SpaceOfTron contract audit

Revision 1 of 10.25.2020

Table of contents

Brief information

Project: spaceoftron.com
Web: TRON
Compiler version: 0.5.10 + commit.a1d534e
Optimization: enabled
The audit date: 10.25.2020

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 behavior
- Other comments

The detected problems full list can be found below.

General conclusion

As the audit result is 1 comment were identified that did not affect the users' funds security the smart-contract. There were no exit scam obvious signs. No bugs or security breach were found either. Comments and improvements are related to the contract non-optimized work and are recommendatory. Remark can lead to the fact that the user will receive less funds for withdrawal than expected, but this behavior occurs only if the contract has less funds than the user has to withdraw. The recommendation is to check the balance of the contract before withdrawing.

Telescr.in guarantees the SpaceOfTron 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**
Warning: there is a probability of losing bonuses and dividends	Remarks	Informational	Medium

A. Errors

No errors were found in this revision.

B. Remarks

1. Warning: there is a probability of losing bonuses and dividends

During the withdrawing process the contract's balance can be less then required amount to withdraw. In this case whole balance of the contract will be withdrawn. However, the debited bonuses won't be back. The same point also applies to the value 'withdrawn'(a property of the Deposit) which is affecting possibility of withdrawing.

C. Improvements

No improvements were found 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
4. Or check sha1 on site telescr.in

Sha1 from bytecode:
b5d14a658eb92b8ae4507f0cb5b2283bed369738 (without metadata)
2142c0598dc738a7809b819a22faa3635f8b78a4 (with metadata)
Contract address (TRON network): TQwBFazacAr2XLkUwpgZU2NzzFwEtPdF2P

Check hash sum

Appendix. Audit summary signature


```
{
  "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
  "msg": "As the audit result is 1 comment were identified that did not
affect the users' funds security the smart-contract. There were no exit
scam obvious signs. No bugs or security breach were found either. Comments
and improvements are related to the contract non-optimized work and are
recommendatory. Remark can lead to the fact that the user will receive
less funds for withdrawal than expected, but this behavior occurs only if
the contract has less funds than the user has to withdraw. The
recommendation is to check the balance of the contract before withdrawing.
Telescr.in guarantees the SpaceOfTron contract security and performance.
Sha1 from bytecode: b5d14a658eb92b8ae4507f0cb5b2283bed369738 (without
metadata), 2142c0598dc738a7809b819a22faa3635f8b78a4 (with metadata)
Contract address (TRON network): TQwBFazacAr2XLkUwpgZU2NzzFwEtPdF2P",
  "sig":
"0xe12f731c2d8300dad4ea1402bb1266cb73f140904f09225b2202cd0268ec8dfe0a6a13c
845e98a3f8ff063783c80779368fb726962e5d3dbcc7ceb9fab7d03201b",
  "version": "3"
}
```


Check signature