Blockchain Security Audit Report

Table Of Contents

1 Executive Summary

On 2023.02.13, the SlowMist security team received the WEMIX3.0 team's security audit application for go-wemix, 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.
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]Keystore Encryption Audit	Some Risks
2	[Encryption]Insecure Encryption Library Audit	Passed
3	[Encryption]Transaction Malleability Attack	Some Risks
4	[Ledger]Transaction Replay Attack	Passed
5	[Off-Chain]False Top-up Audit	Some Risks
6	[RPC]The Ethereum Black Valentine's Day Vulnerability	Passed
7	Non-privacy/Non-dark Coin Audit	Passed
8	[Encryption]ECC Private Key Leak Audit	Passed
9	Rug Pull Attack	Passed

3 Project Overview

3.1 Project Introduction

Go implementation of the Wemix project.

3.2 Coverage

Target Code and Revision:

https://github.com/wemixarchive/go-wemix

Version: w0.10.1

[Encryption]Keystore Encryption Audit

- cmd/ethkey/generate.go

```
// Encrypt key with passphrase.
passphrase := getPassphrase(ctx, true)
scryptN, scryptP := keystore.StandardScryptN, keystore.StandardScryptP
if ctx.Bool("lightkdf") {
    scryptN, scryptP = keystore.LightScryptN, keystore.LightScryptP
}
keyjson, err := keystore.EncryptKey(key, passphrase, scryptN, scryptP)
if err != nil {
    utils.Fatalf("Error encrypting key: %v", err)
}
```

[Encryption]Insecure Encryption Library Audit

Hash:

"crypto/sha256"

"crypto/sha512"

"github.com/ethereum/go-ethereum/crypto/blake2b"

"golang.org/x/crypto/sha3"

"golang.org/x/crypto/ripemd160"

"crypto/hmac"

"golang.org/x/crypto/pbkdf2"

"golang.org/x/crypto/scrypt"

Signature:

"github.com/ethereum/go-ethereum/crypto/bls12381"

"github.com/ethereum/go-ethereum/crypto/bn256/cloudflare"

"github.com/ethereum/go-ethereum/crypto/bn256/google"

"github.com/ethereum/go-ethereum/crypto/secp256k1"

"crypto/ed25519"

"crypto/ecdsa"

"crypto/elliptic"

Encrypt:

"crypto/cipher"

"crypto/subtle"

"crypto/aes"

Use well known cryptographic algorithms.

[Encryption]Transaction Malleability Attack

Allowing transactions with any s value with 0 < s < secp256k1n, as is currently the case, opens a transaction malleability concern, as one can take any transaction, flip the s value from s to 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:

Each transaction is signed with a unique `nonce` value, duplicate transaction not be packed into block again.

(b). Replay transaction on forked chain:

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

Testing on testnet:

```
curl "https://api.test.wemix.com" \ -X POST \ -H "Content-Type: application/json" \ --data \ '{"jsonrpc":"2.0","method":"eth_sendRawTransaction","params":["0xf86f0185174876e8018303345094e80c6ae4f2901233ef7673a6ef2493cd450a5e5c88016345785d8a0000
```

`808208d4a0f74cedd960f94b65f67803411d592ee2ff96a7b7739746c547ec86ce6ba79b5ea01289f2389e23b9`

`d8263c9382df0e0273a9d08917c176ed8d9a5bcd7e1fbcb140"],"id":1}'`

Return:

{"jsonrpc":"2.0","id":1,"error":{"code":-32000,"message":"nonce too low"}}

Transaction cannot be replayed.

[Off-Chain]False Top-up Audit

If we use a maliciously constructed smart contract to falsely top up the exchange address, we can see that:

This is a record of a normal transaction.


```
{"jsonrpc":"2.0","id":1,"result":
{"blockHash":"0x18e54a3b3c624d58c756c099206a2ae06016ea4aae5786ccabe5d39e39f00d03","bl
ockNumber":"0x1162b81","contractAddress":null,"cumulativeGasUsed":"0x9d6d","effective
GasPrice":"0x174876e801","from":"0x3a7cbf14838dc01d6286d3e4a35ffaf89b634a6d","gasUsed
":"0x9d6d","logs":
[],"logsBloom":"0x0000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000","status":"0x1","to":"0xa3d42764ff61c6244b831e6d48e5bb178cef9d59
","transactionHash":"0x7ac34b8a00f4aae3b6598632d06ebdb2204c11f770e46ee2e8dfee36dca29e
6f","transactionIndex":"0x0","type":"0x2"}}
```


This is a transaction with rollback.


```
{"jsonrpc":"2.0","id":1,"result":
{"blockHash":"0x2c9e3f854665df300eea1d636c125bd4dc40db3ea659036c54d406a05e91e087","bl
ockNumber":"0x11625c7","contractAddress":null,"cumulativeGasUsed":"0x19f5f","effectiv
eGasPrice":"0x178411b200","from":"0x3a7cbf14838dc01d6286d3e4a35ffaf89b634a6d","gasUse
d":"0x92a8","logs":
[],"logsBloom":"0x0000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000","status":"0x1","to":"0xa3d42764ff61c6244b831e6d48e5bb178cef9d59
```

```
","transactionHash":"0xfb539dcadac94fab12d813fe1457a5f0e59bcf4dfe98b0d28a4b8d437caa1f
54","transactionIndex":"0x1","type":"0x2"}}
```


[RPC]The Ethereum Black Valentine's Day Vulnerability

If insecure account unlocking is not allowed if node's APIs are exposed to external.

- go-wemix/cmd/gwemix/main.go

```
if !stack.Config().InsecureUnlockAllowed && stack.Config().ExtRPCEnabled() {
    utils.Fatalf("Account unlock with HTTP access is forbidden!")
}
```

Non-privacy/Non-dark Coin Audit

The token WEMIX does not use privacy techniques such as zkp/mimblewimble to hide transfer details, and all token transfer processes are publicly accessible.

[Encryption]ECC Private Key Leak Audit

The generation of the private key seed is based on the `crypto/rand` standard library, and the entropy value is secure.

- crypto/crypto.go

```
func GenerateKey() (*ecdsa.PrivateKey, error) {
return ecdsa.GenerateKey(S256(), rand.Reader)
}
```

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.

3.3 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Weak passphrase	[Encryption]Keystore Encryption Audit	Suggestion	Acknowledged
N2	Transaction malleability risk	[Encryption]Transaction Malleability Attack	Suggestion	Acknowledged
N3	"False top up" risks	[Off-Chain]False Top-up Audit	Low	Acknowledged

4 Findings

4.1 Vulnerability Summary

[N1] [Suggestion] Weak passphrase

Category: [Encryption]Keystore Encryption Audit

Content

The private key is encrypted using keystore and the strength of the password is not verified. A weak passphrase like `123456` can be used in the test, which can be easily cracked.

Solution

Detect password strength.

Status

Acknowledged

[N2] [Suggestion] Transaction malleability risk

Category: [Encryption]Transaction Malleability Attack

Content

Preventing high `s` values reduces the risk, but `secp256k1` is still at 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

Acknowledged

[N3] [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 false 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

Acknowledged

5 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002302150003	SlowMist Security Team	2023.02.13 - 2023.02.15	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 1 low risk, 2 suggestion vulnerabilities.

6 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