Browser Extension Wallet 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 extension, 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 browser extension wallet 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 browser extension wallets are manually analyzed to look for any potential issues.

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

- Transfer security
    - Signature security audit
    - Deposit/Transfer security audit
    - Transaction broadcast security audit
- Secret key security
    - Secret key generation security audit
    - Secret key storage security audit
    - Secret key usage security audit
    - Secret key backup security audit
    - Secret key destruction security audit
    - Random generator security audit
    - Cryptography security audit
- Web front-end security
    - Cross-Site Scripting security audit
    - Third-party JS security audit
    - HTTP response header security audit
- Communication security
    - Communication encryption security audit
    - Cross-domain transmission security audit
- Architecture and business logic security
    - Access control security audit

- Wallet lock security audit
- Business design security audit
- Architecture design security audit
- Denial of Service security audit

3 Project Overview

3.1 Project Introduction

Audit scope

Chrome Extension

Link：https://chrome.google.com/webstore/detail/safeheron/aiaghdjafpiofpainifbgfgjfpclngoh

Version: 0.1.4

Shasum (Safeheron-Chrome-Web-Store.crx):

f6ebbccef868f285c963fc1c2188fbb564c5a4d4179fe09d62165e447cb4fa67

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Cross-domain transmission issue	Cross-domain transmission security audit	Suggestion	Fixed
N2	Wallet lock issue	Wallet lock security audit	Suggestion	Acknowledged
N3	Missing Token Session Timeout Design	Business design security audit	Suggestion	Acknowledged

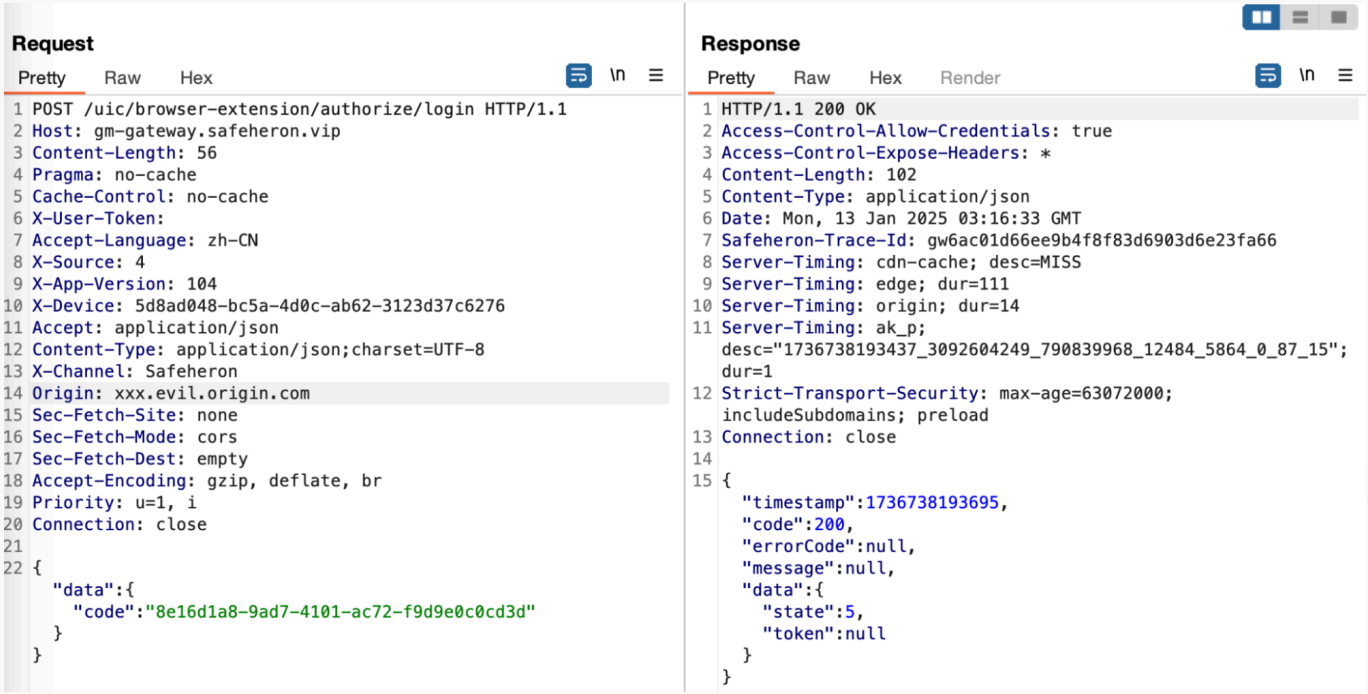
3.3 Vulnerability Summary

[N1] [Suggestion] Cross-domain transmission issue

Category: Cross-domain transmission security audit

Content

The API initiates requests without verifying the source of the Origin.



Request

Pretty Raw Hex

```
1 POST /uic/browser-extension/authorize/login HTTP/1.1
2 Host: gm-gateway.safeheron.vip
3 Content-Length: 56
4 Pragma: no-cache
5 Cache-Control: no-cache
6 X-User-Token:
7 Accept-Language: zh-CN
8 X-Source: 4
9 X-App-Version: 104
10 X-Device: 5d8ad048-bc5a-4d0c-ab62-3123d37c6276
11 Accept: application/json
12 Content-Type: application/json;charset=UTF-8
13 X-Channel: Safeheron
14 Origin: xxx.evil.origin.com
15 Sec-Fetch-Site: none
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=1, i
20 Connection: close
21
22 {
  "data":{
    "code":"8e16d1a8-9ad7-4101-ac72-f9d9e0c0cd3d"
  }
}
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Credentials: true
3 Access-Control-Expose-Headers: *
4 Content-Length: 102
5 Content-Type: application/json
6 Date: Mon, 13 Jan 2025 03:16:33 GMT
7 Safeheron-Trace-Id: gw6ac01d66ee9b4f8f83d6903d6e23fa66
8 Server-Timing: cdn-cache; desc=MISS
9 Server-Timing: edge; dur=111
10 Server-Timing: origin; dur=14
11 Server-Timing: ak_p;
desc="1736738193437_3092604249_790839968_12484_5864_0_87_15";
dur=1
12 Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
13 Connection: close
14
15 {
  "timestamp":1736738193695,
  "code":200,
  "errorCode":null,
  "message":null,
  "data":{
    "state":5,
    "token":null
  }
}
```

Solution

It is recommended to configure an Origin whitelist, allowing access only from addresses within the approved list.

Status

Fixed

[N2] [Suggestion] Wallet lock issue

Category: Wallet lock security audit

Content

The Extension doesn't have a locking feature. Session tokens are stored in variables and won't be logged out unless the browser is closed or the plugin is restarted.

Solution

It is recommended to add a locking feature to prevent malicious submission of signature approvals.

Status

Acknowledged

[N3] [Suggestion] Missing Token Session Timeout Design

Category: Business design security audit

Content

After authentication through App QR code scanning, the plugin issues a Token session. Token information is stored in global variables this.tokenState.userToken or this.token.

During testing, we found that when the browser remained open (testing period exceeded 72 hours), the session did not expire. This reveals that there's no definite timeout setting for sessions.

There's no session expiration configuration in the extension settings.

Solution

It is recommended to set a default expiration time for sessions to prevent them from remaining valid after extended periods of extension inactivity.

Status

Acknowledged

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002502250002	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, three suggestions were identified. Additionally, one suggestions 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.

Official Website

www.slowmist.com

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist