KICK START

Blockchain Security | Smart Contract Audits

Audit

Security Assessment

06.January,2023

TABLE OF CONTENTS

Disclaimer

kickstartlabs reports are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team. kickstartlabsdo not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...) kickstartlabs.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. kickstart labs Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

Network

Binance Smart Chain

Website

infinitybeans.app

Litepaper

docs.infinitybeans.app

Contract Link

InfinityBeans | Address
0x7eebb570d32ccb5717fb19ad83060b1fc6cba45b | BscScan

NFT Addresses:
Silver:
https://bscscan.com/address/0x48e7b9314ac782f4087672d7179
8ca790ed49ad7

Gold:
https://bscscan.com/address/0xa6ef43b0f856b40b751c7c123f
d7fac34142557c

Platinum:
https://bscscan.com/address/0x69a044302974e4c310bed881b
b7a487024735114

Methodology

The auditing process follows a routine series of steps:

Code review that includes the following:

i) Review of the specifications, sources, and instructions provided to kickstart labs to make sure we understand the size, scope, and functionality of the smart contract

ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.

iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.

Imported Packages

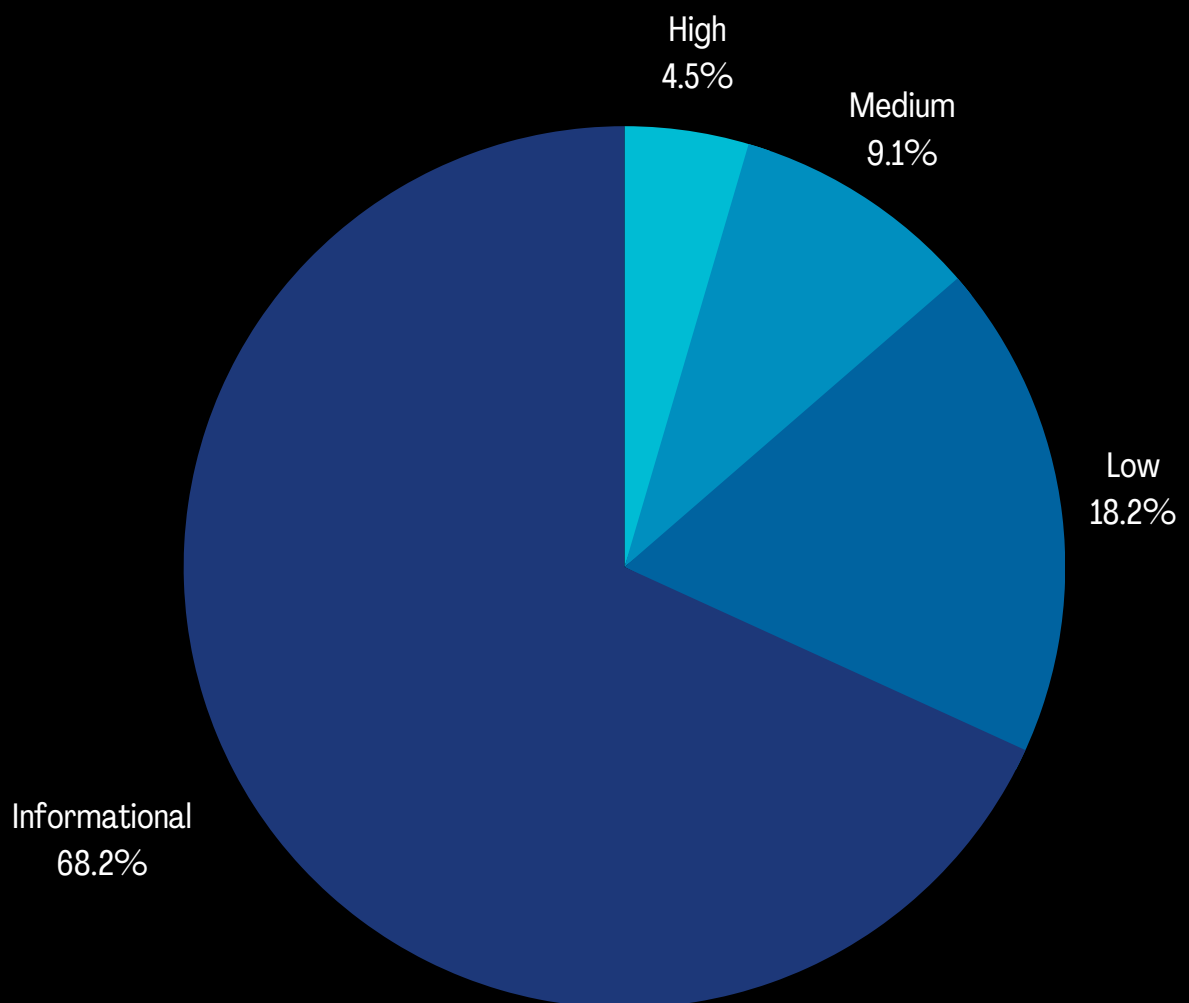- IERC721
- Context
- Ownable
- InfinityBeans
- SafeMath

Tested contract files

This audit covered the following files listed below with a SHA-1 Hash.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.
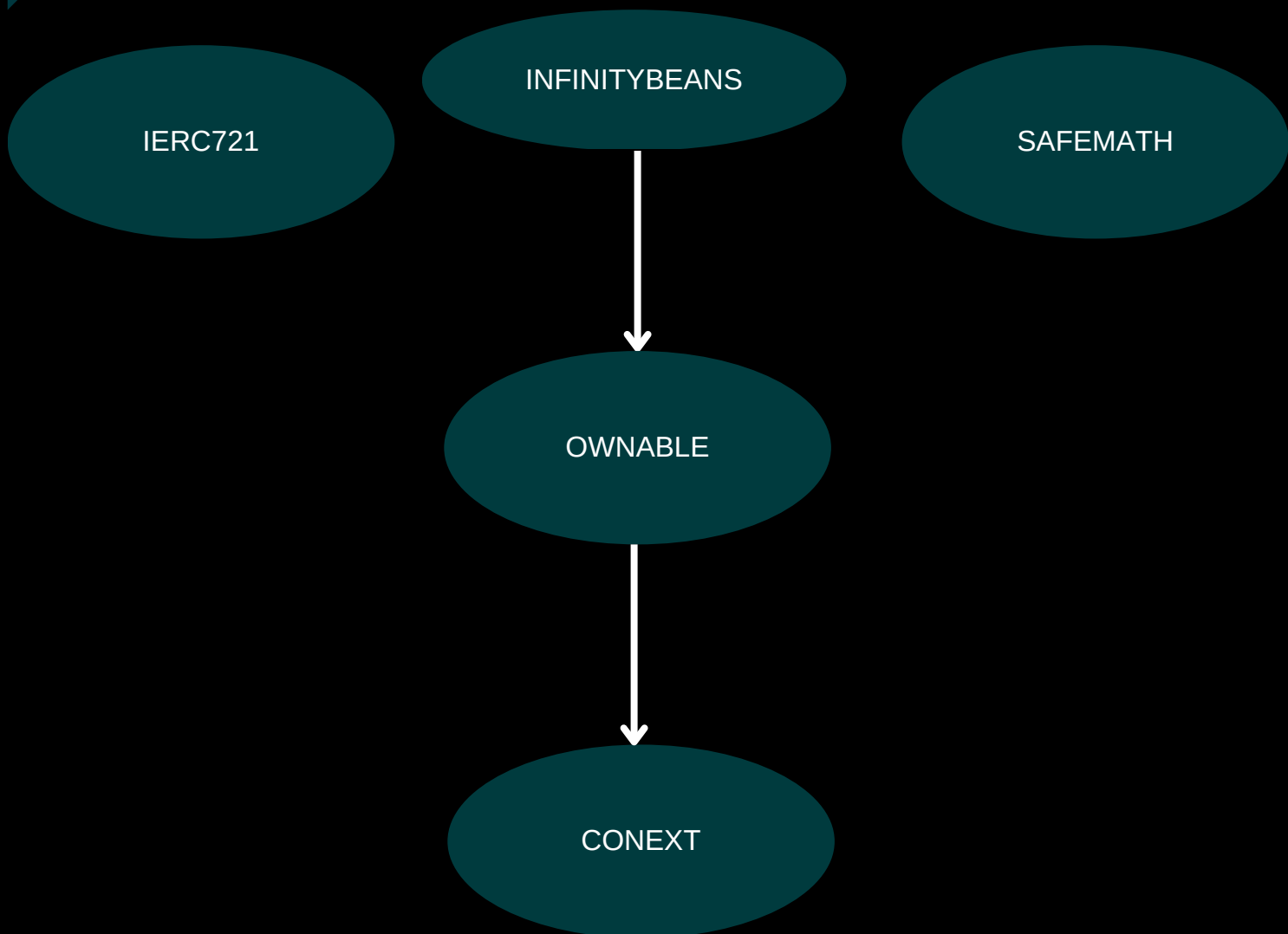
Vulnerability & Risk Level

High
4.5%

Medium
9.1%

Low
18.2%

Informational
68.2%

Inherit Graph

INFINITYBEANS

IERC721

SAFEMATH

OWNABLE

CONEXT

Scope of work

The scope of the audit is the main contract (usual the same name as team appended with .sol).
We will verify the following claims:
1. Overall checkup (Smart Contract Security)

Write functions of contract

1. changeFeeReceiver (0x7c08b964)

2. hireMiners (0x7523b837)

3. rehireMiners (0x5279c9a0)

4. renounceOwnership (0x715018a6)

5. setBuyLimit (0x00c9ac8c)

6. setDepositFeePercent (0x2052eb77)

7. setMaxWallet (0xabe57e70)

8. setMinBuy (0x860779e7)

9. setNftAddresses (0xf0189acd)

10. setRefPercent (0x6fa4f5f7)

11. setWhitelistedUsers (0x34786ec8)

12. setWithdrawFeePercent (0x447cb896)

13. startMining (0x21b79d98)

14. startPublicRound (0x44210174)

15. startWhitelistRound (0x34783c4d)

16. takeProfit (0x70c10578)

17. transferOwnership (0xf2fde38b)

High Issues

01

The ROI System

The system used is called ROI and must be considered HIGH-RISK.

Users' principal deposits cannot be withdrawn, users can get dividends and referral commission. Dividends are paid from deposits of other users. Do always invest with proper knowledge and investigation.

Medium Issues

01
whitelist (enable/disable)

The owner can enable or disable whitelist round anytime (only whitelisted address can deposit when enable)

02
NFT address Variable

The owner can change all three NFT addresses (if any NFT address set to wrong address, deposit will stop)

Low Issues

01 Public Round

The owner can enable or disable public round anytime

02 Whitelist

The owner can include or exclude any address from whitelist

03 Maximum Deposit

The owner can set the maximum deposit amount (1 BNB minimum)

04 Limits

The owner can set the limits according to TVL to manage maximum deposit

Informational

01 **Deposit Fee**

The owner can set the deposit fee (5% maximum)

02 **Withdraw Fee**

The owner can set the withdraw fee (5% maximum)

03 **Referral Reward**

The owner can set the referral reward (1% minimum and10% maximum)

04 **Minimum Deposit**

The owner can set the minimum deposit amount (1 BNB maximum)

05 **Owner Wallet**

The owner can change the owner's wallet (it doesn't affect deposit, withdraw and compound)

06 **Fee Receiver**

The owner can change the fee receiver wallet (it doesn't affect deposit, withdraw and compound)

Informational

07 INVESTMENT PLAN

The basic interest rate based on the audit date is 8% daily
The daily rate will be changed based on the deposit and
withdrawal of the other users

08 Contract Owners Fee

- Deposit (hireMiners) Fee : 5%
- Withdraw (takeProfit) Fee : 5%

Informational

09 Deposit

Users can buy miners by BNB. Miner price will be calculated at the time of deposit
Miner Price Formula: Deposit amount / (Deposit amount + Contract Balance) * Market Value
Miners will produce credits and users can sell credits to earn a profit
95% will be added to the contract as user deposit
5% will be paid to the owner

10 Compound

User can compound their available credits and buy more miners
Miner price will be calculated based on the mentioned formula in the deposit section and real-time numbers of market eggs and contract balance
User can compound any time
No fees on compound

Informational

11 Withdraw

Users can sell credits produced by the miners
Withdraw amount (BNB) Formula: user credits / (user credits + Market Value) * Contract Balance
95% will be paid to the user
5% will be paid to the owner

12 Market Value

It is an amount that will be defined in the initial of the contract and will be changed by deposit, withdrawal and compound
The initial amount is: 108000000000
20% of each deposit, withdrawal, and compound will be added to "Market Value"
An increase in the "Market Value" will reduce the daily rate and increase sustainability

Informational

13 User Credits

each miner will produce one credit each second
Miners produce credits maximum of 12.5 days (300 hours) if user ROI is 8%
Miners produce credits maximum of 10 days (240 hours) if user ROI is 10%
Miners produce credits maximum of 8.3 days (200 hours) if user ROI is 12%
Miners produce credits maximum of 6.6 days (160 hours) if user ROI is 15%
Users should try to withdraw or compound their produced credits within defined duration.
After withdrawal or compound, miners will start working again
Users can sell many times without any limit
If the contract balance is less than the user's withdrawable amount, then user will not be able to withdraw

14 Referral System

The contract pays a 10% referral commission over one level
The commission is 10% of the deposit amount
The commission will be paid directly to the user
User can not use his own wallet as a referral for himself (tax fee receiver wallet get the 10% referral commission in this case)

Informational

- ROI boost system

Three types of NFTs available that can be used to boost the ROI of the user
1- Silver 10%
2- Gold 12%
3- Platinum 15%
User ROI update only on deposit after receiving the NFT
If user has all three kinds of NFT, only the max ROI (Platinum 15%) will apply
Two NFTs of same kind can not double the ROI
User get the miners according to the NFT he is holding

Conclusion

The INFINITYBEANS Smart-Contract found no vulnerabilities,
no backdoors, and no scam scripts.
The code was tested with compatible compilers and simulated
and manually reviewed for all commonly known and specific vulnerabilities.
So, INFINITYBEANS Smart-Contract is safe for use in the
Binance Smart Chain main network.