February 2021

Security Audit

TRONexPRO

TFTbNdj1wSpb4ccT8mp63VSHV4KbqEzQcH

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): **2**

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

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

Note: that is the project from the original TRONex team. Do not confuse with a lot of fakes.

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:

```
    uint public totalDeposits;
    uint public totalInvested;
    uint public totalWithdrawn;
    uint64 refback;
    uint64 bonus;
    uint24[5] refs;
```

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.

2. Transfers inside of referral program (very low severity):

There is 5-level referral program and all bonuses (including refback) is transferred directly to the recipients inside of ‘invest’ function. That actions (up to 6 extra transfers) increase total transaction fee.

Recommendation: that is optimally to use ‘pull payment system’ instead, when user withdraws his available referral bonuses himself.

Notes

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

In the `withdraw`, `getUserDividends`, `getUserAvailable`, `getUserTotalDeposits`, and `getUserTotalWithdrawn` functions, loops unrestrictedly grow as the number of deposits increases. If one creates a large number of parallel deposits from a single wallet, it can lead to an excessive increase of the transaction cost.

Note: maximum amount of deposits from single account - 100.

4. Closing the last payment (very low severity).

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 TRONexPRO contract provides the opportunity to invest any amount in TRX (from 100 TRX) in the contract and get a 200% return on investment, if the contract balance has enough funds for payment.

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

It is allowed to participate in the project only from usual wallet (not smart-contract nor externally owner address).

You can create a Deposit by calling the “invest” function and attaching the required amount of TRX to the transaction (from 100 TRX inclusive).

Each subsequent Deposit is kept separately in the contract, in order to maintain the payment amount for each Deposit.

The daily percentage for user dividends starts from 5% and depends on the following factor:

- Every 12 hours of non-withdrawal of dividends from the smart contract +0.5% (when creating new deposits, the percent keeps growing).

No maximum limit of daily percent is set.

All dividends are calculated at the moment of request and available for withdrawal at any time.

Withdrawal is performed by calling the “withdraw” function from the address the Deposit was made.

Contract owners fee: part of the invested funds is sent to two addresses:

(marketing address) - 5%.
(fund address) - 5%.

There is five-level referral program: in the “invest” function, one can specify the address of the referrer.

As a result, the referrer (upline) will get direct transfer of share of the investor's Deposit according to the following table:

Referrer level	1	2	3	4-5
Percent, %	7	2	1	0.5

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.

Any user that has at least one contribution in the project can specify his own ‘refBackPercent’ - share of the referral bonus that will be returned to his direct referral (only 1 referral level).

To set refBackPercent user must call ‘setRefBackPercent’ function with percent parameter with 2 decimals (means 1% = 100, 100% = 10000).

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

1. `getUserPercentRate` – the current percentage for the specified user.
2. `getUserReferrer` – the user's referrer.
3. `getUserAvailable` – total available amount to withdraw.
4. `isActive` – whether the user has active deposits.
5. `getUserAmountOfDeposits` – the number of user deposits.
6. `getUserTotalDeposits` – the sum of each deposits of the user.
7. `getUserTotalWithdrawn` – user dividend withdrawal amount.
8. `getUserDeposits` - user specified deposits info.
9. `getSiteStats` - total invested value, total deposits, balance of the contract.
10. `getUserStats` - user percent, available to withdraw amount, total user invested, amount of deposits and total withdrawn value.
11. `getUserReferralStats` - user referrer, user refback percent, referrer refback percent and array of amounts of deposits of all-level referrals.

February 2021

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**