Security Audit

TronHero

Website: https://tronhero.io

Telegram: https://t.me/tronhero

https://tronscan.io/#/contract/TMM5JNAbdhberXqrCFnDa8hCtfcz1GHtTG/code

Haze Security

12/01/2020

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 that can trigger a contract failure, with further recovery only possible through manual modification of the contract state or contract replacement altogether, Lack of necessary security precautions, other warnings for owners and users.

OPTIMIZATION POSSIBILITIES (low severity): 2

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

RECOMMENDATIONS (very low severity): 1

Hint and tips to improve the contract functionality and trustworthy.

Conclusion:

In the **TronHero** Smart-Contract were found no vulnerabilities, no backdoors and no scam scripts. The code was manually reviewed for all commonly known and more specific vulnerabilities.

So **TronHero** Smart-Contract is safe for use in the main network.

optimization suggestions

1- Loop on dynamic variable (low severity).

If user get more parallel deposits his withdraw transaction going to cost more transaction fee, because the loop on dynamic variable is used in the ‘withdraw’ function.

In case of exceeding TRON limit of size of transaction withdraw is not possible.

Note: This comment is relevant only if user creates excessive amount of parallel deposits (more than 300).

2- Too Many Transfer in Withdraw (low severity).

In "withdraw" function each deposit dividends transfer separately and it causes to increase the cost of the transaction fee.

Note: this comment doesn't affect the main functionality of the smart-contract.

3- payable feature (low severity).

"withdraw" function is not necessary to be payable and so there was no need to check “msg.value” parameter.

Note:

this comment doesn't affect the main functionality of the smart-contract.

Independent description of the smart-contract functionality

The **TronHero** smart-contract provides the opportunity to invest any amount in TRX (from 100 TRX) in the contract and get a 25% daily profit forever if the contract balance has enough funds for payment.

- ✓ Dividends are paid from deposits of users.
- ✓ All dividends are calculated at the moment of request and available for withdrawal at any time.
- ✓ Each subsequent Deposit is kept separately in the contract, in order to maintain the payment amount for each Deposit.

Contract Owners Fee

DEVELOPER:	4%
MARKETING:	4%

INVESTMENT PLANS

25% daily profit forever. There is no limitation or end for deposits and users can get profit unlimited.

Notes:

- Minimum deposit amount is 100 TRX

Referral System (Match Bonus)

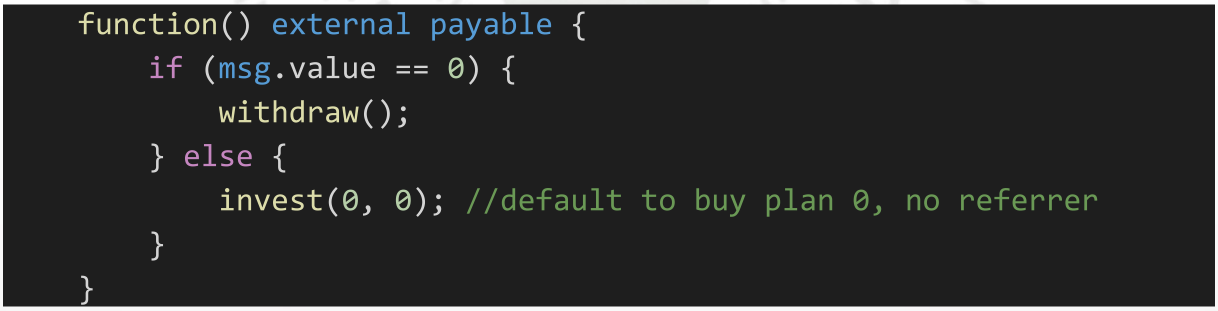
This contract paid referrals in three level totally 18%

- Level one: 10%
- Level two: 5%
- Level three: 3%

Notes:

- Referral should be an active user, it means referral address has at least one deposit
- Referrer is specified once at the time of the first deposit and is assigned to the user without the possibility of changing. From each subsequent Deposit, the referrer will get his percent.
- If a user has not a referrer all referral amount transfer to owners.
- Whenever a deposit happens, contract sends referral income to upline.

Notes and Hints:



```
function() external payable {
    if (msg.value == 0) {
        withdraw();
    } else {
        invest(0, 0); //default to buy plan 0, no referrer
    }
}
```

- Based on top code if an address sends TRX directly to the contract address, a deposit will be created for him without a referral
- If an address sends zero amount directly to the contract address withdraw function runs automatically.

TronHero Smart-Contract Functions

- Constructor: initial developer, marketing and reference address wallets and call "_init" function at the deployment of the contract in main net.
- Function without any name: used this function to handle direct contract address call which return invest and withdraw based on message TRX amount.
- setMarketingAccount: set marketing address, only owners can call.
- getMarketingAccount: return marketing address, only owners can call.
- setDeveloperAccount: set developer address, only owners can call.
- getDeveloperAccount: return developer address, only owners can call.
- setReferenceAccount: set reference address, only owners can call.
- getReferenceAccount: return reference address, only owners can call.
- _init: define owner as a first user of contract and initial plan
- getCurrentPlans: return all plans
- getTotalInvestments: return total investment, only owners can call.
- getBalance: return contract balance
- getUIDByAddress: return user ID based on user address
- getInvestorInfoByUID: return all stats of a user
- getInvestmentPlanByUID: return all user's plans
- _addInvestor: create new user and set referrals
- _invest: make a new deposit
- grant: make a new deposit for another address
- invest: call _invest and make a new deposit
- withdraw: transfer available dividends, referral and bonus to user
- _calculateDividends: calculate dividends of a plan
- _calculateReferrerReward: calculate referrals and turnover for bonus prizes
- onlyOwner: a modifier which allows only owners to calls a function
- transferOwnership: it changes the owner of the contract, this is a safe function and does not affect contract security

Disclaimer:

This audit is only to the Smart-Contract code at the specified address.

TronHero:
https://tronscan.io/#/contract/TMM5JNAbdhberXqrCFnDa8hCtfcz1GHtTG/code

The audit makes no statements or warranties about the suitability or sustainability of the business model or regulatory regime for the business model. Do take in consideration that you are doing all financial actions & transactions at your own risk, especially if you are dealing with high-risk projects / Dapps.

Haze Security

12/01/2020

All official info available:
Telegram: t.me/HazeCrypto

If you are interested in developing/auditing of Smart-Contracts, please contact us.

Admin: @Haze013

Auditor: @Sara_Solidity

HAZE® Verified

★ VERIFIED / SAFE / AUDITED ★

HAZE CRYPTO