Snap Application Security Audit Report

Table Of Contents

1 Executive Summary

On 2023.12.18, the SlowMist security team received the ethereum-attestation-service team's security audit application for eas-metamask-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

Audit Version

Project Address:

https://github.com/ethereum-attestation-service/eas-metamask-snap

commit: 5240e42e4bac22da166fda0737f6d8a3b5b89f8c

Fixed Version

Project Address:

https://github.com/ethereum-attestation-service/eas-metamask-snap

commit: f3f5be615d318941cfabba9c784a9ee55a17f1a2

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Data cannot be parsed correctly	Others	Suggestion	Confirmed
N2	DNSSEC Not Configured	DNSSEC security audit	Suggestion	Fixed
N3	Unused permissions	Snap permissions security audit	Suggestion	Fixed

3.3 Vulnerability Summary

[N1] [Suggestion] Data cannot be parsed correctly

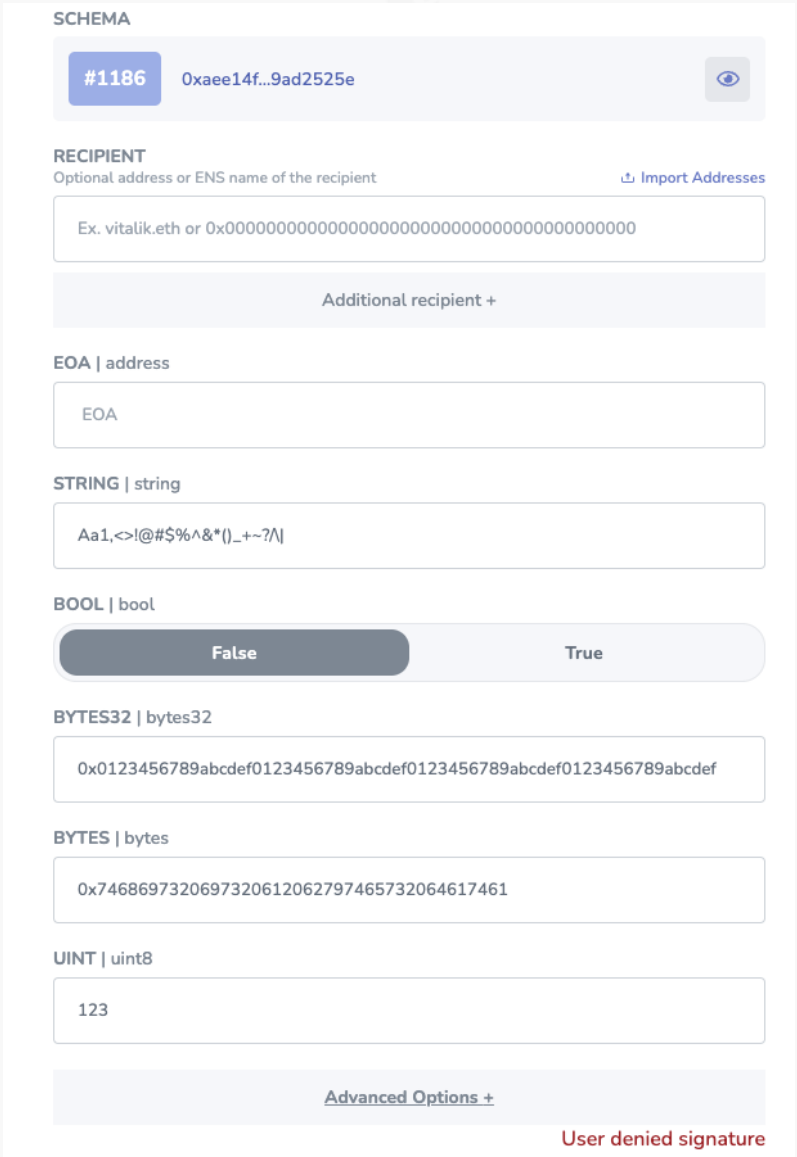
Category: Others

Content

Created a schema with the following parameters:

- address
- string
- bool

- bytes32
- bytes
- uint8



When I make a normal request, the data can be parsed correctly.

{"target":"metamask-contentscript","data":{"name":"metamask-provider","data":
{"method":"eth_sendTransaction","params":
[{"gas":"0x5f6f7","value":"0x0","from":"0x415cc25d8c5c1808051ab39187fcbbbd51f65aa6","to":"0xc2679fbd37d54388ce493f1db75320d236e1815e","data":"0xf17325e70000000000000000000000000000000000000000000000000000000000000000000000020aee14f81ad29240a77ad323c31b86407fa219a14ea56995e447ebc8e9ad2525e000000000000000000000000000000000000000000000000000000000000000400000000000000000000000000415cc25d8c5c1808051ab39187fcbbbd51f65aa60000000000000000000000000000000000000000000000000000000000000000

00000000000000000000000000000000000000000000000100000000000000000000000000000000000000000000

0000000000000000000000000000000000000000000000000000000000000000000000000000000c000000000000

000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

00000000000000000000140000000000000000000000000415cc25d8c5c1808051ab39187fcbbbd51f65aa600000000

00000000000000000000000000000000000000000000000000000c00000000000000000000000000000000000000

000000000000000000000000000123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef00000

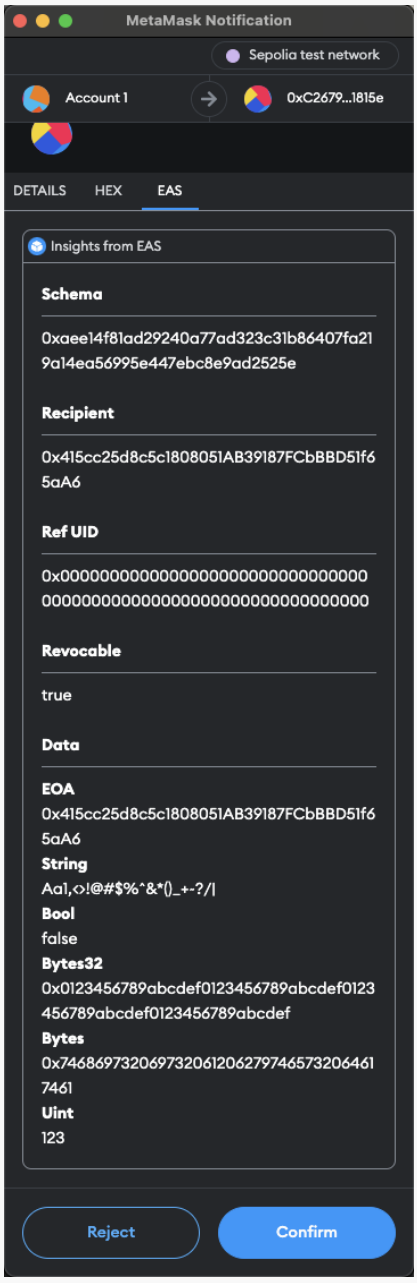
0000000000000000000000000000000000000000000000000000000100000000000000000000000000000000000

0000000000000000000000007b0000000000000000000000000000000000000000000000000000000000000000174

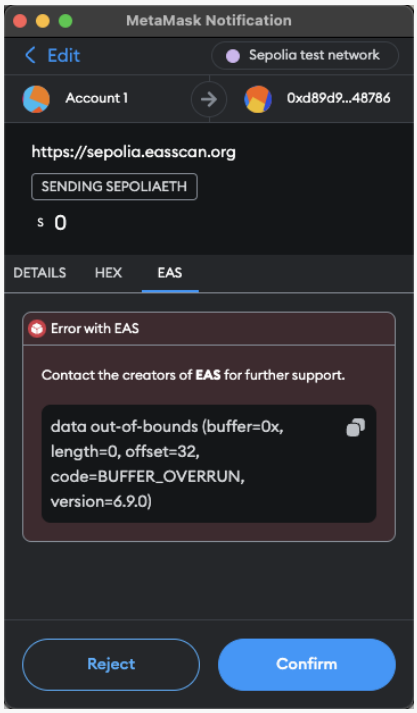
161312c3c3e21402324255e262a28295f2b7e3f2f5c7c0000000000000000000000000000000000000000000000000

00000000000000000000000000001474686973206973206120627974657320646174610000000000000000000000

00"}],"jsonrpc":"2.0","id":3606434041}}}



When the recipient address or EOA is modified to the short address "0x415cc25d8c5c1808051ab39187fcbbbd51f65a", an error message is returned instead of a message indicating that the recipient address or EOA format is incorrect. This is not conducive to users identifying the problem with the parameters.



When special characters are passed in the string, the correct content cannot be parsed correctly.

{"target":"metamask-contentscript","data":{"name":"metamask-provider","data":

{"method":"eth_sendTransaction","params":

[{"gas":"0x5f6f7","value":"0x0","from":"0x415cc25d8c5c1808051ab39187fcbbbd51f65aa6","to":"0xc2679fbd37d543

88ce493f1db75320d236e1815e","data":"0xf17325e70000000000000000000000000000000000000000000000000000000

0000000000020aee14f81ad29240a77ad323c31b86407fa219a14ea56995e447ebc8e9ad2525e000000000000000000

0000000000000000000000000000000000000000000400000000000000000000000000415cc25d8c5c1808051ab391

87fcbbbd51f65aa600000000000000000000000000000000000000000000000000000000000000000000000000000000

0000000000000000000000000000000000000000000100000000000000000000000000000000000000000000000000

0000000000000000000000000000000000000000000000000000000000000000000000000000000000c000000000000

0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

0000000000000000000140000000000000000000000000415cc25d8c5c1808051ab39187fcbbbd51f65aa600000000

0000000000000000000000000000000000000000000000000000000000c0000000000000000000000000000000000000

0000000000000000000000000123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef00000

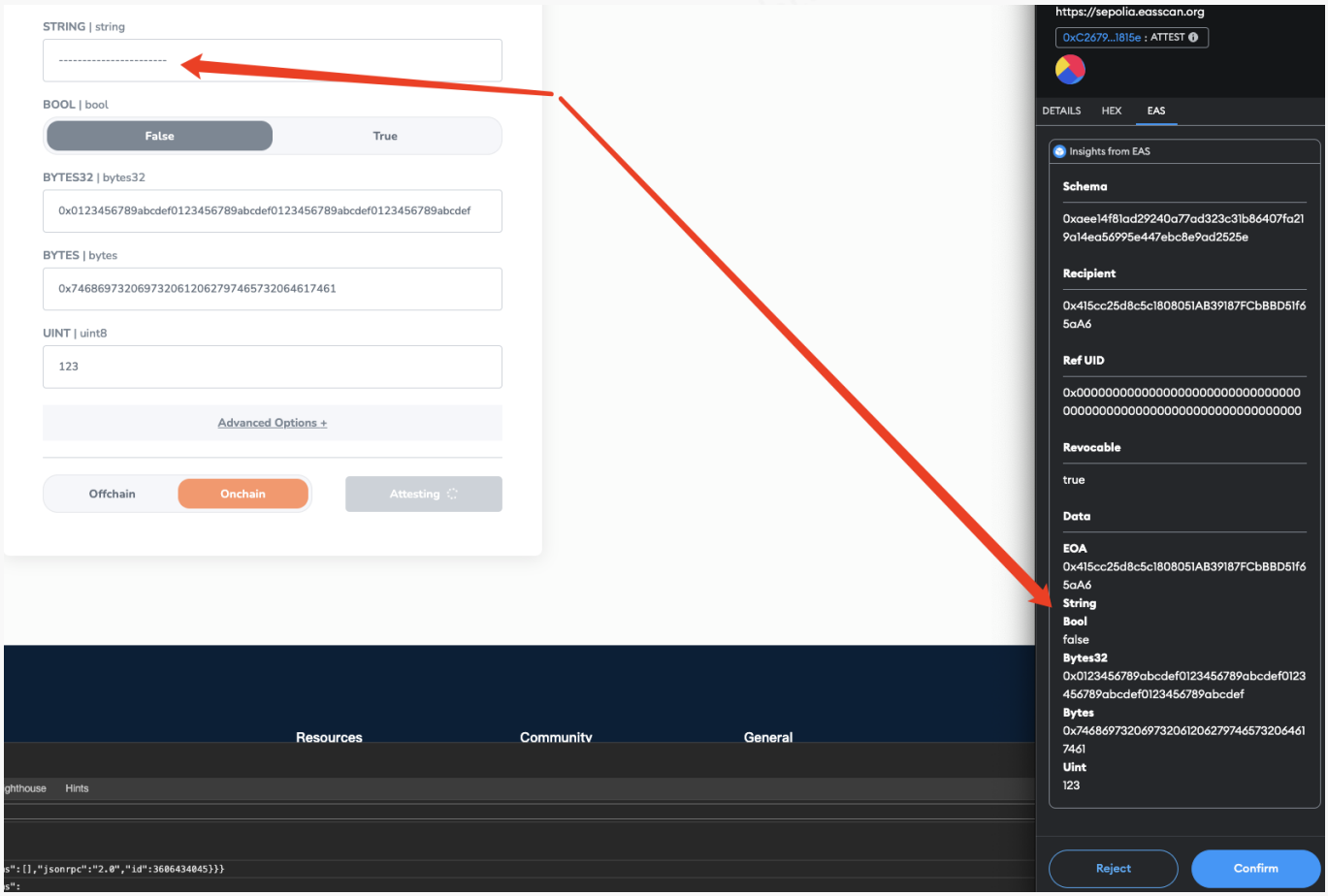
0000000000000000000000000000000000000000000000000000000000100000000000000000000000000000000000

0000000000000000000000007b000000000000000000000000000000000000000000000000000000000000172

d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d0000000000000000000000000000000000000000000000

0000000000000000000000000000000147468697320697320612062797465732064617461000000000000000000

00000"}],"jsonrpc":"2.0","id":3606434047}}}



Solution

1. It is recommended to check whether the recipient address and EOA meet the correct format. If the wrong address format is used, return the correct error message.
2. It is recommended to check whether the parsing of special characters in the code is correct.

Status

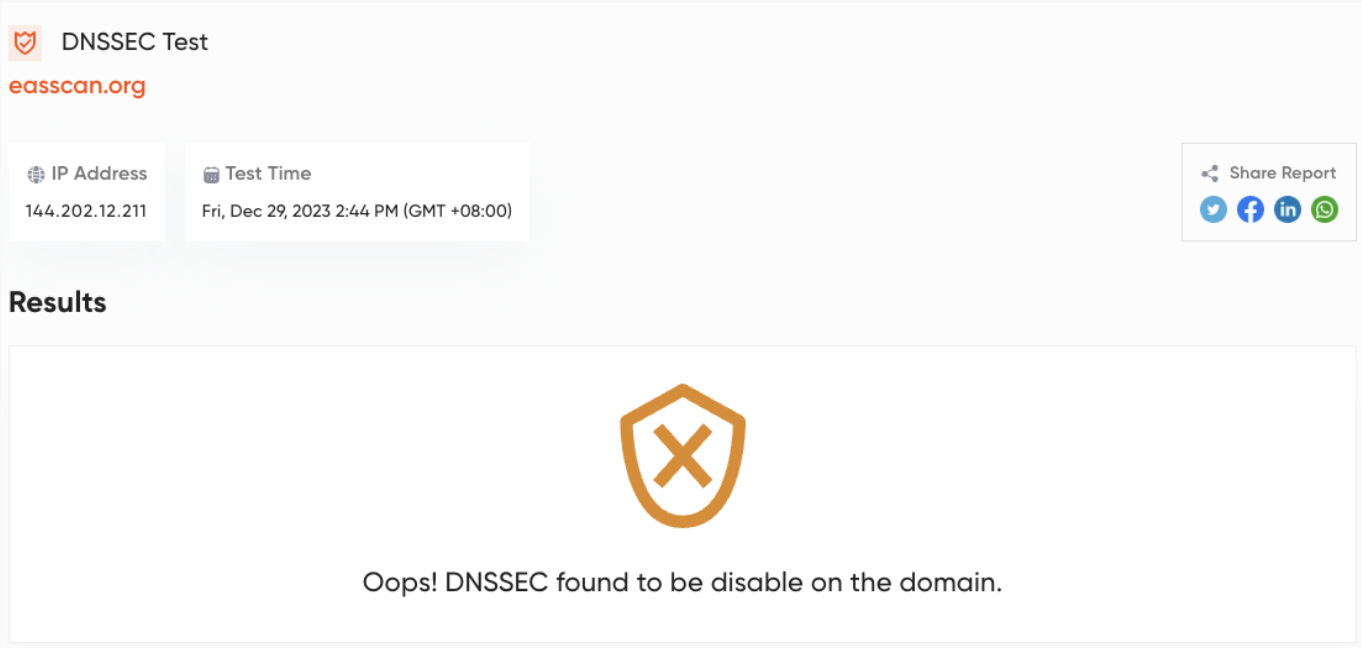
Confirmed; After communication, the project team will fix this issue in a future version.

[N2] [Suggestion] DNSSEC Not Configured

Category: DNSSEC security audit

Content

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



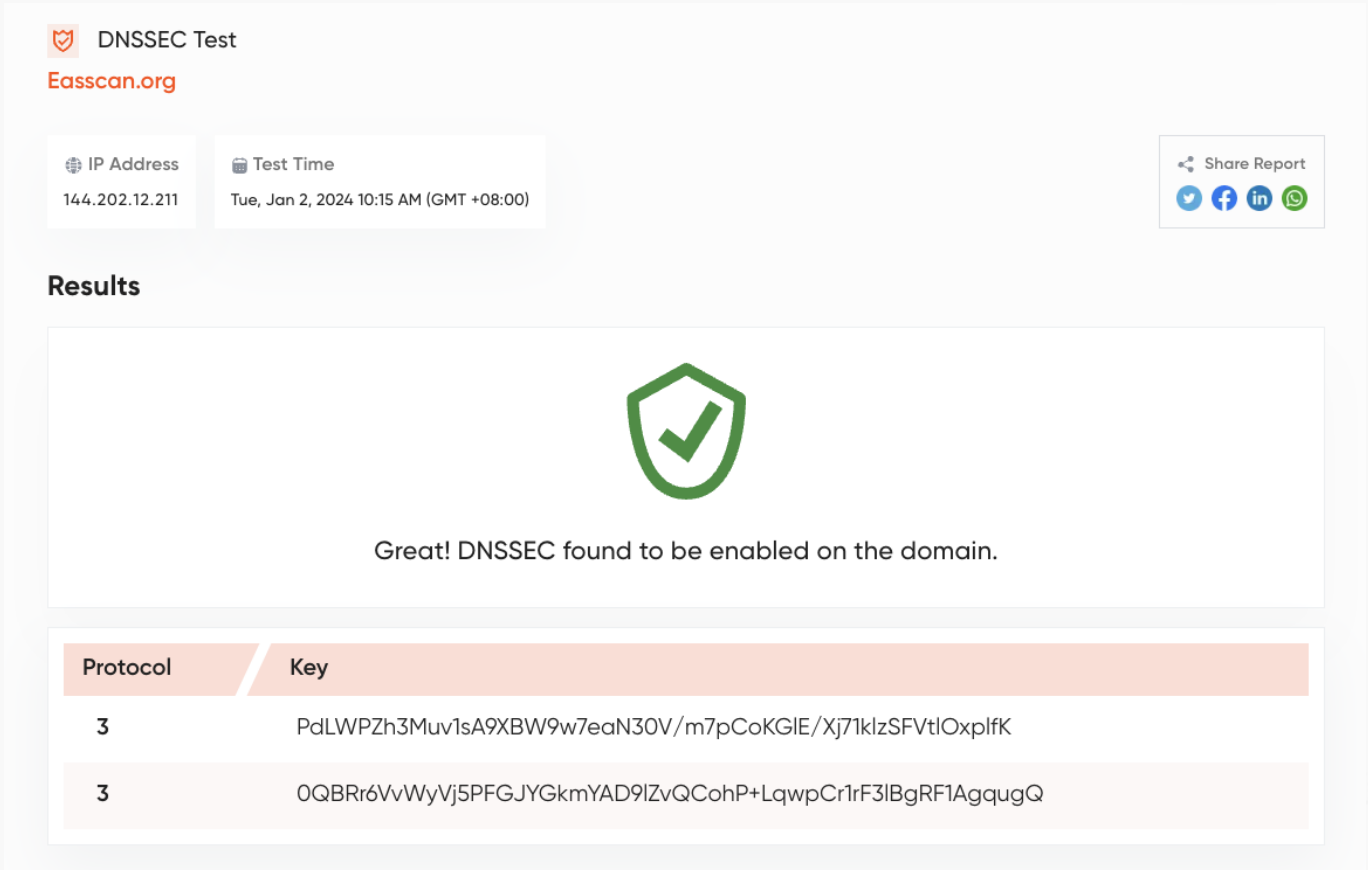
DNSSEC can protect websites from the following attacks:

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

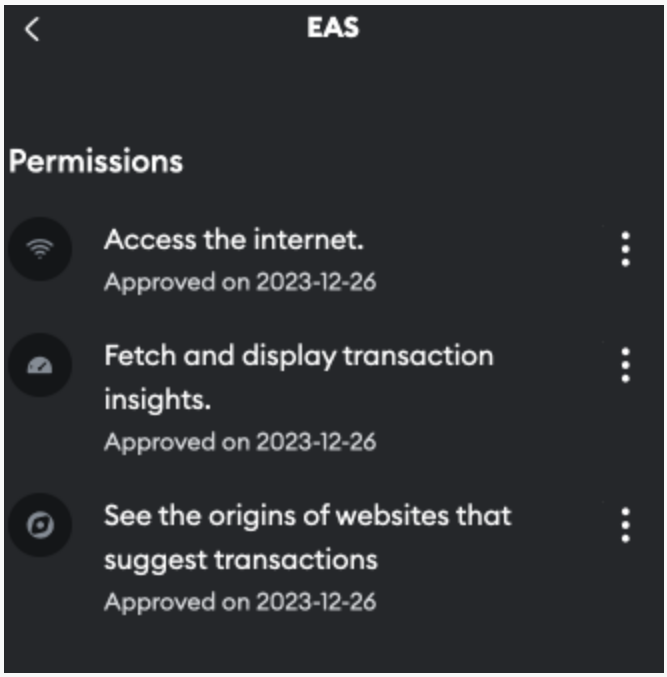
Fixed; The project team has correctly configured DNSSEC.

[N3] [Suggestion] Unused permissions

Category: Snap permissions security audit

Content

Snap has the following permissions.




```
"initialPermissions": {
  "endowment:network-access": {},
  "endowment:transaction-insight": {
    "allowTransactionOrigin": true
  }
},
```

Snap has the allowTransactionOrigin permission, which is used to obtain the transition Origin. However, this permission is not used in the code. It is need to confirm whether you need to obtain this permission in the actual production environment.

Solution

It is need to confirm whether need to obtain this permission in the actual production environment.

Status

Fixed; The project team removed the permission in the new commit.

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002312180002	SlowMist Security Team	2023.12.18 - 2023.12.18	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 3 suggestions. 2 suggestions have been confirmed and fixed. All the others 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