

The TronApex smart contract audit

Revision 1 dated 12.03.2020

Contents:

| | |
|---|---|
| The TronApex smart contract audit..... | 1 |
| Contents: | 2 |
| Brief information | 3 |
| Information | 3 |
| General conclusion | 3 |
| Liability disclaimer | 3 |
| Aggregated data | 4 |
| Received data | 4 |
| A. Errors | 5 |
| 1. Edge values incorrect processing..... | 5 |
| B. Remarks | 6 |
| C. Warnings | 7 |
| Application. Error classification | 8 |
| Application. Digital bytecode print | 9 |
| Application. The audit report signature | 1 |

Brief information

Project: tronapex.com
Web: TRON
Compiler version: 0.5.9
Optimization: enabled
The audit date: 12.03.2020

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, error was discovered that do not directly affect the funds' safety.

The detected problems full list can be found below.

General conclusion

As the audit result, 1 error was revealed that did not affect the users' funds security on the contract. The exit scam clear signs - not found. The error is related to withdrawal restrictions processing.

Telescr.in guarantees the safety and performance of the TronApex contract.

Liability disclaimer

The telescr.in the 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).

[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 |
|--|-------|----------|------------------------|
| Edge values incorrect processing | Error | Average | low |

A. Errors

1. Edge values incorrect processing

In the `WithdrawDividends` function, when checking which range the user total invested value is, it does not take into account its possible equality with the `WithdrawalDividendsRuleOneMax` and `WithdrawalDividendsRuleTwoMax` values.

B. Remarks

Not found.

C. Warnings

Not found.

Application. Error classification

| Informational | |
|----------------------|---|
| priority | 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. |
| <i>Average</i> | The problem affects some functionality but does not result in economically significant users' 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. |
| <i>Average</i> | 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 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:

026187d694da024ba2fe4ab80e3303420162c5cb

Sha1 from bytecode (non-metadata):

59b28a964383abbb66af09e2912535701f1c6dc6

Contract address:

TWehXUMJfpLduYrsqdhvnmQwBzHKPrmSv

[Check the digital print](#)

Application. The audit report signature

```
{  
  "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",  
  "msg": "As the audit result, 1 error was revealed that did not affect the users' funds security on the contract. The exit scam clear signs - not found. The error is related to withdrawal restrictions processing. Telescr.in guarantees the safety and performance of the TronApex contract. Sha1 from bytecode: 026187d694da024ba2fe4ab80e3303420162c5cb Sha1 from bytecode (non-metadata): 59b28a964383abbb66af09e2912535701f1c6dc6 Contract address: TWehXUMJfpLduYrsqdhvnmQwBzHKPrmSv",  
  "sig": "0xae420c4e0aefc47d459be4be100be3615ffef617285585bb9073a953f40963b56e3d1fc35c9afb6d7d782cac979ff03e3b642821c262507d7e759cb053fa8cc61c",  
  "version": "3"  
}
```



[Check the signature](#)