finteh.org | audit report

SuperMiner

2226091

hash b41c999897e190370c175e28059b04ab5cf4f793063514ab8559f31561a31ea8

url bscscan.com/address/0xF0EA7697B99c2DEd2F1B61F8698E930B7F293Cfa#code

solidity

Introduction

Checks The Contract Code For Security Vulnerabilities And Bad Practices

Vulnerability analysis

High Severity Issues

✅ No high severity issues found

Medium Severity Issues

✅ No medium severity issues found

Low Severity Issues

⚠️ Old version of Solidity v0.5.16

finteh.org recommended

Upgrade to the current version v0.8.17

Transaction Origin: 'tx.origin' used

⚠ **Pos: 395;Pos: 409:** Check-effects-interaction: Potential violation of Checks-Effects-Interaction pattern in SuperMiner.withdraw(): Could potentially lead to re-entrancy vulnerability.

⚠ **Pos: 257;Pos: 260;Pos: 296;Pos: 312;Pos: 315;Pos: 339;Pos: 402;Pos: 417:** Block timestamp: Use of "now": "now" does not mean current time. "now" is an alias for "block.timestamp". "block.timestamp" can be influenced by miners to a certain degree, be careful.

⚠ Gas requirement of function SuperMiner.transferOwnership is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

⚠ **Pos: 427:55:** Similar variable names: SuperMiner.getReferralAmount(uint256,uint256) : Variables have very similar names "parent" and "percent".

⚠ **Pos: 141:16; Pos: 175:20:** Data truncated: Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.

finteh.org recommended

Use SafeMath.sol by OpenZeppelin against all odds

Solidity unit testing

Deployment

- ✔️ Should set the right owner (183ms)
- ✔️ Try to change owner from another account (57ms)
- ✔️ Change owner (54ms)
- ✔️ Try to init from another account (60ms)
- ✔️ Init (107ms)
- ✔️ Should set the right CEO
- ✔️ Try to change ceo address from another acc
- ✔️ Change ceo address (44ms)
- ✔️ Try to change commission from another acc
- ✔️ Try to change commission more then 10
- ✔️ Change commission (42ms)
- ✔️ Change MAXIMUM_DEPOSIT_AMOUNT amount (40ms)

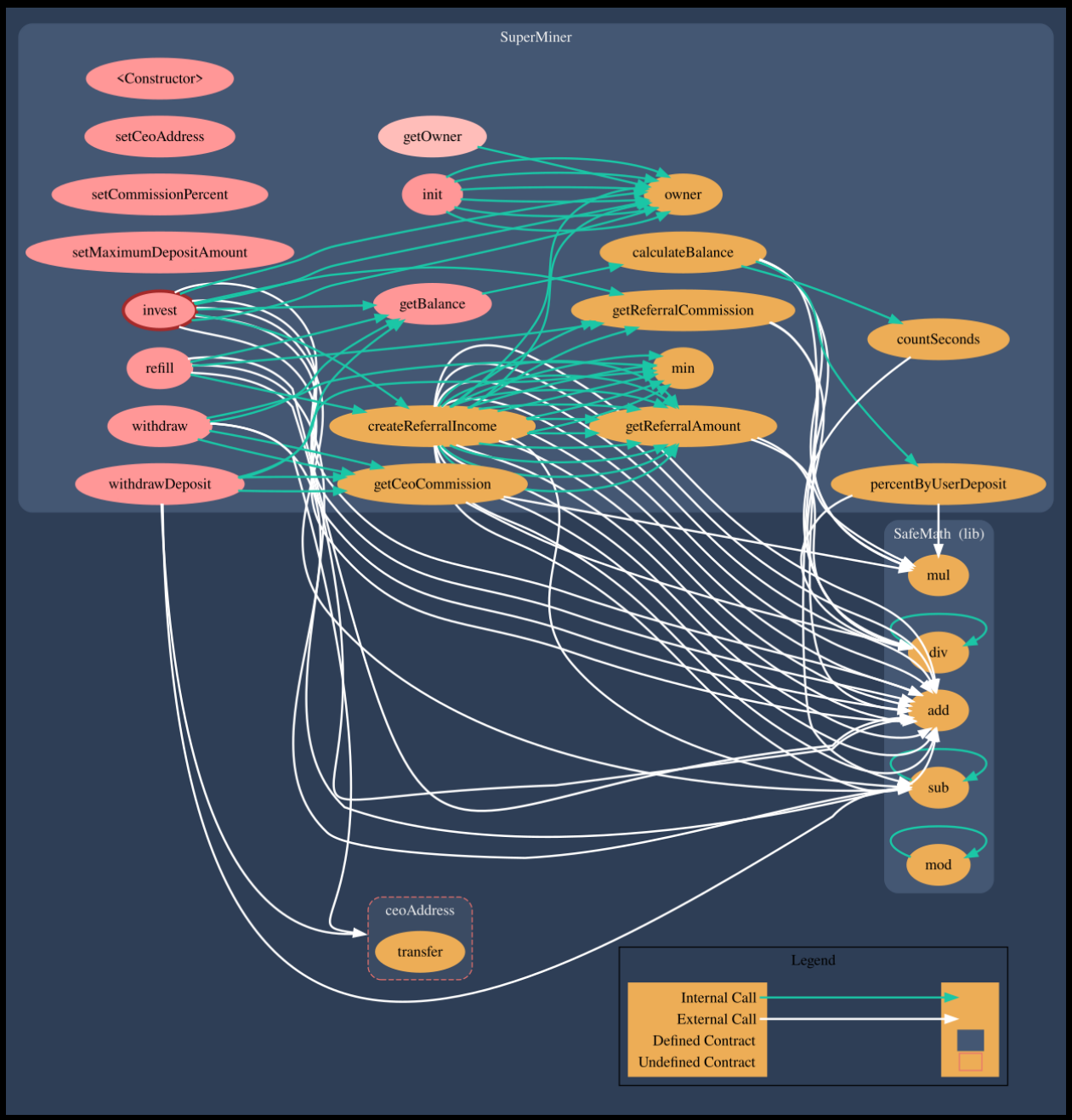
Invest operation

- ✔️ Invest with not initialised contract
- ✔️ Invest with not active parent (64ms)

finteh.org | audit report

- ✔️ Invest more then MAXIMUM_AMOUNT (71ms)
- ✔️ Invest less then MINIMUM_AMOUNT (60ms)
- ✔️ Invest owner (100ms)
- ✔️ Valid invest to first line (157ms)
- ✔️ Valid invest to second line (248ms)
- ✔️ Valid invest to third line (323ms)
- ✔️ Valid invest to fourth line (422ms)
- ✔️ Valid invest to fifth line (525ms)
- ✔️ Valid invest to sixth line (506ms)
- ✔️ Check compression (172ms)
- ✔️ Get Balance without save part (110ms)
- ✔️ Get Balance with save part (191ms)
- ✔️ Refill action (207ms)
- ✔️ Withdraw deposit (229ms)
- ✔️ Withdraw save balance (281ms)

29 passing (4s)



1.1 Main scheme of contract SuperMiner

Logic functionality

Rewards distribution

The main functions of the contract

1) Receiving BNB

2) Withdraw deposit

3) Withdraw balance

4) Reinvest from balance to deposit

Interest accruals go to the deposit and are calculated every second, the total amount of accruals is 1.5 percent per 24 hours

When depositing and reinvesting 25% commission on the referral system

1st generation 10%

2nd generation 6%

3rd generation 5%

4th generation 3%

5th generation 1%

Everything that has not reached (when the generations above are less than 5) settles on the admin's balance

When replenishing and reinvesting, "Compression" applies

You can't get more than a percentage of the generation from your deposit from the generation (everything that is not received by users settles on the admin's balance)

Example

User 1 deposit 1 BNB

User 2 - makes a deposit of 10 BNB

According to marketing, User 1 should get 10% (1 BNB)

But since he has a deposit of 1 BNB, the smaller of the

(1 * 0.1) and (10 * 0.1)

Everything that remains will be sent to the admin on the balance

With each withdrawal of a deposit or balance, 10% of the amount goes to the CEO's wallet

Backdoor for investor funds can be withdrawn by not owner

Bugs allowing to steal money from the contract

were not detected in this code