BINANCE SMART CHAIN

Security Audit

BNBFARM

Contract:
https://bscscan.com/address/0x80A53390D43601B188291a5484C67f060cbfc3cc#code

Haze Security
03/22/2021

www.hazecrypto.net

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 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): 1

Hint and tips to improve contract functionality and trustworthy.

Conclusion:

In the **BNBFARM** 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 **BNBFARM** Smart-Contract is safe for use in the Binance Smart Chain main network.

Optimization suggestions

1- Loop on the dynamic variable (low severity).

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

In case of 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).

Independent description of the smart-contract functionality

The **BNBFarm** smart-contract provides the opportunity to invest any amount in BNB (from 0.05 BNB) in the contract and get a 120 to unlimited return on investment in four different plans 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 every 36 hours
- Each subsequent Deposit is kept separately in the contract, in order to maintain the payment amount for each Deposit.

Launch Date: Wed Mar 24 2021 16:00:00 GMT+0000

Contract Owners Fee

DEVELOPER: 4%

MARKETING: 4%

FUND: 4%

FOUR INVESTMENT PLANS

Plans	Total Return	Days	Daily Profit
1	unlimited	forever	5%
2	200%	20	10%
3	150%	10	15%
4	120%	6	20%

Notes:

- Minimum deposit amount is 0.05 BNB

Referral System (Match Bonus)

This contract paid referrals in three level totally 8.1%

- Level one: 4%
- Level two: 2%
- Level three: 2%
- Return to investor: 0.1%

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.

Withdraw Limit:

- users can only withdraw every 36 hours

Notes and Hints:

- In this contract based on function “grant”, user can send BNB create new deposit for another address and his address is upline.

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

- Based on above code if an address sends BNB 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.

BNBFarm Smart-Contract Functions

- Constructor: initial developer, marketing and fund address wallets and call "_init" function at the deployment of the contract in mainnet.
- Function without any name: used this function to handle direct contract address call which return invest and withdraw based on message BNB amount.
- setMarketingAccount: set new marketing address
- getMarketingAccount: only called by owner and return marketing address.
- setDeveloperAccount: set new developer address
- getDeveloperAccount: only called by owner and return developer address.
- setReferenceAccount: set new fund address
- getReferenceAccount: only called by owner and return reference address.
- _init: define owner as a first user of contract and initial plans
- getCurrentPlans: return all plans
- getTotalInvestments: return total investment for only owners
- 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

Disclaimer:

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

BNBFARM:
https://bscscan.com/address/0x80A53390D43601B188291a5484C67f060cbfc3cc#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

03/22/2021

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

Website: https://hazecrypto.net/bnbfarm/

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

Admin: @Haze013

Auditor: @Sara_Solidity