November 2020

Security Audit

TronMint

TVfNcBxaMPtVKPmqUs2j4D3DmKXXYArC3p

www.grox.solutions

CRITICAL ISSUES (critical, high severity): **0**

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; high priority unacceptable bugs for deployment at mainnet; critical warnings for owners, customers or investors.

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 (very low severity): **1**

Possibilities to decrease cost of transactions and data storage of Smart-Contracts.

NOTES AND RECOMMENDATIONS (very low severity): **2**

Tips and tricks, all other issues and recommendations, as well as errors that do not affect the functionality of the Smart-Contract.

Conclusion:

In the TronMint Smart-Contract were found no vulnerabilities and no backdoors. The code was manually reviewed for all commonly known and more specific vulnerabilities.

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

AUDIT RESULT:

Optimization possibilities

1. Recording statistical parameters in the blockchain (very low severity):

List of statistical parameters that also increase the cost of transactions and increase the amount of data stored in the blockchain:

```
    uint256 public totalUsers;
    uint256 public totalInvested;
    uint256 public totalWithdrawn;
    uint256 public totalDeposits;
    uint256 levels[3];
    uint256 totalRewards;
```

Recommendation: use events and log this information instead of writing it to the blockchain.

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

Notes

2. Loops over dynamic variables (very low severity):

In the withdraw, `getUserDividends`, `getUserAvailable`, `getUserTotalDeposits`, and `getUserTotalWithdrawn` functions, cycles unrestrictedly grow as the number of deposits increases. If you create a large number of parallel deposits from a single wallet, this can lead to an excessive increase in the transaction cost and incorrect display and processing of information. Notice that there is a limit of size of transaction in TRON Blockchain.

Note: this comment is only relevant for a certain user, if he creates an excessive number of deposits (more than 300) from his wallet.

3. Closing the last payment (very low risk).

If the last user who leaves the project has a payout greater than the smart-contract balance, he will receive the entire available balance, but it will be recorded that the entire payout was closed.

Note: this comment is not critical, since after the smart contract balance is empty, it is unlikely that the contract will be used again. So it makes sense for last user to get at least something.

Independent description of the smart-contract functionality:

The TronMint contract provides the opportunity to invest any amount in TRX (from 50 TRX) in the contract and get a 250% return on investment, if the contract balance has enough funds for payment.

Dividends are payed from deposits of users (Ponzi scheme).

You can create a Deposit by calling the “invest” function and attaching the required amount of TRX to the transaction (from 50 TRX inclusive). Each subsequent Deposit is kept separately in the contract, in order to maintain the payment amount for each Deposit.

The percentage charged to the user starts from 1.5% and depends on the following factors:

- For every 1'000'000 TRX on the maximum smart contract balance +0.1% until 8.5%. This Contract Bonus cannot decrease.
- For every 1 day of non-withdrawal of dividends from the smart contract +0.1% until 5% (when creating repeated deposits, the percent keeps growing).
- For 5 referrals on the 1 level - 0.1%, for 15 referrals - 0.5%, 50 - 1%, 100 - 1.5%, 250 - 2%, 500 - 2.5%.
- For 2'500 TRX invested by user - 0.1%, for 10'000 TRX - 0.5%, 25'000 TRX - 1%, 100'000 TRX - 1.5%, 250'000 - 2%, 1'000'000 TRX - 2.5%.

The maximum total user percent - 20% (1.5 + 8.5 + 5 + 2.5 + 2.5).

Hold Bonus is going to be saved if user withdraws amount less or equal than his referral bonuses (dividends are not concerned). Also if user withdraws part of dividends his Hold Bonus will be saved relatively.

Withdrawals of dividends are available at any time. Withdrawal by the use is performed by calling the “withdraw” function from the address the Deposit was made. All dividends are calculated at the moment of request and available for withdrawal at any time.

Contract owners Commission: part of the invested funds is sent to two addresses:
(marketing address) - 12%.
(the project address) – 2%.
Also 1% of every 1 million TRX on the balance goes to refbonus of first investor (owner).

Three-level referral program: in the “invest” function, you can specify the ID of the referrer. As a result, the referrer will get opportunity to withdraw % of the investor's Deposit according to the following table:

Referrer level	1	2	3
Percentage, %	5-6-7-8-10*	2	1

* - 5% standard, 6% if the total invested referral amount of all levels is more than 100'000 TRX, 7% if more than 250'000 TRX, 8% if more than 500'000 TRX, 10% if more than 1'000'000 TRX.

Also, there is the custom RefBack Percent feature in the smart-contract: any user can set percent that will be returned back to the direct referrals (1 level) using function setRefBackPercent.
Note: percents in the contract have 2 decimals (1% = 100).

Requirements for the referrer: you can not specify your own wallet as a referrer, as well as a wallet that does not have at least one contribution in the smart contract. If wrong referrer is provided, no referrer is set.

The 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 percents.

Owner set start of the project at deploy of the contract (18 of November 6:20 GMT) and every investor who invests before this date gets bonus to his investment amount: standard bonus - 5%, if deposit is more than 100'000 TRX - 10%, if more than 500'000 TRX - 15%, if more than 1'000'000 TRX - 20%.

The contract contains statistical functions that do not require sending transactions:

1. `getContractBalance` – smart contract balance (with decimals, for TRX – 6 characters).
2. `getContractBalanceRate` – the current percentage for a new user.
3. `getUserPercentRate` – the current percentage for the specified user.

4. `getUserDividends` – the current amount of dividends available to withdraw.
5. `getUserCheckpoint` – the date of the last withdrawal in UNIX Time.
6. `getUserReferrer` – the user's referrer.
7. `getUserReferralBonus` – available referral bonuses for withdrawal.
8. `getUserAvailableBalanceForWithdrawal` – total available amount to withdraw (dividends + referral bonuses).
9. `isActive` – whether the user has active deposits.
10. `getUserDepositInfo` – information about the user's specified Deposit (the sequential number of the Deposit starting from 0).
11. `getUserAmountOfDeposits` – the number of user deposits.
12. `getUserTotalDeposits` – the sum of each deposits of the user.
13. `getUserTotalWithdrawn` – user dividend withdrawal amount.
14. `getUserDownlineCount` - amounts of referrals of all levels.
15. `getHoldBonus` - hold bonus of the user.
16. `getUserDownlineBonus` - contract amount of referrals bonus.
17. `getUserWhaleBonus` - contract amount of deposit bonus.
18. `getPrelaunchBonus` - contract prelaunch bonus by amount of deposit.
19. `getUserId` - get ID of user.
20. `getUserById` - get user by ID.
21. `getDirectBusiness` - total Invested amount by referrals of user.
22. `getUserLastDepositDate` - last deposit date (UNIX time).
23. `getUserRefbackPercent` - refback percent of the user (2 decimals, 1% = 100).

November 2020

Disclaimer:

This audit is not a call to participate in the project and applies only to the Smart-Contract code at the specified address.

Do not forget that you are doing all financial actions at your own risk, especially if you deal with high-risk projects.

Warning:

Beware of fake audits.
All official info available on 3 resources only:

Website: **www.grox.solutions**
Telegram: **www.t.me/groxsolutions (@groxsolutions)**
YouTube: **www.youtube.com/c/groxsolutions**

If you have any questions or are interested in developing/auditing of Smart-Contracts, please contact us and we will consult you.

Telegram: **www.t.me/gafagilm (@gafagilm)**
E-mail: **info@grox.solutions**