Snap Application Security Audit Report

Table Of Contents

1 Executive Summary

On 2024.05.06, the SlowMist security team received the FinTax team's security audit application for fintax-snap, 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 the 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 application is manually analyzed to look for any potential issues.

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

Serial Number.	Audit Items
1	Snaps user interface security audit
2	Snaps permissions security audit
3	Insecure entropy source audit
4	Cryptography security audit
5	Cross-Site Scripting security audit
6	Third-party components security audit
7	Communication encryption security audit
8	Business design security audit
9	Architecture design security audit
13	Web API security audit
14	DNSSEC security audit
15	SSL/TLS security audit

3 Project Overview

3.1 Project Introduction

A professional tool for managing crypto asset taxes and finance.

Audit Version

Project Address: https://github.com/InTaxDev/fintax-snap/invitations

Commit: 3c37ce4a3d2c7c81f3724dec5771a30f8a4dc420

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Snap permissions information	Others	Information	Confirmed
N2	DNSSEC Not Configured	DNSSEC security audit	Suggestion	Fixed

3.3 Vulnerability Summary

[N1] [Information] Snap permissions information

Category: Others

Content

This snap only uses the following two permissions, and no over-authorization issue wes found.

Code location: Code location: fintax-snap/snap.manifest.json #L19-27

```
"initialPermissions": {
  "endowment:network-access": {},
  "snap_manageState": {},
  "endowment:rpc": {
    "dapps": true,
    "snaps": false
  },
  "endowment:ethereum-provider": {}
}
```

Solution

N/A

Status

Confirmed

[N2] [Suggestion] DNSSEC Not Configured

Category: DNSSEC security audit

Content

We checked the interfaces used by snap and found that DNSSEC is not configured.

.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
com	Found 1 DS records for com in the . zone DS=19718/SHA-256 has algorithm ECDSAP256SHA256 Found 1 RRSIGs over DS RRset RRSIG=5613 and DNSKEY=5613 verifies the DS RRset Found 2 DNSKEY records for com DS=19718/SHA-256 verifies DNSKEY=19718/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19718 and DNSKEY=19718/SEP verifies the DNSKEY RRset
thetaxdao.com	No DS records found for thetaxdao.com in the com zone No DNSKEY records found ns4.diymysite.com is authoritative for thetaxdao.com thetaxdao.com A RR has value 54.169.200.154 No RRSIGs found
thetaxdao.com	ns3.diymysite.com is authoritative for thetaxdao.com thetaxdao.com A RR has value 54.169.200.154 No RRSIGs found

DNSSEC can protect websites from the following attacks:

1. DNS spoofing: An attacker injects malicious DNS records into the DNS cache, redirecting users to malicious websites.
2. Cache poisoning: An attacker injects malicious DNS records into the DNS cache, redirecting users to malicious websites.
3. Domain hijacking: An attacker changes the DNS records of a legitimate domain to point to a malicious website.

If a domain is not configured with DNSSEC, DNS clients cannot verify the authenticity of DNS records. This makes it easier for attackers to exploit DNS attacks to deceive users or hijack websites.

Solution

It is recommended to configure DNSSEC correctly.

Status

Fixed; The project team have changed the interface domain to "https://www.fintax.tech" and completed the configuration of DNSSEC.

.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
tech	Found 2 DS records for tech in the . zone DS=50095/SHA-256 has algorithm RSASHA256 DS=28487/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=5613 and DNSKEY=5613 verifies the DS RRset Found 2 DNSKEY records for tech DS=28487/SHA-256 verifies DNSKEY=28487/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=28487 and DNSKEY=28487/SEP verifies the DNSKEY RRset
fintax.tech	Found 1 DS records for fintax.tech in the tech zone DS=54931/SHA-256 has algorithm ECDSAP256SHA256 Found 1 RRSIGs over DS RRset RRSIG=5851 and DNSKEY=5851 verifies the DS RRset Found 2 DNSKEY records for fintax.tech DS=54931/SHA-256 verifies DNSKEY=54931/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=54931 and DNSKEY=54931/SEP verifies the DNSKEY RRset vip1.alidns.com is authoritative for fintax.tech fintax.tech A RR has value 13.212.239.5 Found 1 RRSIGs over A RRset RRSIG=56113 and DNSKEY=56113 verifies the A RRset
fintax.tech	vip2.alidns.com is authoritative for fintax.tech fintax.tech A RR has value 13.212.239.5 Found 1 RRSIGs over A RRset RRSIG=56113 and DNSKEY=56113 verifies the A RRset

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002405060002	SlowMist Security Team	2024.05.06 - 2024.05.06	Passed

Summary conclusion: The SlowMist security team used a manual and SlowMist team's analysis tool to audit the project, during the audit work, we found 1 suggestion. All the issues have been fixed.

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