



Blockchain Security Audit Report



Table Of Contents

1 Executive Summary

2 Audit Methodology

3 Project Overview

3.1 Project Introduction

3.2 Coverage

3.3 Vulnerability Information

4 Findings

4.1 Vulnerability Summary

5 Audit Result

6 Statement

1 Executive Summary

On 2022.08.15, the SlowMist security team received the Hupayx team's security audit application for Taycan, 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 DeFi project, and it is strongly recommended to fix the critical vulnerabilities.
High	High severity vulnerabilities will affect the normal operation of the DeFi project. It is strongly recommended to fix high-risk vulnerabilities.
Medium	Medium severity vulnerability will affect the operation of the DeFi project. It is recommended to fix medium-risk vulnerabilities.
Low	Low severity vulnerabilities may affect the operation of the DeFi project in certain scenarios. It is suggested that the project party 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 the chain includes two steps:

Chain codes are scanned/tested for commonly known and more specific vulnerabilities using automated analysis tools.

Manual audit of the codes for security issues. The codes are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that was considered during the audit of the chain:

NO.	Audit Items	Result
1	[Encryption]Random generator security audit	Passed
2	[Encryption]Cryptographic Attack Audit	Passed
3	[Encryption]Transaction Malleability Attack	Some Risks
4	[Ledger]Transaction Replay Attack	Some Risks
5	[Off-Chain]False Top-up Audit	Some Risks
6	[RPC]The Ethereum Black Valentine's Day Vulnerability	Some Risks
7	[Supply Chain]Code Diff	Passed
8	Rug Pull Attack	Passed

3 Project Overview

3.1 Project Introduction

Taycan is a scalable, high-throughput Proof-of-Stake blockchain that is fully compatible and interoperable with Ethereum. It's built using the Cosmos SDK which runs on top of Tendermint Core consensus engine. and is forked from EVMOS

3.2 Coverage

Target Code and Revision:

<https://github.com/hupayx-com/evmos>

version: v7.0.0-hupayx

[Encryption]Random generator security audit

It is necessary to generate private keys with a secure random library.

Evmos does not provide a method to generate private keys, user should generating private keys using external tools.

[Encryption]Cryptographic Attack Audit

Hash:

github.com/tendermint/tendermint/crypto/tmhash (Base on SHA256)

Signature:

github.com/cosmos/cosmos-sdk/crypto/keys/secp256k1

github.com/cosmos/cosmos-sdk/crypto/keys/secp256r1

github.com/evmos/ethermint/crypto/ethsecp256k1

github.com/cosmos/cosmos-sdk/crypto/keys/ed25519

Use well known cryptographic algorithms.

[Encryption]Transaction Malleability Attack

Allowing transactions with any s value with $0 < s < \text{secp256k1n}$, as is currently the case, opens a transaction malleability concern, as one can take any transaction, flip the s value from s to $\text{secp256k1n} - s$, flip the v value (27 -> 28, 28 -> 27), and the resulting signature would still be valid. This is not a serious security flaw, especially since Ethereum uses addresses and not transaction hashes as the input to an ether value transfer or other transaction, but it nevertheless creates a UI inconvenience as an attacker can cause the transaction that gets confirmed in a block to have a different hash from the transaction that any user sends, interfering with user interfaces that use transaction hashes as tracking IDs.

[Ledger]Transaction Replay Attack

(a). Replay transaction on origin chain:

Duplicate transaction not be packed into block again.

(b). Replay transaction on forked chain:

Use `chain_id` to distinguish different chains when signing transactions, and there is no replay attack problem for transactions between different chains.

evmos/types/utils.go

```
const (  
    // MainnetChainID defines the Evmos EIP155 chain ID for mainnet  
    MainnetChainID = "evmos_22023"  
    // TestnetChainID defines the Evmos EIP155 chain ID for testnet  
    TestnetChainID = "evmos_2023"  
)
```

[Off-Chain]False Top-up Audit

Using EVM, an attacker can deploy evil contracts to launch attacks.

[RPC]The Ethereum Black Valentine's Day Vulnerability

When we start a node with default config:

```
$ evmosd start
```

The RPC is enabled by default.

[Supply Chain]Code Diff

Forked from Evmos project <https://github.com/evmos/evmos>, version v7.0.0.

The main changes are:

1. Change chain id.
2. Change coin name.
3. Remove hard fork code.

Rug Pull Attack

A rug pull is a malicious maneuver in the cryptocurrency industry where crypto developers abandon a project and run away with investors' funds.

There is no special authority(eg. admin/manager) here.

3.3 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	"False top up" risks	[Off-Chain]False Top-up Audit	Low	Confirming
N2	RPC "Black Valentine's Day" vulnerability	[RPC]The Ethereum Black Valentine's Day Vulnerability	Low	Confirming
N3	Transaction malleability risk	[Encryption]Transaction Malleability Attack	Suggestion	Confirming

NO	Title	Category	Level	Status
N4	Not return error when replay a transaction	[Ledger]Transaction Replay Attack	Low	Confirming

4 Findings

4.1 Vulnerability Summary

[N1] [Low] "False top up" risks

Category: [Off-Chain]False Top-up Audit

Content

There are 2 kinds of "False top up" risks:

(a). When using a contract for native token top-up, the transfer process may be aborted by a malicious contract revert, but the transaction status is successful, which may result in a fake top-up if no valid event judgment is performed.

(b). Failed transactions are also packed into blocks, and if the status of the transaction is not checked, the exchange will have a "false top-up" problem.

Solution

Exchanges, etc. need to check whether the status of the transaction is successful and determine whether the event is correct, it is recommended to prohibit the use of contract top-up.

Status

Confirming

[N2] [Low] RPC "Black Valentine's Day" vulnerability

Category: [RPC]The Ethereum Black Valentine's Day Vulnerability**Content**

RPC has a wallet function, attackers may steal funds through the RPC port if the port open for non-local access.

```
request:
curl https://taycan-rpc.hupayx.io:8545 \
  -X POST \
  -H "Content-Type: application/json" \
  -d '{"jsonrpc":"2.0","method":"eth_accounts","params":[],"id":1}'
repo:
{"jsonrpc":"2.0","id":1,"result":[]}
```

Vulnerability reference: <https://mp.weixin.qq.com/s/Kk2IsoQ1679Gda56Ec-zJg>

Solution

The exchange should disable the wallet modules or keep the port open in the local host.

Status

Confirming

[N3] [Suggestion] Transaction malleability risk**Category: [Encryption]Transaction Malleability Attack****Content**

Preventing high `s` values reduces the risk, but there is still a risk of malleability.

Vulnerability reference:

<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-2.md>

Solution

When a withdrawal transaction fails, the original transaction needs to be rebroadcast or repackaged with the same `nonce` to prevent malicious repeated withdrawals.

Status

Confirming

[N4] [Low] Not return error when replay a transaction**Category: [Ledger]Transaction Replay Attack****Content**

```
curl https://taycan-rpc.hupayx.io:8545 \
-X POST \
-H "Content-Type: application/json" \
-d '{"jsonrpc":"2.0","id":1,"result":
{"blockHash":"0x21dde4b0801e005559c57c28904b26f26000b4d874d02fc579a20756603d7a1","blockNumber":"0x5349f","from":"0xe75f98ee41db8f8e92d8eacb0d374f958b21aa82","gas":"0x5208","gasPrice":"0x13400607a900","maxFeePerGas":"0x17198ef45b00","maxPriorityFeePerGas":"0x59682f00","hash":"0x37937bdf222d392cc155776745ed12bab1e59ab03245d473fa4ca428f645296f","input":"0x","nonce":"0x0","to":"0xe75f98ee41db8f8e92d8eacb0d374f958b21aa82","transactionIndex":"0x0","value":"0xde0b6b3a7640000","type":"0x2","accessList":[],"chainId":"0x5607","v":"0x0","r":"0x1d2dd0a4bbdceb6b3b07ad16fe93c05c3067a983d49e305e7c27d896853df1bf","s":"0xaf9ffd598705250c4994cf44f697f28522a56da6bbc1c3ab5d27c1c9d39261b"}}}'
```

Solution

Return error message when replay a transaction.

Status

Confirming

5 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002208230001	SlowMist Security Team	2022.08.15 - 2022.08.23	Low Risk

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 3 low risk, 1 suggestion vulnerabilities.

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](https://twitter.com/SlowMist_Team)



Github
<https://github.com/slowmist>