CRYPTOCODING

SERVICES

smart-contract audit

2018

Cryptocoding Servises

telegram: @maxwInter24

https://cryptocoding.servises

Request from client

Web: https://5eth.io/

Source: https://github.com/5ethio/Eth5io

Contacts: @****** (Telegram)

Project Report

Method of auditing

An audit of a smart contract based on the source code, associated with a block chain from the GitHub repository, was provided. A manual verification method was used. To examine their messages, automated code analysis tools were used.

The check took place in a test network using authoring methods and tools for calling the functions described in the contract.

Critical remarks

The negative points include the fact that there is no library of Safe Mathematics in the project code. There is a huge amount of formulas in the code that can give an incorrect result due to overflow. This is the probability is very small, but it is.

During testing of the smart contract, a small problem of the “last investor” was discovered. Since the contract gives only the entire dividends, large investors may be faced with the fact that they will not find their deposit at the end of the project’s life.

Eth5io.sol line: 245

```
function addInvestors(address[] addr, uint[] amount, bool[] isSuper)
```

This function is called only once at the beginning of the contract life. It allows you to add an array of addresses with 0 balance and assignment of referral status.

Eth5io.sol line: 261

```
function nextRound();
```

The function is performed when there is no funds in the project for paying dividends. All addresses, referral statuses and deposits are removed and the base and a new cycle begins.

Vulnerabilities

There are no external vulnerabilities on access rights to methods. Every function is verified.

Owner cannot manipulate or manage contract funds.

Safe Math

Unsafe math is used here and elsewhere. In this case, it does not lead to vulnerability.

Standard vulnerability checks and errors

Reentrancy (Not detected)

Any interaction from the contract A with another contract B and any transfer of ether
gives control to contract B. This allows B to open A before all internal changes are completed. In addition, you also need to consider multi-contractual situations. The opened contract (B) can change the state of the third (C) contract, on which you depend.

In this decision there are no references to third-party contracts. The broadcast is transmitted via send or transfer, so malicious code cannot be started.

Race Conditions (Not Detected)

Race conditions occur in the event when changes in the parameters of a smart contract can occur independently from two different entry points. Thus, an attacker who sees an attempt to change parameters can make a transaction and changes caused by such a transaction will be overwritten by the victim who relied on a different state of the contract.

Timestamp Dependence (Not critical)

The timestamp changes after interacting with the contract, this can lead to the loss of accumulated deviends.

The dividends are calculated from the entry point into the contract. Sending 0 values is also an entry point.

Gas limit overflow (Not detected)

Cycles that do not have a fixed number of iterations, such as cycles, that depend on the value store are unsafe. Due to the restriction of the gas block, transactions can consume only a certain amount of gas.

DoS with revert (Not detected)

If the code in the cycle depends on the contract parameters that may be influenced by third parties, refers to third-party contracts, or transfers the broadcast to third-party addresses, by carelessness or malicious intent, a third person can create a situation in which an exclusion occurs at a certain iteration, blocking the entire cycle.

DoS with Block Gas Limit (Not detected)

There are no cycles and recursion of contract parameters, the owner and third parties cannot influence, there are no references to third-party contracts or broadcasts to third-party addresses, through carelessness or malicious intent, a third person cannot create a situation in which significant gas rejection occurs that blocks the entire cycle for a specific iteration, due to exceeding the gas limit for the block.

Common Conditions

Start and end dates

Start and end dates can not be changed by the owner. This does not give the opportunity to violate the interests of the investor. For example, you cannot delay a round for an indefinite period.

Prices and bonuses

Bonuses are awarded depending on the referral status of the address participating in the contract. There are 4 types of referral payments. Test Basic VIP and SVIP. Basic 5% VIP 10% SWIP 15% Test is not taken into account.

The size of the fund

The size of the fund depends only on the funds invested in it.

Funds Management

After receiving the funds at the contract address, the funds are charged to the address except for 10% of the advertising address and 5% of the technical support of the contract. Payments continue until such time as the balance of the contract is positive. If the required balance of the fund is not available, the investor will not receive any payment. This makes it possible to violate the interests of the investor.

Prices and bonuses

Bonuses are awarded depending on the referral status of the address participating in the contract. There are 4 types of referral payments. Test Basic VIP and SVIP. Basic 5% VIP 10% SWIP 15% Test is not taken into account.

The size of the fund

The size of the fund depends only on the funds invested in it.

Funds Management

After receiving the funds at the contract address, the funds are charged to the address except for 10% of the advertising address and 5% of the technical support of the contract. Payments continue until such time as the balance of the contract is positive. If the required balance of the fund is not available, the investor will not receive any payment. This makes it possible to violate the interests of the investor.

Positive Options

There is no possibility to withdraw funds from the sending fund of a malicious code and stop payments.

Audit is not a statement or guarantee as to the utility of the code, the security of the code, the suitability of the business model, the regulatory regime for the business model or any other statement of suitability for the use of contracts according to their purpose, or the absence of errors in these contracts.

The audit documentation is for discussion purposes only.