BINANCE
SMART CHAIN

Security Audit

SQUADUP

Website: https://xxxx

Haze Security
08/17/2021

Contracts

SQUADUP:
https://bscscan.com/address/xxxx#code

exchange:
https://bscscan.com/address/xxxx#code

stake:
https://bscscan.com/address/xxxx#code

farm:
https://bscscan.com/address/xxxx#code

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.

MEDIUM ISSUES (high, medium severity): 1

The owner's privileges, access and permission that cause changes in the contract results and parameters, enable/disable main modules and features, exclude/include specific users.

ERRORS, BUGS AND WARNINGS (medium, low severity): 0

Bugs can negatively affect the usability of a program, errors that can trigger a contract failure, Lack of necessary security precautions, other warnings for owners and users, warning codes that are valid code but the compiler thinks are suspicious.

OPTIMIZATION (low severity): 1

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

RECOMMENDATIONS (very low severity): 0

Hint and tips to improve contract functionality and trustworthiness.

Conclusion:

In the **SQUADUP** Smart-Contract were found no vulnerabilities, no backdoors and no scam scripts.

The code was tested with compatible compilers and simulate manually reviewed for all commonly known and specific vulnerabilities.

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

Optimization suggestions

1- **Loop on the dynamic variable** – stake contract (low severity).

If the user gets more parallel deposits his withdrawal transaction going to cost more transaction fees because the loop on the dynamic variable is used in the 'withdraw' function.

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

Note:

This comment is relevant only if a user creates an excessive amount of parallel deposits (more than 100).

2- **Owner Privileges** (medium severity):

The owner has access to change parameters in the MasterChef contract. These privileges can limit change the output rate of rewards

- updateMultiplier
- updateSqdPerBlock

Independent Description of the smart-contract functionality

The SQUADUP is a token deployed in the Binance blockchain and users can earn it in farms and staking. There is a special exchange contract that manages buy and sell orders.

- ❖ It is a standard BEP20 Token with a mint and burn feature. Only the exchange contract has the privilege of mint and mint
- ❖ All libraries which were used for calculation and the token in the contract are standard and safe.

Token Info (all information based on audit date)

- Total Supply: xxx SQD
- Holders: x addresses
- Total Transactions: x
- Name: SquadUp
- Symbol: SQD
- Decimals: 18
- Contract: xxxx:

Mint Token

Mint can only call by the owner which is the exchange contract.

The owner of the SQUADUP token contract can not be changed.

Exchange Contract

In the exchange contract, users can buy and sell SQD tokens.

Buy Fees

In each transaction, 10% transfer to the referrer and owner

- ❖ owner: 8%
- ❖ Referrer: 2%

Note:

- The referrer address should have some tokens in his wallet
- The user can not use his address as the referrer
- If there isn't a valid referrer address, the referrer fee will remain in the exchange contract

Sell Fees

There isn't any fee for sell transactions.

Buy & Sell Price

The pricing system is a fork of the "Ethereum Gold" project.

Ethereum Gold Whitepaper, Price System:

> *increases the token price as tokens are bought and decreases the price as tokens are sold. When tokens are bought they are minted by the contract and added to the total supply, the Ethereum collected in the sale is stored safely in the contract. When tokens are sold exchange burns them and decreases the total supply.*

Note:

- The initial token price is 0.005 BNB
- The token price incremental is 0.00001 BNB

Stake Contract

The Stake smart contract provides the opportunity to invest any amount in SQD (from 1 SQD) in the contract and get 104% to 616% return on investment in 1 to 28 days if the contract balance has enough funds for payment.

- ✓ It is an ROI System and High-Risk, invest by enough investigation and knowledge
- ✓ Dividends are paid from deposits of users.
- ✓ All dividends are calculated at the moment of request and available for withdrawal only once a day
- ✓ Each subsequent Deposit is kept separately in the contract, to maintain the payment amount for each Deposit.

Contract Owners Fee

No owner fee

SIX INVESTMENT PLANS

Plans	Total Return	Daily Profit	Days	Withdraw time
1	110%	110%	1	Any Time
2	120%	40%	3	Any Time
3	210%	30%	7	Any Time
4	364%	26%	14	Any Time
5	504%	24%	21	Any Time
6	616%	22%	28	Any Time

- ❖ The minimum deposit amount is 0.05 BNB
- ❖ 10% of each withdrawal amount will be deducted and remain in the contract, so the final total result is 10% less than the above table numbers

Referral System (Match Bonus)

This contract pays referrals in three-level with a totally of 8%

- Level one: 5%
- Level two: 2.5%
- Level three: 0.5%

Notes:

- Referral should be an active user. it means the referral address has at least one deposit

Plans Daily Profit

Each 1 SQD token increases the daily profit of all plans by 0.001%

Masterchef

It is a contract that controls the farms.

- Farms can be created and updated
- Each token can only have one farm
- Users can deposit in farms
- Deposit Fees:
    - There is a fee in each farm that transfers a specific amount of tokens to the owner wallet
    - The maximum deposit fee is 5%
- Withdraw Fee:
    - There is a fee in each farm that transfers a specific amount of tokens to the owner wallet
    - The maximum withdrawal fee is 5%

- Users can increase their investment
- Users can withdraw their investments anytime
- On each new deposit and withdrawal, users will receive earned rewards.
- Users can force withdraw their total investment without receiving the rewards.

Disclaimer:

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

SQUADUP:
https://bscscan.com/address/0xaaef057b1969354865ecf7a06b620de615237d0c#code

Haze Security is a 3rd party auditing company who works on audits based on client requests. And as a professional auditing firm, we check on the contract for any vulnerabilities, backdoors, and/or scam scripts.

Therefore:

We are not financial advisors nor do we partner with the contract owners

Operations and website administration is fully on the client's side

We do not have influence over client operations, which can lead to website changes, withdrawal function closes, etc. One always has the option to do this through the contract.

Any concerns about the project themselves need to be raised directly to the project owners and not through Haze Security.

Investors are not in any way obliged, coerced or influenced to invest in projects audited by Haze Security.

We are not responsible for your funds or guarantee you profits.

We highly recommend that investors do their own research and gain crypto experience before investing

To report any scam, malpractices and irregularities, please send a message via Telegram to @Haze013 or @Sara_Solidity for blacklisting.

Haze Security

08/17/2021

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

Admin: @Haze013

Auditor: @Sara_Solidity

All official info available:

Website: https://hazecrypto.net/squadup

Telegram Channel: t.me/HazeCrypto

Telegram Community: t.me/HazecryptoCommunity

Twitter: twitter.com/HazeCryptoTM

Instagram: instagram.com/HazeCryptoTM