Audit of smart contract TronEcology

revision 1 dated 03.07.2021

Summary

Brief information

Project: TronEcology
Network: TRON
Compiler version: ^0.5.9
Optimization: Enabled
Audit date: 03.07.2021

Information

The contract code was reviewed and analysed for vulnerabilities, logical errors and developer exit scams possibilities. This work was carried out concerning the project source code and documentation provided by the customer.

Provided documentation is sufficient to validate the project

General conclusion

As a result of the audit, no errors was found that affect the security of users' funds on the contract.

Telescr.in guarantee the safety and performance of the contract TronEcology

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.

Confirmed by digital signature

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	Line of error
Overflow possibility	warning	medium	medium	170, 172, 361, 362, 411, etc...
Unessesary operation	notice	low	N/a	181

A. Errors

Not found.

B. Warnings

1. Overflow possibility

In the most of calculations SafeMath is not used

C. Notice

1. Unessesary operation

There's no reason to multiply by 1

D. Remarks

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.
medium	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.
medium	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 ^0.5.9 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:
        49931fceea5fa3f16e7bd1d0f67a58e2cbea73d9
Sha1 from bytecode (non-metadata):
        1d458788092def7e68cca65a4822e3341e3aecec
Contract address:
        TBFh35NE8esEWPaU1UX2XiJqBCWrXhn1PF

Check the digital print

Application. Signature of the audit report

{   "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",   "msg": "As a result of the audit, no errors was found that affect the security of users' funds on the contract. Telescr.in guarantee the safety and performance of the contract TronEcology . Sha1 of contract - 49931fceea5fa3f16e7bd1d0f67a58e2cbea73d9. Sha1 without meta of contract - 1d458788092def7e68cca65a4822e3341e3aececContract address - TBFh35NE8esEWPaU1UX2XiJqBCWrXhn1PF",   "sig": "0xba1e1fca9a0dbf6a1d2aa81b51193a1dfe9316f45bc6d4f29b82fae68199f1902a3ce347b5bd672bc2f4cc85a64266af7f4778d8564927f652c15aff805fe2d71b",   "version": "3" }

Check the signature