TRONexWorld contract audit

Revision 3 of 10.28.2020

Table of contents

Brief information

Project: tronex.world
Web: TRON
Compiler version: 0.5.10 + commit.a1d534e
Optimization: enabled
The audit date: 10.28.2020

Data

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.

The audit revealed:
- Logical error
- The discrepancy between declared and actual behaviour
- Other comments

The detected problems full list can be found below.

General conclusion

As the audit result is contract without errors and comments. There was no exit scam obvious signs *(exit scam - a situation in which contract developers have controlled access to participants' funds and can perform withdrawal operations without their knowledge)*. No bugs or security breach were found either.

Telescr.in guarantees the TRONexWorld contract 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).

Digitally signed.

Aggregated data

The Contract analysis was performed using the following methods:

- Static analysis
  - Checking the code for common errors leading to the most common vulnerabilities
- Dynamic analysis
  - 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

No errors were found.

B. Remarks

The code improvements recommended in the previous revision have been applied by the developers in this revision.

C. Improvements

The code improvements recommended in the previous revision have been applied by the developers in this revision.

Appendix. 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 behaviour 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.

Appendix. Bytecode hash sum

The audit was carried out for the code certain version on the compiler version 0.5.10 + commit.a1d534e with the optimization enabled.

To check the contract bytecode for identity to the one that was analysed 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: ab8c50bd67eb74fd685b1db03e53ed927cb19013

Check hash sum

Appendix. Audit summary signature

```
{
  "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
  "msg": "As the audit result is contract without errors and comments.
There was no exit scam obvious signs (exit scam - a situation in which
contract developers have controlled access to participants' funds and can
perform withdrawal operations without their knowledge). No bugs or
security breach were found either. Telescr.in guarantees the TRONexWorld
contract security and performance. Actual for bytecode with sha1:
ab8c50bd67eb74fd685b1db03e53ed927cb19013",
  "sig":
"0xa8eeffa5961a92b834f902d00bc6a2ec4a407e18c107489a7d48dc2488d9c15e54daac2
c093029cf8727297ac75db3b0da834d8a9756b90ecfa12d5f3a0fc9281c",
  "version": "3"
}
```

Check signature