Browser Extension Wallet Security Audit Report

Table Of Contents

1 Executive Summary

On 2022.11.07, the SlowMist security team received the frontier team's security audit application for frontier-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/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.

Level	Description
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 Version

https://github.com/frontierdotxyz/frontier-extension

commit hash: 5520df2ab625f264131b5621834204b72c782bf9

Fixed Version

commit hash: 8060a25e62ec9049c64625bca81e73a5f8f3951d

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Account information is stored unencrypted	Others	Low	Fixed
N2	Signature source not reminded	Signature security audit	Low	Fixed
N3	manifest.json allows extensions to be used in all mode	Access control security audit	Suggestion	Fixed
N4	Add contact address can be any string	Architecture design security audit	Low	Fixed
N5	Failed to export mnemonic phrase after changing wallet password	Secret key backup security audit	Low	Fixed

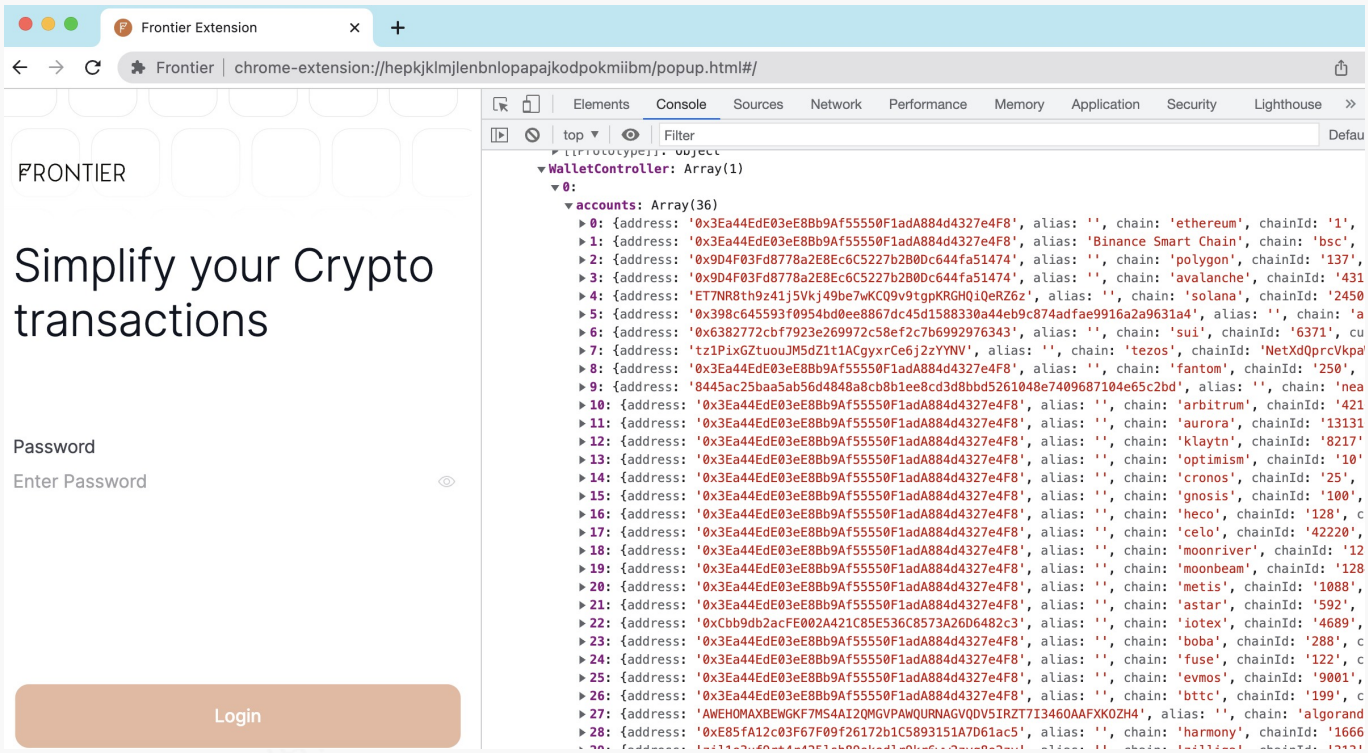
3.3 Vulnerability Summary

[N1] [Low] Account information is stored unencrypted

Category: Others

Content

The basic information of wallet account is stored in chrome.storage.local without encrypted storage and timely update, so you can use `chrome.storage.local.set` to modify the payment address of the wallet.



Solution

It is recommended that the basic address information of the wallet should be updated in time, and the better way is to store it encrypted.

Status

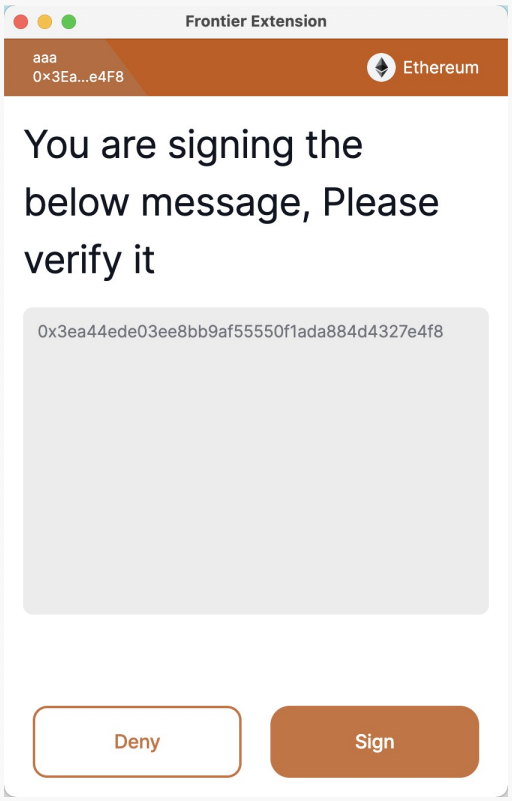
Fixed

[N2] [Low] Signature source not reminded

Category: Signature security audit

Content

When interacting with the DApp, Frontier does not reveal the DApp domain origin of the request signature, which makes it easy for users to be confused.



- src/pages/approvals/container/PrivateSign.tsx#line61-91

```
<div className="relative flex flex-col h-screen">
            <ApprovalsHeader {...walletDetail} />

            <div className="grow relative">
                <div className="px-4 py-4 pb-4">
                    <h1 className=" leading-12 mr-4 heading2">
                        {translate("approvals.signMessageConsent")}
                    </h1>
                </div>
                <div className="bg-neutral-50 dark:bg-neutralDark-100 mx-4 p-3 max-h-
64 min-h-[256px] rounded-lg overflow-y-auto hide-scrollbar">
                    <p
                        className={`label3 break-all text-text-500 dark:text-
textDark-700 text-sm whitespace-pre-line`}
                    >
                        {typeof params?.decodedMessage === "string"
                            ? params.decodedMessage
                            : JSON.stringify(params?.decodedMessage, null, "\t")}
                    </p>
                </div>
            </div>
```

```
            <div className="px-6 pt-8 pb-4">
                <div className="mt-10">
                    <ApprovalsGroupButtons
                        leftBtnName={translate("approvals.groupDenyButton")}
                        rightBtnName={translate("approvals.groupSignButton")}
                        rightOnClick={handleSuccess}
                        leftOnClick={handleCancel}
                    />
                </div>
            </div>
        </div>
```

Solution

It is recommended to display the signed domain origin when interacting with the DApp.

Status

Fixed

[N3] [Suggestion] manifest.json allows extensions to be used in all mode

Category: Access control security audit

Content

Configuration in manifest.json:

```
"content_scripts": [
  {
    "js": [
      "assets/content-script-loader.content.801468f9.js"
    ],
    "matches": [
      "<all_urls>"
    ],
    "run_at": "document_start",
    "all_frames": true
  }
```

Allowing all url protocols, such as HTTP protocol, is easy to expand the attack surface of man-in-the-middle hijacking. It is recommended not to support it. It is recommended to only allow it in the HTTPS domain.

Solution

Allowing all url protocols, such as HTTP protocol, is easy to expand the attack surface of man-in-the-middle hijacking. It is recommended not to support it. It is recommended to only allow it in the HTTPS domain.

Status

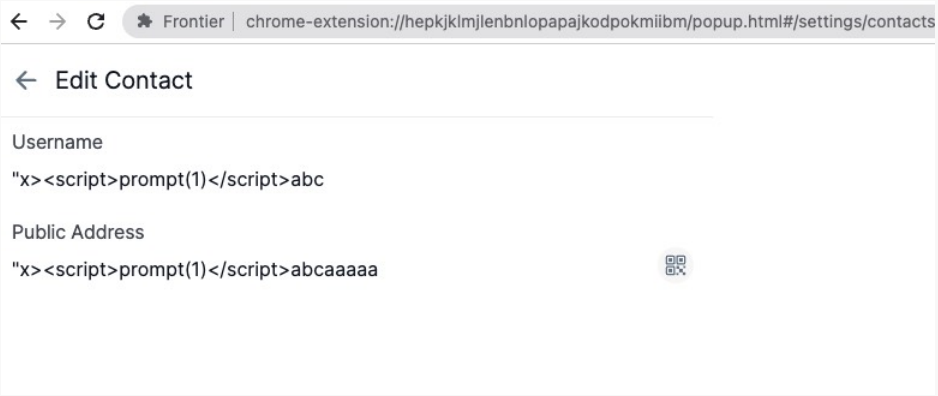
Fixed

[N4] [Low] Add contact address can be any string

Category: Architecture design security audit

Content

When adding a contact address, the address format is not verified, and any character string can be added.



Solution

Any input needs to be strictly checked to avoid the possibility of risk during context parsing.

Status

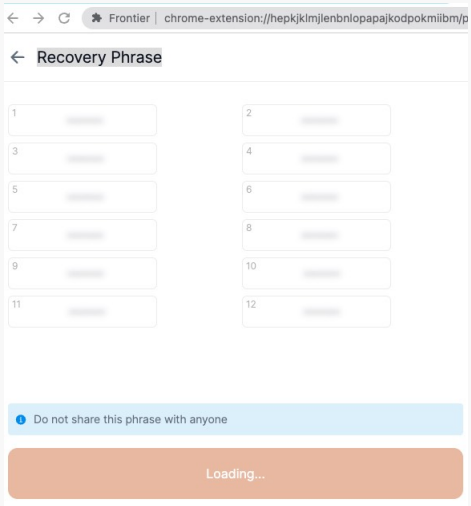
Fixed

[N5] [Low] Failed to export mnemonic phrase after changing wallet password

Category: Secret key backup security audit

Content

Failed to export mnemonic phrase after changing wallet password.



Solution

After changing the wallet password, the mnemonic information should be re-encrypted with the new password.

Status

Fixed

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002211160001	SlowMist Security Team	2022.11.07 - 2022.11.16	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 4 low risk, 1 suggestion vulnerabilities. And all findings were comfirmed fixed.We extend our gratitude for frontier-extension 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