RCTBridge setUp]E…
NSt3__110__function6__funcIZ18-[RCTBridge setUp]E…
NSt3__110__function6__funcIZZ28-[RCTCxxBridge han…
NSt3__110__function6__funcIZNK8facebook5react9UIM…
ZNK8facebook5react9UIManager39getNewestPositioned…
```

```
        a28322:
b5ee22      db      "-28322", 0                 ; DATA XREF=cfstring__28322
        aEncryptoFailed:
b5ee29      db      "encrypto failed", 0        ; DATA XREF=cfstring_encrypto_failed
        aPbkdf2nsstring:
b5ee39      db      "pbkdf2:(NSString *)pwd :(NSString *)salt :(NSUInteger)rounds :(RCTPromiseResolveBlock)resolve :(RCTPromiseRejectBl
        aPrivatejailbre:
b5eeb6      db      "/private/jailbreak.txt", 0     ; DATA XREF=cfstring__private_jailbreak_txt
        aIsjailbroken_100b5eecd:        // aIsjailbroken
b5eecd      db      "isJailBroken", 0           ; DATA XREF=cfstring_isJailBroken
        aCanmocklocatio:
b5eeda      db      "canMockLocation", 0        ; DATA XREF=cfstring_canMockLocation
        aApplicationscy:
b5eeea      db      "/Applications/Cydia.app", 0    ; DATA XREF=cfstring__Applications_Cydia_app
        aLibrarymobiles:
b5ef02      db      "/Library/MobileSubstrate/MobileSubstrate.dylib", 0 ; DATA XREF=cfstring__Library_MobileSubstrate_MobileSubstrate_d
        aBinbash:
b5ef31      db      "/bin/bash", 0              ; DATA XREF=cfstring__bin_bash
        aUsrsbinsshd:
b5ef3b      db      "/usr/sbin/sshd", 0         ; DATA XREF=cfstring__usr_sbin_sshd
        aEtcapt:
b5ef4a      db      "/etc/apt", 0               ; DATA XREF=cfstring__etc_apt
        aPrivatevarliba:
b5ef53      db      "/private/var/lib/apt", 0   ; DATA XREF=cfstring__private_var_lib_apt
        aUsrsbinfridase:
b5ef68      db      "/usr/sbin/frida-server", 0     ; DATA XREF=cfstring__usr_sbin_frida_server
        aUsrbincycript:
b5ef7f      db      "/usr/bin/cycript", 0       ; DATA XREF=cfstring__usr_bin_cycript
        aUsrlocalbincyc:
b5ef90      db      "/usr/local/bin/cycript", 0     ; DATA XREF=cfstring__usr_local_bin_cycript
        aUsrliblibcycri:
b5efa7      db      "/usr/lib/libcycript.dylib", 0  ; DATA XREF=cfstring__usr_lib_libcycript_dylib
        aApplicationsfa:
b5efc1      db      "/Applications/FakeCarrier.app", 0  ; DATA XREF=cfstring__Applications_FakeCarrier_app
        aApplicationsic:
b5efdf      db      "/Applications/Icy.app", 0      ; DATA XREF=cfstring__Applications_Icy_app
        aApplicationsin:
b5eff5      db      "/Applications/IntelliScreen.app", 0    ; DATA XREF=cfstring__Applications_IntelliScreen_app
        aApplicationsmx:
b5f015      db      "/Applications/MxTube.app", 0   ; DATA XREF=cfstring__Applications_MxTube_app
        aApplicationsro:
b5f02e      db      "/Applications/RockApp.app", 0  ; DATA XREF=cfstring__Applications_RockApp_app
        aApplicationssb:
b5f048      db      "/Applications/SBSettings.app", 0   ; DATA XREF=cfstring__Applications_SBSettings_app
        aApplicationswi:
b5f065      db      "/Applications/WinterBoard.app", 0  ; DATA XREF=cfstring__Applications_WinterBoard_app
        aApplicationsbl:
b5f083      db      "/Applications/blackra1n.app", 0    ; DATA XREF=cfstring__Applications_blackra1n_app
```

Solution

It is also recommended to include detection for common hooking frameworks, such as Frida, in the checks and issue warnings accordingly.

Reference: https://web.archive.org/web/20181227120751/http://www.vantagepoint.sg/blog/90-the-jiu-jitsu-of-detecting-frida

Status

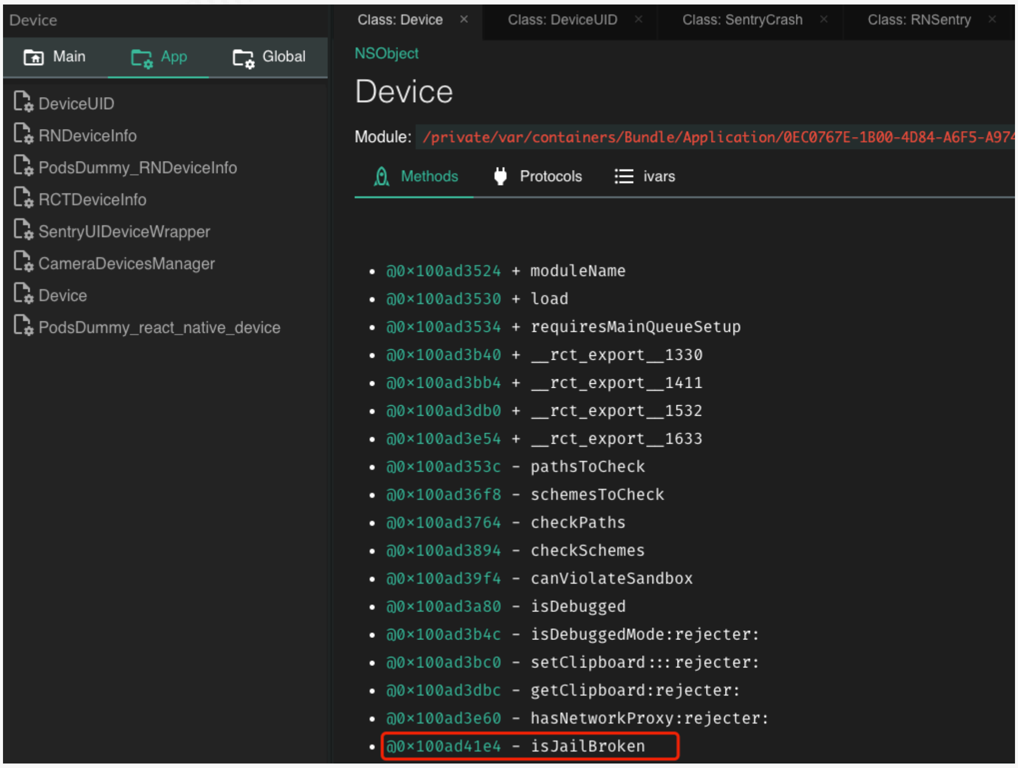
Acknowledged

[N2] [Suggestion] Code Decompilation issue

Category: Code decompilation detection

Content

During actual testing, we couldn't access the App's header file information, but by decompiling the binary file, we were able to discover relevant function information.



DeviceUID
RNDeviceInfo
PodsDummy_RNDeviceInfo
RCTDeviceInfo
SentryUIDeviceWrapper
CameraDevicesManager
Device
PodsDummy_react_native_device

NSObject

Device

Module: /private/var/containers/Bundle/Application/0EC0767E-1B00-4D84-A6F5-A974

```
• @0×100ad3524 + moduleName
• @0×100ad3530 + load
• @0×100ad3534 + requiresMainQueueSetup
• @0×100ad3b40 + __rct_export__1330
• @0×100ad3bb4 + __rct_export__1411
• @0×100ad3db0 + __rct_export__1532
• @0×100ad3e54 + __rct_export__1633
• @0×100ad353c - pathsToCheck
• @0×100ad36f8 - schemesToCheck
• @0×100ad3764 - checkPaths
• @0×100ad3894 - checkSchemes
• @0×100ad39f4 - canViolateSandbox
• @0×100ad3a80 - isDebugged
• @0×100ad3b4c - isDebuggedMode:rejecter:
• @0×100ad3bc0 - setClipboard:::rejecter:
• @0×100ad3dbc - getClipboard:rejecter:
• @0×100ad3e60 - hasNetworkProxy:rejecter:
• @0×100ad41e4 - isJailBroken
```

Solution

It is recommended to obfuscate your code before packaging the app to increase the cost of decompilation.

For reference, you can check out:

https://github.com/chenxiancai/STCObfuscator

https://github.com/housenkui/HSKConfuse

Status

Acknowledged

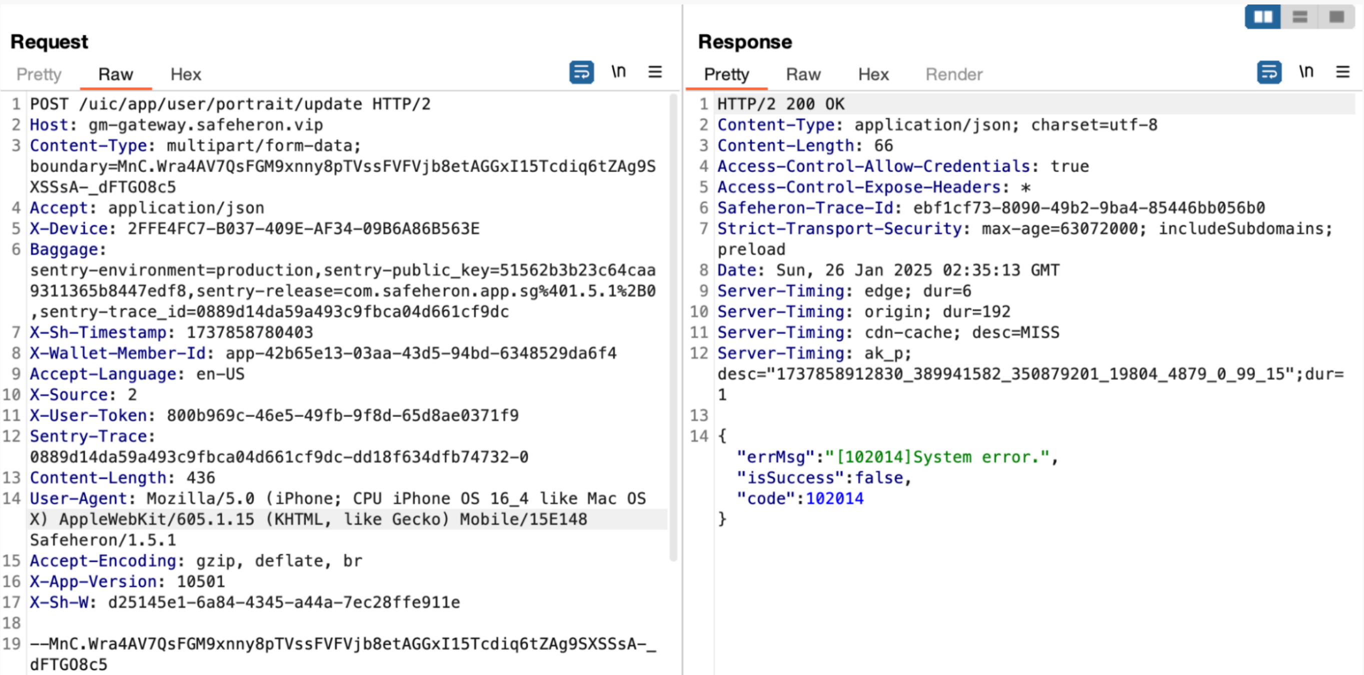
[N3] [Suggestion] Missing Signature Verification for File Upload Requests

Category: Business security audit

Content

When replaying an upload request for the profile picture in Personal Info under normal circumstances, the server responds with: "[102014]System error."

The upload interface is: "https://gm-gateway.safeheron.vip/uic/app/user/portrait/update".



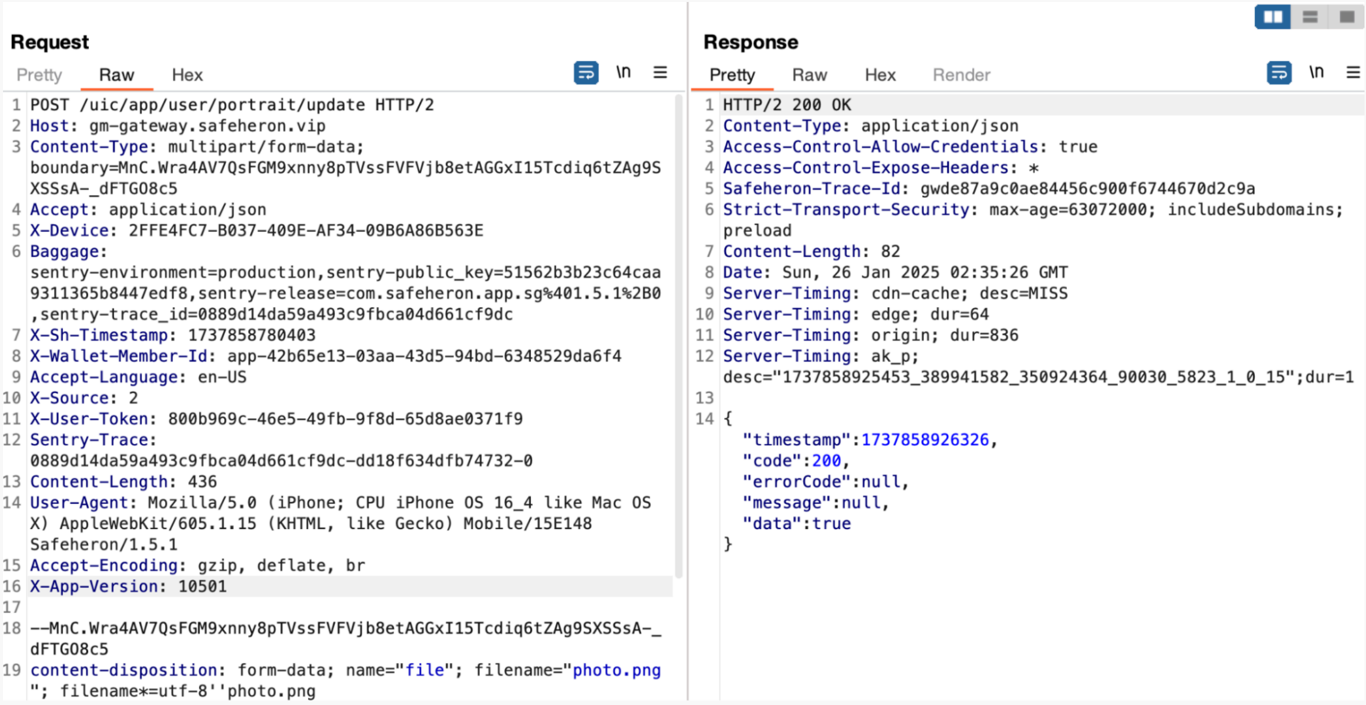
```
POST /uic/app/user/portrait/update HTTP/2
Host: gm-gateway.safeheron.vip
Content-Type: multipart/form-data;
boundary=MnC.Wra4AV7QsFGM9xnny8pTVssFVFVjb8etAGGxI15Tcdiq6tZAg9S
XSSsA-_dFTG08c5
Accept: application/json
X-Device: 2FFE4FC7-B037-409E-AF34-09B6A86B563E
Baggage:
sentry-environment=production,sentry-public_key=51562b3b23c64caa
9311365b8447edf8,sentry-release=com.safeheron.app.sg%401.5.1%2B0
,sentry-trace_id=0889d14da59a493c9fbca04d661cf9dc
X-Sh-Timestamp: 1737858780403
X-Wallet-Member-Id: app-42b65e13-03aa-43d5-94bd-6348529da6f4
Accept-Language: en-US
X-Source: 2
X-User-Token: 800b969c-46e5-49fb-9f8d-65d8ae0371f9
Sentry-Trace:
0889d14da59a493c9fbca04d661cf9dc-dd18f634dfb74732-0
Content-Length: 436
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_4 like Mac OS
X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148
Safeheron/1.5.1
Accept-Encoding: gzip, deflate, br
X-App-Version: 10501
X-Sh-W: d25145e1-6a84-4345-a44a-7ec28ffe911e

--MnC.Wra4AV7QsFGM9xnny8pTVssFVFVjb8etAGGxI15Tcdiq6tZAg9SXSSsA-_
dFTG08c5
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 66
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: ebf1cf73-8090-49b2-9ba4-85446bb056b0
Strict-Transport-Security: max-age=63072000; includeSubdomains;
preload
Date: Sun, 26 Jan 2025 02:35:13 GMT
Server-Timing: edge; dur=6
Server-Timing: origin; dur=192
Server-Timing: cdn-cache; desc=MISS
Server-Timing: ak_p;
desc="1737858912830_389941582_350879201_19804_4879_0_99_15";dur=
1

{
  "errMsg":"[102014]System error.",
  "isSuccess":false,
  "code":102014
}
```

After removing the X-Sh-W-Sig and X-Sh-W header fields from the HTTP POST request, the upload succeeds.



```
POST /uic/app/user/portrait/update HTTP/2
Host: gm-gateway.safeheron.vip
Content-Type: multipart/form-data;
boundary=MnC.Wra4AV7QsFGM9xnny8pTVssFVFVjb8etAGGxI15Tcdiq6tZAg9S
XSSsA-_dFTG08c5
Accept: application/json
X-Device: 2FFE4FC7-B037-409E-AF34-09B6A86B563E
Baggage:
sentry-environment=production,sentry-public_key=51562b3b23c64caa
9311365b8447edf8,sentry-release=com.safeheron.app.sg%401.5.1%2B0
,sentry-trace_id=0889d14da59a493c9fbca04d661cf9dc
X-Sh-Timestamp: 1737858780403
X-Wallet-Member-Id: app-42b65e13-03aa-43d5-94bd-6348529da6f4
Accept-Language: en-US
X-Source: 2
X-User-Token: 800b969c-46e5-49fb-9f8d-65d8ae0371f9
Sentry-Trace:
0889d14da59a493c9fbca04d661cf9dc-dd18f634dfb74732-0
Content-Length: 436
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_4 like Mac OS
X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148
Safeheron/1.5.1
Accept-Encoding: gzip, deflate, br
X-App-Version: 10501

--MnC.Wra4AV7QsFGM9xnny8pTVssFVFVjb8etAGGxI15Tcdiq6tZAg9SXSSsA-_
dFTG08c5
content-disposition: form-data; name="file"; filename="photo.png
"; filename*=utf-8''photo.png
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gwde87a9c0ae84456c900f6744670d2c9a
Strict-Transport-Security: max-age=63072000; includeSubdomains;
preload
Content-Length: 82
Date: Sun, 26 Jan 2025 02:35:26 GMT
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=64
Server-Timing: origin; dur=836
Server-Timing: ak_p;
desc="1737858925453_389941582_350924364_90030_5823_1_0_15";dur=1

{
  "timestamp":1737858926326,
  "code":200,
  "errorCode":null,
  "message":null,
  "data":true
}
```

Solution

It is recommended to implement signature verification for profile picture upload requests in the personal information section.

Status

Acknowledged

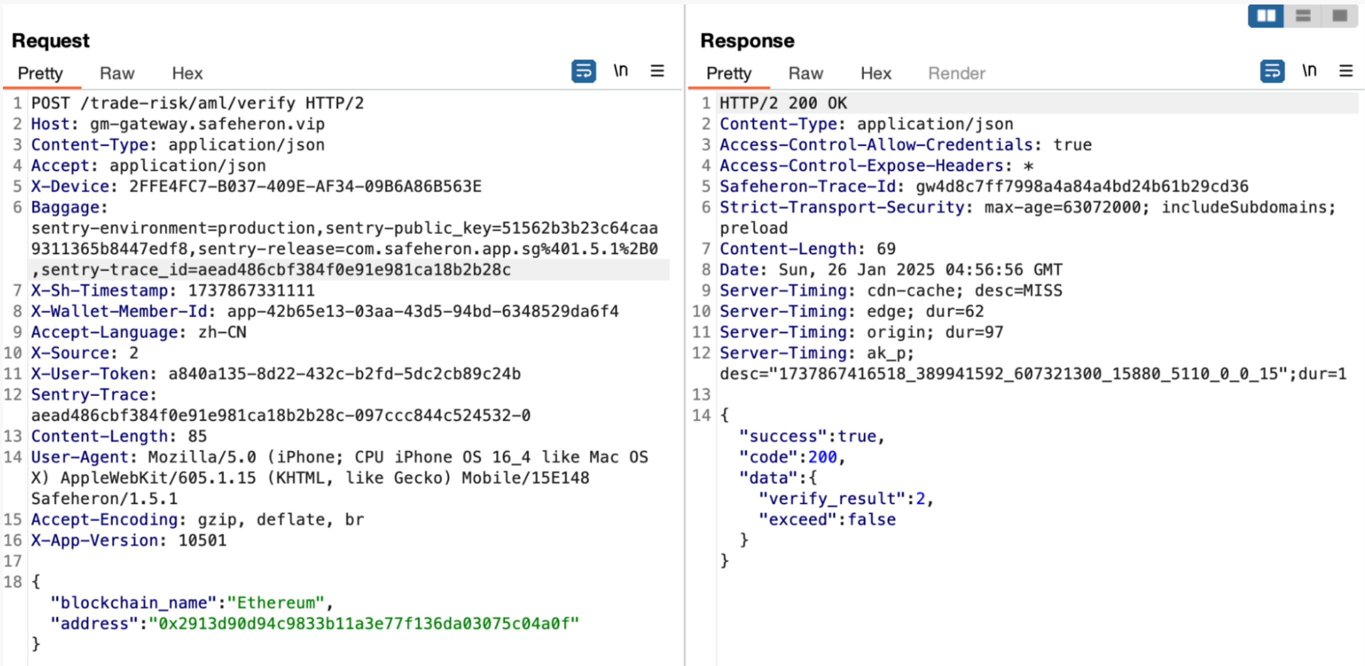
[N4] [Suggestion] Missing Signature Verification for AML Query Requests

Category: Business security audit

Content

At the AML query interface, queries can still be performed after removing the X-Sh-W-Sig and X-Sh-W fields.

The query interface is: https://gm-gateway.safeheron.vip/trade-risk/aml/verify



```
POST /trade-risk/aml/verify HTTP/2
Host: gm-gateway.safeheron.vip
Content-Type: application/json
Accept: application/json
X-Device: 2FFE4FC7-B037-409E-AF34-09B6A86B563E
Baggage:
sentry-environment=production,sentry-public_key=51562b3b23c64caa
9311365b8447edf8,sentry-release=com.safeheron.app.sg%401.5.1%2B0
,sentry-trace_id=aead486cbf384f0e91e981ca18b2b28c
X-Sh-Timestamp: 1737867331111
X-Wallet-Member-Id: app-42b65e13-03aa-43d5-94bd-6348529da6f4
Accept-Language: zh-CN
X-Source: 2
X-User-Token: a840a135-8d22-432c-b2fd-5dc2cb89c24b
Sentry-Trace:
aead486cbf384f0e91e981ca18b2b28c-097ccc844c524532-0
Content-Length: 85
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_4 like Mac OS
X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148
Safeheron/1.5.1
Accept-Encoding: gzip, deflate, br
X-App-Version: 10501

{
  "blockchain_name":"Ethereum",
  "address":"0x2913d90d94c9833b11a3e77f136da03075c04a0f"
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gw4d8c7ff7998a4a84a4bd24b61b29cd36
Strict-Transport-Security: max-age=63072000; includeSubdomains;
preload
Content-Length: 69
Date: Sun, 26 Jan 2025 04:56:56 GMT
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=62
Server-Timing: origin; dur=97
Server-Timing: ak_p;
desc="1737867416518_389941592_607321300_15880_5110_0_0_15";dur=1

{
  "success":true,
  "code":200,
  "data":{
    "verify_result":2,
    "exceed":false
  }
}
```

Solution

It is recommended to add signature verification to the AML query interface to prevent misuse of the API.

Status

Fixed; Currently, the AML query interface limits the number of access attempts per session.

[N5] [Suggestion] Secret Key Destruction issue

Category: Secret key destruction security audit

Content

When logging out and logging back into the App, you don't need to import your local mnemonic phrase as it isn't deleted.

Only uninstalling the App will completely remove the local mnemonic phrase information.

Solution

It is recommended to delete the locally stored mnemonic phrase shard information when logging out.

Status

Acknowledged

[N6] [Suggestion] Screenshot/screen recording issue

Category: Screenshot/screen recording detection

Content

The sensitive information page has a security reminder asking users not to take screenshots, but it doesn't actually detect or block system screenshots or screen recordings.

Solution

It is recommended that the App detect whether the system is currently taking screenshots or recording the screen, and block these actions.

Status

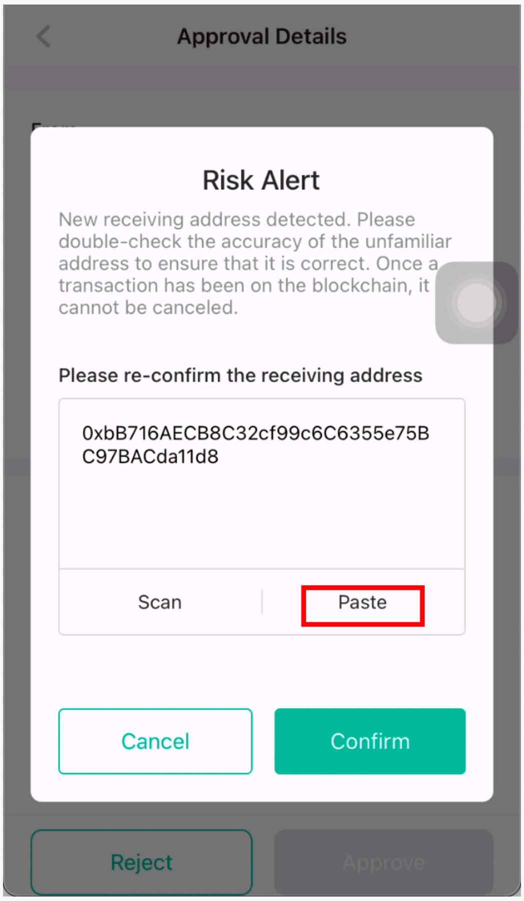
Acknowledged

[N7] [Suggestion] Paste copy issue

Category: Paste copy detection

Content

When copying sensitive information, there's a copy notification, but the clipboard isn't cleared promptly after pasting is completed.



Approval Details

Risk Alert

New receiving address detected. Please double-check the accuracy of the unfamiliar address to ensure that it is correct. Once a transaction has been on the blockchain, it cannot be canceled.

Please re-confirm the receiving address

0xbB716AECB8C32cf99c6C6355e75BC97BACda11d8

Solution

It is recommended to clear the clipboard promptly after copying and pasting is completed.

Status

Acknowledged

[N8] [Suggestion] Keyboard Keystroke Cache issue

Category: Keyboard keystroke cache detection

Content

The App uses the system's built-in keyboard rather than a custom keyboard.

Solution

It is recommended to integrate a secure keyboard function into the App to prevent third-party keyboards from capturing input information.

Status

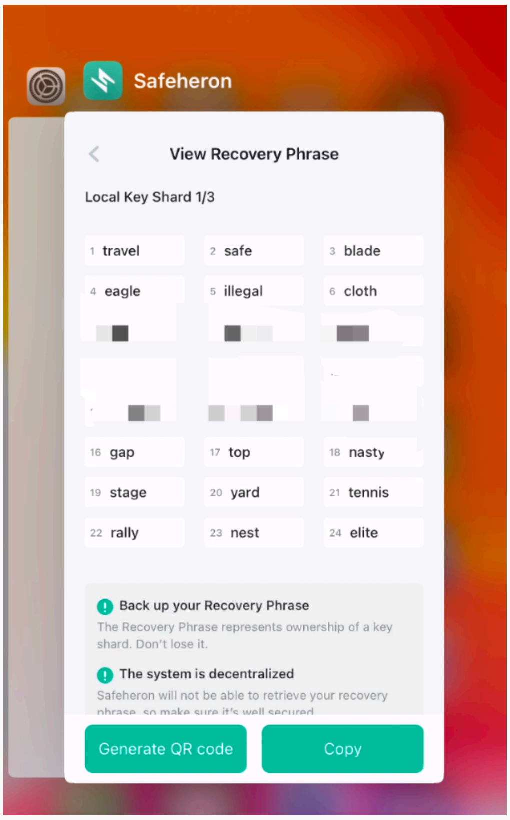
Acknowledged

[N9] [Suggestion] Background obfuscation issue

Category: Background obfuscation detection

Content

When the wallet app is suspended in the background, the interface isn't masked or blurred, allowing other apps to potentially read the screen content.



View Recovery Phrase

Local Key Shard 1/3

1 travel	2 safe	3 blade
4 eagle	5 illegal	6 cloth
[redacted]	[redacted]	[redacted]
16 gap	17 top	18 nasty
19 stage	20 yard	21 tennis
22 rally	23 nest	24 elite

Back up your Recovery Phrase
The Recovery Phrase represents ownership of a key shard. Don't lose it.

The system is decentralized
Safeheron will not be able to retrieve your recovery phrase, so make sure it's well secured

Solution

It is recommended to detect when the App is suspended and apply blurring effects, which can effectively prevent other apps from reading sensitive information during app switching.

Status

Acknowledged

[N10] [Suggestion] User interaction issue

Category: User interaction security

Content

Functionality	Support	Notes
WYSIWYS	✓	Approving a transaction will display the complete transaction details.

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

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

Solution

It is recommended to improve the related user interactions.

Status

Acknowledged

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002502250003	SlowMist Security Team	2025.01.08 - 2025.02.25	Passed

Summary conclusion: The SlowMist security team employs a manual approach along with the SlowMist team's analysis tool to conduct an audit of the project. During the audit process, ten suggestions were identified. Additionally, one suggestion have been fixed. All other 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.

SLOWMIST

Official Website

www.slowmist.com

✉

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist