Audit of smart contracts Move Stake

Revision 1 dated 09.18.2023

Contents

Brief information

Project: movestake.io
Network: Multi Chain
Compiler version: 0.8.4
Optimization: enabled
The audit date: 09.18.2023

Information

The contract code was reviewed and analyzed for vulnerabilities, logical errors, and the developers' exit scams possibility. This work was carried out concerning the project source code provided by the customer.

During the audit, no errors were found that could affect the security of the funds.

The detected problems full list can be found below.

General conclusion

As a result of the audit, no errors were found that affect the security of users' funds on the contract. No obvious signs of an exit scam were found.

Telescr.in guarantees the Move Stake contracts security and performance.

Liability disclaimer

The telescr.in team within this audit framework is not responsible for the developers or third parties' actions on the platforms associated with this project (websites, mobile applications, and so on). The audit confirms and guarantees only the smart contract correct functioning in the revision provided by the project developers (check the revision).

Aggregated data

The Contract analysis was performed using the following methods:

- Static analysis
  - o Checking the code for common errors leading to the most common vulnerabilities
- Dynamic analysis
  - o The Contract launching and carrying out the attacks various kinds to identify vulnerabilities
- Code Review

Received data

Recommendation	Type	Priority	Occurrence probability
Not found			

A. Errors

Not found

B. Remarks

Not found

C. Warnings

Not found

Application. Error classification

Priority	
informational	This question is not directly related to functionality but may be important to understand.
Low	This question has nothing to do with security, but it can affect some behavior in unexpected ways.
Average	The problem affects some functionality but does not result in an economically significant user funds loss.
high	This issue can result in the user funds loss.
Probability	
Low	It is unlikely that the system is in a state in which an error could occur or could be caused by any party.
Average	This problem may likely arise or be caused by some party.
high	It is highly likely that this problem could arise or could be exploited by some parties.

Application. Digital bytecode print

The audit was carried out for the code certain version on the compiler version 0.8.4 with the optimization enabled.

To check the contract bytecode for identity to the one that was analyzed during the audit, you must:
1. Get contract bytecode (in any block explorer)
2. Get SHA1 from bytecode string
3. Compare with reference in this report

Sha1 from bytecode:

7eeca3b6fcfea7d31d2436f91c863564e6c2099b – Token
5bca3bf4b747385b39f130253c8208403e95a371 - ReferralTree
a60eb902f776d547027de82b1f2709ec38204f42 - RewardsType0
7851090c149cbe94c3012fa554569312042e3893 – RewardsType1
8152b1c0ba1e86ac5dc08a7d92c73b89e82c37ae – RewardsType2
426276a57342380874dc5f3a22cee76e4d7c4f6d - MultisigWithTimelock

Sha1 from bytecode (non-metadata):

811a0e7e55181375f808689079e243ce06dfac54 – Token
1f66bc317ec5321cf94b427594356b511b85c4a1 - ReferralTree
a21fd891c3f1f5c3d26316dfaccd29c82f2c4627 - RewardsType0
a99947de36a337a4cbd4fa5f6d66964aa32100c0 – RewardsType1
997f10a8c83053b2096c16b0f6be02d5e687adab – RewardsType2
ddf7ceecd33ba53b6f4aa8123a5560071e67db48 - MultisigWithTimelock

Contract address:

Ethereum :
https://etherscan.io/address/0xb584D4bE1A5470CA1a8778E9B86c81e165204599

BNB :
https://bscscan.com/address/0xBE51D38547992293c89CC589105784ab60b004A9

Polygon :
https://polygonscan.com/address/0xAC313d7491910516E06FBfC2A0b5BB49bb072D91

optimism :
https://optimistic.etherscan.io/address/0x5800249621DA520aDFdCa16da20d8A5Fc0f814d8

Avalanche :
https://snowtrace.io/address/0x040993fbF458b95871Cd2D73Ee2E09F4AF6d56bB

Arbitrum :
https://arbiscan.io/address/0xc0E02AA55d10e38855e13B64A8E1387A04681A00