Security Audit

TRONX

https://tronscan.org/#/contract/TYmZZsGRcdwnCPgGXSDytyzYHLPt7JKTL2

HAZE SECURITY

12/28/2020

www.hazecrypto.net

Haze Security

CRITICAL ISSUES (critical, high severity): 0

Critical and harmful access for owners, user block ability, Bugs and vulnerabilities that enable theft of funds, lock access to funds without possibility to restore it, or lead to any other loss of funds to be transferred to any party.

ERRORS, BUGS AND WARNINGS (medium, low severity): 0

Bugs can negatively affect the usability of a program, errors that can trigger a contract failure, Lack of necessary security precautions, other warnings for owners and users, warning codes that are valid code but the compiler thinks are suspicious.

OPTIMIZATION (low severity): 0

Methods to decrease the cost of transactions in Smart-Contract.

RECOMMENDATIONS (very low severity): 2

Hint and tips to improve contract functionality and trustworthy.

In the **TRONX** Smart Contract there were no vulnerabilities found, no backdoor codes, and no scam scripts.

The code was tested with compatible compilers and simulate manually reviewed for all commonly known and specific vulnerabilities.

TronX Smart Contract is **safe** for use in the Tron main network.

Optimization suggestions

1- Direct Transfer TRX to Contract (low severity).

If a user transfer TRX directly to contract address and the user has no active upline, the amount adds to contract balance but deposit does not act.

```
82
83      function() payable external {
84          _deposit(msg.sender, msg.value);
85      }
86
```

Note:

This comment is relevant only if a user does not use the contract deposit function and transfer amount directly to the contract address

2- Unused Variable

“permanent_top” is defined and does not use in contract. It is better to remove it.

Note: this issue doesn't affect the main functionality and security of the smart-contract.