Sep. 2021

Security Audit

SUPERMINER

HAECHI LABS

www.haechi.io

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 replacementaltogether; Lack of necessary security precautions; other warnings for owners and users.

OPTIMIZATION

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 SUPERMINER smart-contract were found no vulnerabilities and no backdoors. The code was manually reviewed for all commonly know and more specific vulner abilities.

So SUPERMINER 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
uint256
```

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. Cycles on parallel deposits (very low severity):

In the withdraw, get User Dividends, get User Available, get User Total Deposits, and get User Total Withdrawn functions, cycles unrestrictedly grow as the number of deposits increases.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.

Note: this comment is only relevant for a certain user, if he creates an excessive number of deposits.

3. Closing the

If thelast user who leaves the project has a payout greater than the smart- balance, he will receive the entire available balance, but it will be recorded that contract the entire payout 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 SUPERMINER contract provides the opportunity to invest any amount in BNB in the contract and get 5% return on investment,if the contract balance has enough funds for payment.

You can create a Deposit by calling the “invest” function and attaching the required amount of BNB to the transaction.

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

The percentage on the following factors:

- Withdrawals of dividends are available at any time
- Withdrawal by the user is performed by calling the “withdraw” function from the address the Deposit was made.

All accruals are summed up and available for withdrawal at any time, i.e. it does not matter at what point the user decides to withdraw the dividends.

You can specify the address of the referrer. As a result, the referrer will get opportunity to withdraw 10% of the investor's deposit.

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.

The referrer is specified once at the time of any deposit and is assigned to the user without the possibility of changing. From each subsequent deposit, the referrer will get his percent’s.

The contract contains 11statistical functions that do not require sending transactions:

1. **getContractBalance** - smart contract balance (with decimals, for BNB -6 characters).
2. **getUserDividends** -the current amount of dividends available to withdraw.
3. **getUserCheckpoint** – the date of the last withdrawal in UNIX Time.
4. **getUserReferrer** - the user's referrer.
5. **getUserReferralBonus** - available referral bonuses for withdrawal.
6. **getUserAvailable**– total available amount to withdraw (dividends + referral bonuses).
7. **isActive** – whether the user has active deposits.
8. **getUserDepositInfo** – information about the user's specified Deposit (the sequential number of the Deposit starting from 0).
9. **getUserAmountOfDeposits**– the number of user deposits.
10. **getUserTotalDeposits**– the sum of each deposits of the user.
11. **getUserTotalWithdrawn**– user dividend withdrawal amount.

Security Audit

SUPERMINER

HAECHI LABS

Sep. 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.

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

Telegram: **@heachi**
E-mail: **info@hachi.io**