XDPoSChain Security Audit Report

Contents

11. Executive Summary

On April 19, 2021, the SlowMist security team received the XDPoSChain team's security audit application for XDPoSChain , 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.

SlowMist blockchain system test method:

Black box testing	Conduct security tests from an attacker's perspective externally.
Grey box testing	Conduct security testing on code module 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 wether there are vulnerabilities in programs suck as nodes, SDK, etc.

SlowMist blockchain risk level:

Critical vulnerabilities	Critical vulnerabilities will have a significant impact on the security of the blockchain, and it is strongly recommended to fix the critical vulnerabilities.
High-risk	High-risk vulnerabilities will affect the normal operation of blockchain. It is

vulnerabilities	strongly recommended to fix high-risk vulnerabilities.
Medium-risk vulnerablities	Medium vulnerability will affect the operation of blockchain. It is recommended to fix medium-risk vulnerabilities.
Low-risk vulnerabilities	Low-risk vulnerabilities may affect the operation of blockchain in certain scenarios. It is suggested that the project party should evaluate and consider whether these vulnerabilities need to be fixed.
Weaknesses	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.
Enhancement Suggestions	There are better practices for coding or architecture.

2. Project Background (Context)

2.1 Project Introduction

Project Website: https://xinFin.org

Coin Symbol: XDC

Project source code: https://github.com/XinFinOrg/XDPoSChain

Audit version: v1.0.1

2.2 Scope of Audit

The main types of security audit include:

(other unknown security vulnerabilities are not included in the scope of responsibility of this audit)

No.	Audit Category	Audit Result
1	Code Compliance Audit	Some Risks
2	Random Number Generation Algorithm Audit	PASS
3	Keystore Audit	Some Risks
4	Cryptographic Component Call Audit	PASS
5	Encryption Strength Audit	PASS
6	Length Extension Attack Audit	PASS
7	Transaction Malleability Attack Audit	PASS
8	Replay Attack Audit	PASS
9	Top-up Program Audit	PASS
10	RPC Permission Audit	Some Risks

3. Code Overview

3.1 Infrastructure

XDPoSChain is based on the open source go-ethereum(v1.8.3) development.

3.2 Code Compliance Audit

Fork open source blockchain source code or using similar protocol will cause problems such as replay attacks and node peer pool pollution. We conduct relevant security compliance assessments for this.

```
accounts/abi/bind/backends/simulated.go
accounts/keystore/key.go
accounts/keystore/keystore_passphrase.go
common/hexutil/json.go
common/bytes.go
common/constants.go
common/types.go
common/types_test.go
consensus/clique/clique.go
consensus/XDPoS/api.go
consensus/XDPoS/snapshot.go
consensus/XDPoS/XDPoS.go
consensus/XDPoS/XDPoS_test.go
consensus/consensus.go
consensus/errors.go
console/console.go
console/console_test.go
core/state/statedb.go
core/types/block.go
core/types/block_test.go
core/types/transaction.go
core/types/transaction_signing.go
core/types/transaction_test.go
core/block_validator_test.go
core/blockchain.go
core/blockchain_test.go
core/chain_makers.go
core/error.go
core/genesis.go
core/genesis_test.go
core/state_processor.go
core/state_transition.go
core/tx_list.go
core/tx_pool.go
```

core/tx_pool_test.go
core/types.go
crypto/bn256/cloudflare/gfp_decl.go
crypto/bn256/google/bn256.go
crypto/bn256/google/curve.go
crypto/bn256/google/twist.go
dashboard/assets.go
eth/downloader/api.go
eth/downloader/downloader.go
eth/downloader/downloader_test.go
eth/downloader/queue.go
eth/fetcher/fetcher.go
eth/fetcher/fetcher_test.go
eth/filters/api.go
eth/gasprice/gasprice.go
eth/api.go
eth/api_backend.go
eth/backend.go
eth/backend_test.go
eth/config.go
eth/handler.go
eth/handler_test.go
eth/peer.go
eth/protocol_test.go
eth/sync.go
ethstats/ethstats.go
internal/build/util.go
internal/cmdtest/test_cmd.go
internal/debug/flags.go
internal/ethapi/api.go
internal/ethapi/backend.go
internal/jsre/deps/bindata.go
internal/web3ext/web3ext.go
les/api_backend.go
les/odr_test.go
les/request_test.go
miner/miner.go
miner/worker.go
node/config.go
node/defaults.go
node/service.go

```
p2p/discover/table.go
p2p/discover/table_test.go
p2p/discover/udp.go
p2p/discover/udp_test.go
p2p/simulations/adapters/inproc.go
p2p/dial.go
p2p/dial_test.go
p2p/peer.go
p2p/peer_error.go
p2p/rlpx.go
p2p/server.go
p2p/server_test.go
params/config.go
rpc/server.go
rpc/types.go
swarm/api/http/error.go
tests/block_test_util.go
trie/trie.go
vendor/github.com/btcsuite/btcd/btcec/secp256k1.go
vendor/github.com/rjeczalik/notify/debug_debug.go
vendor/github.com/rjeczalik/notify/debug_nodebug.go
vendor/github.com/rjeczalik/notify/watcher_fsevents_cgo.go
vendor/github.com/rjeczalik/notify/watcher_notimplemented.go
vendor/github.com/rjeczalik/notify/watcher_readdcw.go
vendor/github.com/rjeczalik/notify/watcher_stub.go
vendor/github.com/rjeczalik/notify/watcher_trigger.go
vendor/github.com/syndtr/goleveldb/leveldb/storage/mem_storage.go
vendor/github.com/syndtr/goleveldb/leveldb/util.go
whisper/whisperv6/api.go
whisper/whisperv6/api_test.go
```

P2P protocol is the same with Ethereum mainnet, it may cause node peer pool pollution.

Reference: https://mp.weixin.qq.com/s/UmricgYGUakAlZTb0ihqdw

3.3 Random Number Generation Algorithm 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)
}
```

3.4 Keystore Audit

Use the keystore to encrypt the storage, and the password strength is not verified. Weak passwords such as `123456` can be used in the test, which can be easily cracked.

3.5 Cryptographic Component Call Audit

Signature algorithm: Secp256k1

Hash algorithm: SHA256

Using Ethereum cryptography-related components widely used in the industry, no security risks have been found.

3.6 Encryption Strength Audit

Weak hash functions such as md5 and sha1 are not used.

3.7 Length Extension Attack Audit

In cryptography and computer security, a length extension attack is a type of attack where an attacker can use Hash(message1) and the length of message1 to calculate Hash(message1 ‖ message2) for an attacker-controlled message2, without needing to know the content of message1. Algorithms like MD5, SHA-1, and SHA-2 that are based on the Merkle－Damgard construction are susceptible to this kind of attack. The SHA-3 algorithm is not susceptible.

No error calls were found.

3.8 Transaction Malleability Attack Audit

The digital signature of the inputs and outputs do not cover the parents and the nonce. On one hand, this is important to let the transactions be recoved in case of a split-brain, but, on the other hand, it makes possible to a malicious node to change the transaction hash, or to generate many conflicts. This problem were fixed in EIP-2.

Vulnerability reference:

https://en.bitcoinwiki.org/wiki/Transaction_Malleability

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

3.9 Transaction Replay Attack Audit

Each transaction is signed with a unique `nonce` value, and there is no replay attack problem in the same chain.

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

- core/types/transaction_signing.go

```
// Hash returns the hash to be signed by the sender.
// It does not uniquely identify the transaction.
func (s EIP155Signer) Hash(tx *Transaction) common.Hash {
return rlpHash([]interface{}{
tx.data.AccountNonce,
tx.data.Price,
tx.data.GasLimit,
```

```
tx.data.Recipient,
tx.data.Amount,
tx.data.Payload,
s.chainId, uint(0), uint(0),
})
}
```

3.10 Top-up Program Audit

The structure of Receipt is as follows, the `Status` field is used to mark the status of the transaction.

- core/types/receipt.go

```
// Receipt represents the results of a transaction.
type Receipt struct {
// Consensus fields
PostState []byte `json:"root"`
Status uint `json:"status"`
CumulativeGasUsed uint64 `json:"cumulativeGasUsed" gencodec:"required"`
Bloom Bloom `json:"logsBloom" gencodec:"required"`
Logs []*Log `json:"logs" gencodec:"required"`

// Implementation fields (don't reorder!)
TxHash common.Hash `json:"transactionHash" gencodec:"required"`
ContractAddress common.Address `json:"contractAddress"`
GasUsed uint64 `json:"gasUsed" gencodec:"required"`
}
```

Initiate a transfer transaction on the main network, the test data is as follows:

```
curl --request POST \
  --url https://rpc.xinfin.network//getTransactionByHash \
  --header 'content-type: application/json' \
  --data
'{"jsonrpc":"2.0","method":"eth_getTransactionByHash","params":["0x85c73e0113cb10b5d08435e
c1a49ccfda587753ccf0aec6d98df499eabaaa584"],"id":1}'
  {
  "jsonrpc": "2.0",
  "id": 1,
  "result": {
    "blockHash":
"0xb8e8eec36ae0b6b0c8a22ddb43c2a068b321ccd2bfd1a913ea40ca733f127d1e",
```

```
      "blockNumber": "0x1beb57d",
      "from": "xdc472c619028ba67b817b48f8d64dbb7699ce0fadf",
      "gas": "0x1908b100",
      "gasPrice": "0x9c4",
      "hash": "0x85c73e0113cb10b5d08435ec1a49ccfda587753ccf0aec6d98df499eabaaa584",
      "input": "0x",
      "nonce": "0x1a96",
      "to": "xdce034d0a2f44f365f827650f2be39f24c8e9833d9",
      "transactionIndex": "0x0",
      "value": "0x409e52b48369a00000",
      "v": "0x88",
      "r": "0xfc2e32f3639d850f186e361a5ddfb576f09438d749662b42e65597766a946212",
      "s": "0x661fdb0a2ba66fb4b9cd789b6779f0de424b3bfc88c24099d965622b4f6d4acc"
   }
}
```


```
curl --request POST \
   --url https://rpc.xinfin.network//getTransactionReceipt \
   --header 'content-type: application/json' \
   --data
'{"jsonrpc":"2.0","method":"eth_getTransactionReceipt","params":["0x85c73e0113cb10b5d08435e
c1a49ccfda587753ccf0aec6d98df499eabaaa584"],"id":1}'
```


```
{
   "jsonrpc": "2.0",
   "id": 1,
   "result": {
      "blockHash":
"0xb8e8eec36ae0b6b0c8a22ddb43c2a068b321ccd2bfd1a913ea40ca733f127d1e",
      "blockNumber": "0x1beb57d",
      "contractAddress": null,
      "cumulativeGasUsed": "0x5208",
      "from": "xdc472c619028ba67b817b48f8d64dbb7699ce0fadf",
      "gasUsed": "0x5208",
      "logs": [],
      "logsBloom":
"0x000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000",
      "status": "0x1",
      "to": "xdce034d0a2f44f365f827650f2be39f24c8e9833d9",
      "transactionHash":
"0x85c73e0113cb10b5d08435ec1a49ccfda587753ccf0aec6d98df499eabaaa584",
      "transactionIndex": "0x0"
   }
}
```


When the exchange passes the recharge receipt, it needs to strictly verify the values of `to`, `value` and `status`.

3.11 RPC Permission Audit

RPC has a wallet function. By default, the node keeps the RPC port open in the WAN, which is insecure. The exchange should disable the account module and keep the port open in the local host.

Vulnerability reference: https://mp.weixin.qq.com/s/Kk2lsoQ1679Gda56Ec-zJg

4. Audit Result

4.1 Low-risk Vulnerabilitys

- Weak passwords can be used in the keystore, which can be easily cracked.
- P2P protocol is the same with Ethereum mainnet, it may cause node peer pool pollution.

4.2 Enhancement Suggestions

- There are RPC "Black Valentine's Day Vulnerabilities", which can lead to node privacy disclosure or asset theft. It is recommended to prohibit unlocking accounts when opening RPC, or only open RPC ports locally.
- Keep RPC port closed, or do not open in WAN.

4.3 Conclusion

Audit result: PASS

Audit No. : BCA002104300001

Audit date: April 30, 2021

Audit team: SlowMist security team

Summary conclusion: After correction, all problems found have been fixed and the above risks have been eliminated by XDPoSChain. Comprehensive assessed, XDPoSChain no risks above already.

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 base 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 this 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