Snap Application

Security Audit Report

Table Of Contents

1 Executive Summary

On 2024.01.31, the SlowMist security team received the HashDit team's security audit application for HashDit-Snaps-main, 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

File Name: HashDit-Snaps-main.zip

sha256: 7eec40915d599e055e7e3eb459928377f7633bb100439eed2dffe71b5a7e504c

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Improve the detection rules	Others	Information	Acknowledged
N2	Incomplete address database records	Others	Medium	Fixed
N3	Lack of DNSSEC security configuration	DNSSEC security audit	Suggestion	Confirmed

3.3 Vulnerability Summary

[N1] [Information] Improve the detection rules

Category: Others

Content

When calling the Approve function, tx can bypass the security detection of HashDit-Snap.

Because MM will parse the transactions of Approve and enter the editing interface of the Custom spending cap, this will lead to bypassing the HashDit-Snap detection interface.

The following two methods did not trigger HashDit-Snap's risk detection:

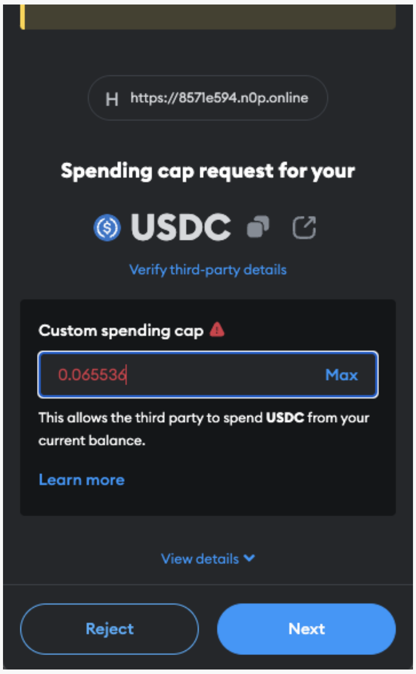
1. approve
2. approval for all

PoC:

Use the approve function to authorize the 0x4fabb145d64652a948d72533023f6e7a623c7c53.

approve(address,uint256)

```
ethereum.request({"method":"eth_sendTransaction","params":
[{"from":"0x415cc25d8c5c1808051AB39187FCbBBD51f65aA6","to":"0xA0b86991c6218b36c1d19D4
a2e9Eb0cE3606eB48","gas":"0x30d40","data":"0x095ea7b3000000000000000000000000005fbdb231
5678afecb367f032d93f642f64180aa3000000000000000000000000000000000000000000000000000000
0000010000","gasPrice":"0x76c3b0342"}]})
```



https://8571e594.n0p.online

Spending cap request for your

USDC

Verify third-party details

Custom spending cap

0.065536 Max

This allows the third party to spend **USDC** from your current balance.

Learn more

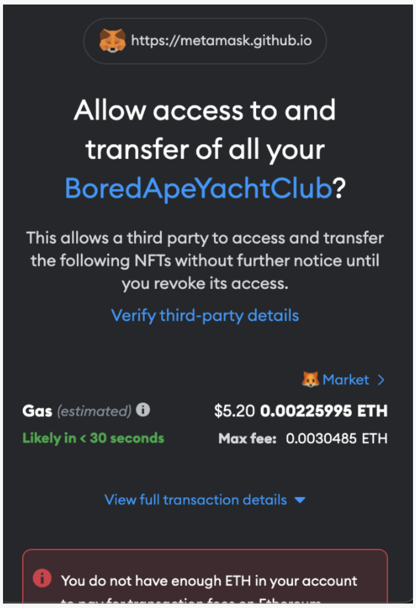
View details

PoC:

Use the approval for all function to authorize the 0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d.

SetApprovalForAll(address, bool)

```
window.postMessage({"target":"metamask-contentscript","data":{"name":"metamask-
provider","data":{"method":"eth_sendTransaction","params":[{"from":"Your
EOA","to":"0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d","data":"0xa22cb465000000000000
000000000000b85492afc686d5ca405e3cd4f50b05d358c75ede0000000000000000000000000000000000
00000000000000000000000000001"}],"jsonrpc":"2.0","id":2206383974}}})
```



https://metamask.github.io

Allow access to and transfer of all your BoredApeYachtClub?

This allows a third party to access and transfer the following NFTs without further notice until you revoke its access.

Verify third-party details

Market >

Gas (estimated) $5.20 0.00225995 ETH

Likely in < 30 seconds Max fee: 0.0030485 ETH

View full transaction details

You do not have enough ETH in your account

Solution

The MM mechanism causes the risk detection bypass issue. Therefore, in our communication with the project team, the project team clearly stated that if MM changes the approve() method in the future, they will support the risk detection function for this type of transaction the first time.

Status

Acknowledged

[N2] [Medium] Incomplete address database records

Category: Others

Content

Use the phishing address to test whether Snap's risk judgment is accurate and find that the risk returned is low.

PoC:

Transfer funds to malicious addresses through wallets.

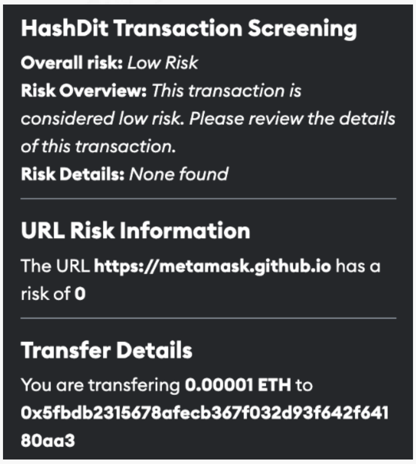
```
window.postMessage({"target":"metamask-contentscript","data":{"name":"metamask-provider","data":{"method":"eth_sendTransaction","params":[{"from":"Your EOA","to":"Evil Address","value":"0x9184e72a000"}],"jsonrpc":"2.0","id":2770317532}}})
```

Test the transfer to the malicious address 0x5FbDB2315678afecb367f032d93F642f64180aa3.

```
window.postMessage({"target":"metamask-contentscript","data":{"name":"metamask-provider","data":{"method":"eth_sendTransaction","params":
```

```
[{"from":"0x415cc25d8c5c1808051ab39187fcbbbd51f65aa6","to":"0x5FbDB2315678afecb367f03
2d93F642f64180aa3","value":"0x9184e72a000"}],"jsonrpc":"2.0","id":2770317532}}})
```

Snap displays the following content:



HashDit Transaction Screening

Overall risk: *Low Risk*

Risk Overview: *This transaction is considered low risk. Please review the details of this transaction.*

Risk Details: *None found*

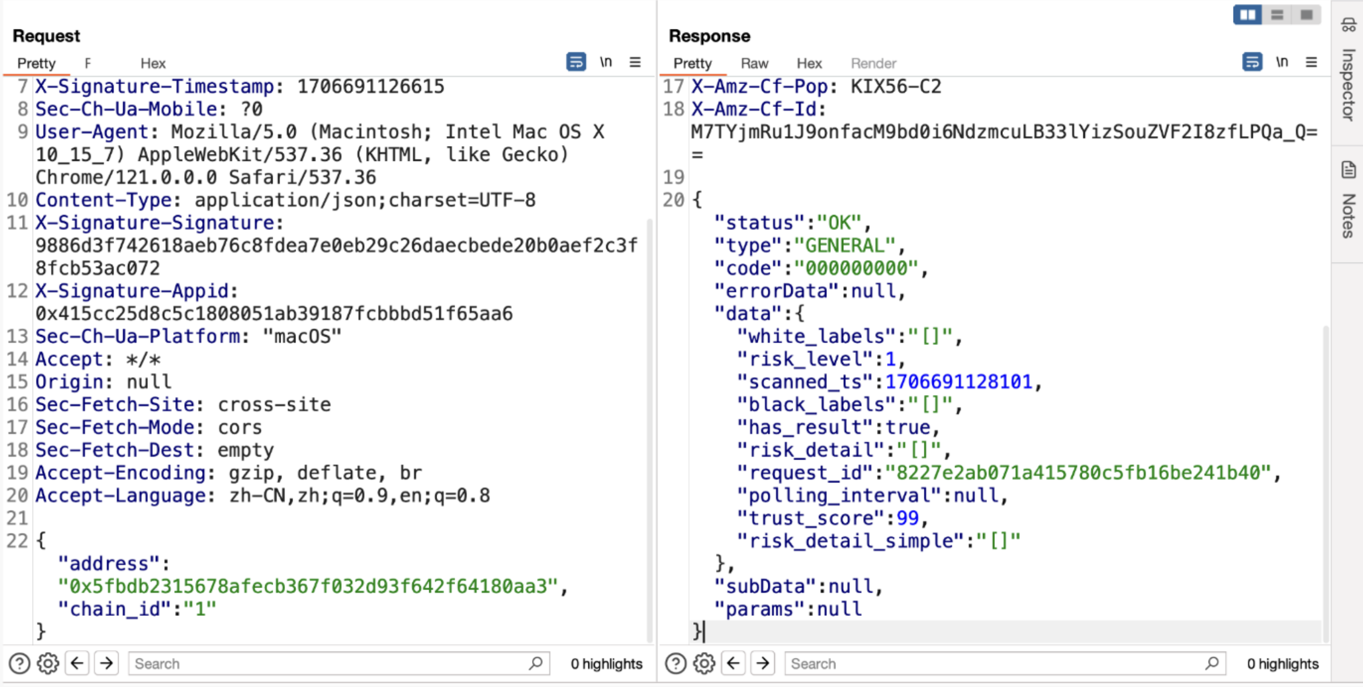
URL Risk Information

The URL **https://metamask.github.io** has a risk of **0**

Transfer Details

You are transfering **0.00001 ETH** to **0x5fbdb2315678afecb367f032d93f642f64180aa3**

Through the interface, it was found that the risk level of the phishing address was only 1, and the trust_score reached 99.



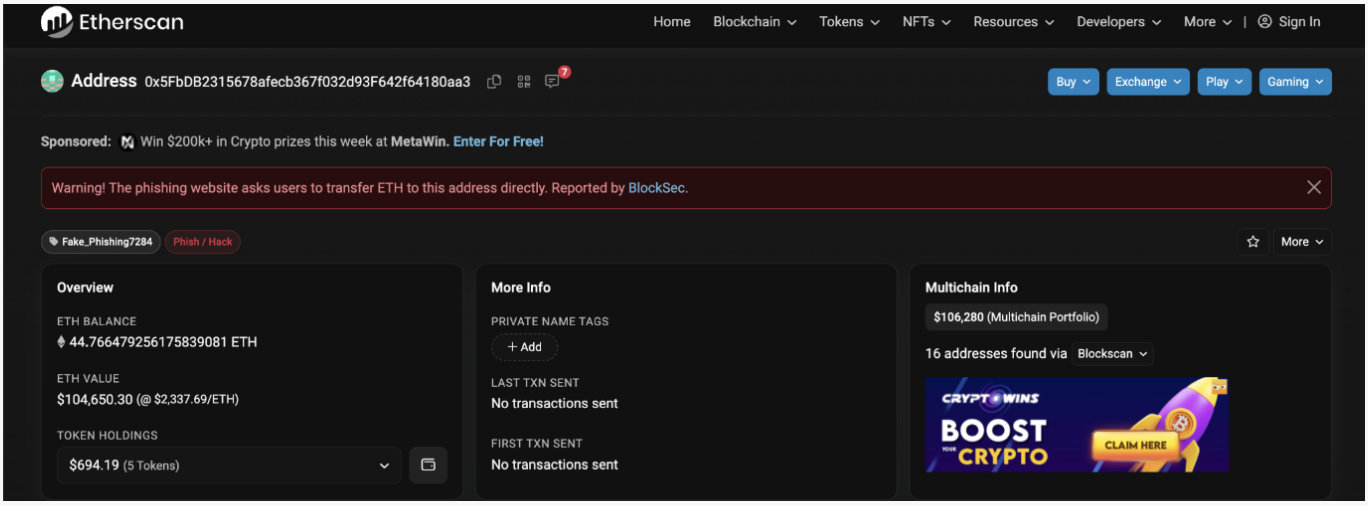
```
X-Signature-Timestamp: 1706691126615
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.0.0 Safari/537.36
Content-Type: application/json;charset=UTF-8
X-Signature-Signature:
9886d3f742618aeb76c8fdea7e0eb29c26daecbede20b0aef2c3f
8fcb53ac072
X-Signature-Appid:
0x415cc25d8c5c1808051ab39187fcbbbd51f65aa6
Sec-Ch-Ua-Platform: "macOS"
Accept: */*
Origin: null
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

{
  "address":
  "0x5fbdb2315678afecb367f032d93f642f64180aa3",
  "chain_id":"1"
}
```

```
X-Amz-Cf-Pop: KIX56-C2
X-Amz-Cf-Id:
M7TYjmRu1J9onfacM9bd0i6NdzmcuLB33lYizSouZVF2I8zfLPQa_Q=
=

{
  "status":"OK",
  "type":"GENERAL",
  "code":"000000000",
  "errorData":null,
  "data":{
    "white_labels":"[]",
    "risk_level":1,
    "scanned_ts":1706691128101,
    "black_labels":"[]",
    "has_result":true,
    "risk_detail":"[]",
    "request_id":"8227e2ab071a415780c5fb16be241b40",
    "polling_interval":null,
    "trust_score":99,
    "risk_detail_simple":"[]"
  },
  "subData":null,
  "params":null
}
```

Etherscan has flagged it as a phishing address.



Address 0x5FbDB2315678afecb367f032d93F642f64180aa3

Sponsored: Win $200k+ in Crypto prizes this week at MetaWin. Enter For Free!

Warning! The phishing website asks users to transfer ETH to this address directly. Reported by BlockSec.

Fake_Phishing7284 Phish / Hack

Overview

ETH BALANCE
44.766479256175839081 ETH

ETH VALUE
$104,650.30 (@ $2,337.69/ETH)

TOKEN HOLDINGS
$694.19 (5 Tokens)

More Info

PRIVATE NAME TAGS
+ Add

LAST TXN SENT
No transactions sent

FIRST TXN SENT
No transactions sent

Multichain Info

$106,280 (Multichain Portfolio)

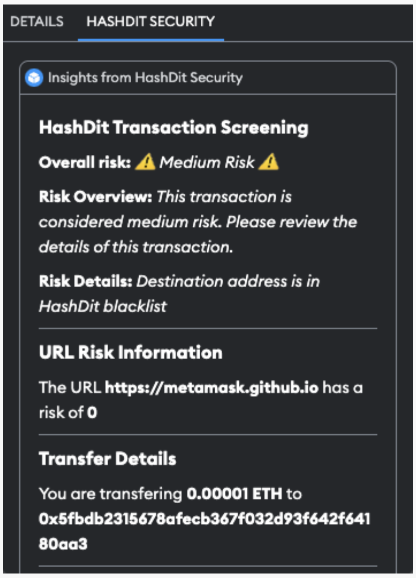
16 addresses found via Blockscan

Solution

It is recommended to access a more complete malicious address library to prevent users from losing funds due to the inability to identify malicious addresses. The SlowMist AML team has been diligently maintaining a comprehensive database of malicious addresses, which currently contains over 90 million risk-tagged addresses. For more information, please visit the official SlowMist AML website: https://aml.slowmist.com/

Status

Fixed; According to our communication with the project team, they said they have updated the database of malicious addresses and added over 200,000 blacklisted addresses. The address used in the example is now included in the database and is considered Medium Risk by HashDit-Snap.



Insights from HashDit Security

HashDit Transaction Screening

Overall risk: ⚠ *Medium Risk* ⚠

Risk Overview: *This transaction is considered medium risk. Please review the details of this transaction.*

Risk Details: *Destination address is in HashDit blacklist*

URL Risk Information

The URL **https://metamask.github.io** has a risk of **0**

Transfer Details

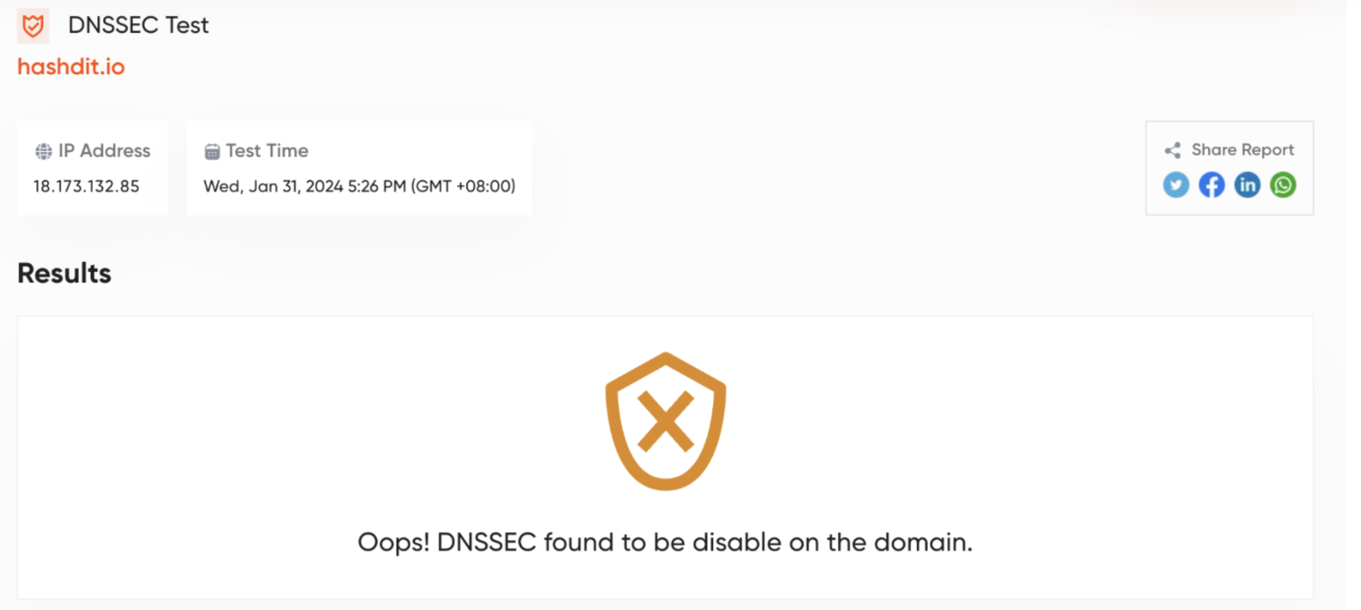
You are transfering **0.00001 ETH** to **0x5fbdb2315678afecb367f032d93f642f64180aa3**

[N3] [Suggestion] Lack of DNSSEC security configuration

Category: DNSSEC security audit

Content

The requested interface is not configured with DNSSEC.



DNSSEC Test

hashdit.io

IP Address
18.173.132.85

Test Time
Wed, Jan 31, 2024 5:26 PM (GMT +08:00)

Results

Oops! DNSSEC found to be disable on the domain.

Solution

It is recommended to configure DNSSEC correctly.

Status

Confirmed; After communication, it was learned that the project team has started to fix this issue.

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002402010001	SlowMist Security Team	2024.01.31 - 2024.02.01	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 a medium risk, a suggestion and a information. The medium risk has been fixed and the suggestion has been confirmed.

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