CONTRACT WOLF

Blockchain Security - Smart Contract Audits

Security Assessment

April 16, 2022

Disclaimer 3

Scope of Work & Engagement 3

Links 4

Project Description 5

Logo 5

Risk Level Classification 6

Methodology 7

Used Code from other Frameworks / Smart Contracts (Imports) 8

Token Description 9

Inheritance Graph 10

Overall Checkup 11

Verify Claim 12

Write Functions of Contract 13

Audit Result 14

Audit Comments 15

Disclaimer

ContractWolf.io audits and reports should not be considered as a form of project's "advertisement" and does not cover any interaction and assessment from "project's contract" to "external contracts" such as Pancakeswap or similar.

ContractWolf does not provide any warranty on its released reports.

ContractWolf should not be used as a decision to invest into an audited project and is not affiliated nor partners to its audited contract projects.

ContractWolf provides transparent report to all its "clients" and to its "clients participants" and will not claim any guarantee of bug-free code within it's **SMART CONTRACT**.

ContractWolf presence is to analyze, audit and assess the client's smart contract's code.

Each company or projects should be liable to its security flaws and functionalities.

Scope of Work

Juicy Beanz team agreed and provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract.

The goal of this engagement was to identify if there is a possibility of security flaws in the implementation of the contract or system.

ContractWolf will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, whitepaper and repository which has been provided by **Juicy Beanz.**

Network

Binance Smart Chain (BEP20)

Contract link

https://bscscan.com/address/0x1446a6562625257ac3a1e92a8090e34ae3116b26

Website

https://juicybeanz.com

Telegram

https://t.me/JuicyBeanzOfficial

Twitter

https://twitter.com/JuicyBeanz_BSC

Others

Mudra Manager

https://mudra.website/?certificate=yes&type=0&lp=0x2e4143cba544c484d7b3b9bf53eb880c3a5a2a7f

Poo Coin

https://poocoin.app/tokens/0x1446a6562625257ac3a1e92a8090e34ae3116b26

Description

Juicy Beans ($BNZ) is the biggest BINANCE rewards Token on the Binance Smart Chain! Not just that, JUICY BEANZ will also serve as the governance Token for BEANZ ON TOAST our upcoming nft and p2e concept.

Logo

Risk Level Classification

Risk Level represents the classification or the probability that a certain function or threat that can exploit vulnerability and have an impact within the system or contract.
Risk Level is computed based on CVSS Version 3.0

Level	Value	Vulnerability
Critical	9 - 10	An Exposure that can affect the contract functions in several events that can risk and disrupt the contract
High	7 - 8.9	An Exposure that can affect the outcome when using the contract that can serve as an opening in manipulating the contract in an unwanted manner
Medium	4 - 6.9	An opening that could affect the outcome in executing the contract in a specific situation
Low	0.1 - 3.9	An opening but doesn't have an impact on the functionality of the contract
Informational	0	An opening that consists of information's but will not risk or affect the contract

Auditing Approach

Every line of code along with its functionalities will undergo manual review to check its security issues, quality, and contract scope of inheritance. The manual review will be done by our team that will document any issues that there were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:

    - Review of the specifications, sources, and instructions provided to ContractWolf to make sure we understand the size, scope, and functionality of the smart contract.
    - Manual review of code, our team will have a process of reading the code line-by-line with the intention of identifying potential vulnerabilities and security flaws.

2. Testing and automated analysis that includes:

    - Testing the smart contract functions with common test cases and scenarios, to ensure that it returns the expected results.

3. Best practices review, the team will review the contract with the aim to improve efficiency, effectiveness, clarifications, maintainability, security, and control within the smart contract.

4. Recommendations to help the project take steps to secure the smart contract.

Used Code from other Frameworks/Smart Contracts (Direct Imports)

Imported Packages

- Auth
- DividendDistributor
- IBEP20
- IDEXFactory
- IDEXRouter
- IDividendDistributor
- JuicyBeanz
- SafeMath

Description

Optimization enabled: No

Decimal: 18

Symbol: $BNZ

Max / Total supply: 100,000,000

Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	2	1	4	1

Exposed Functions

Version	Public	Private	External	Internal
1.0	16	0	57	26

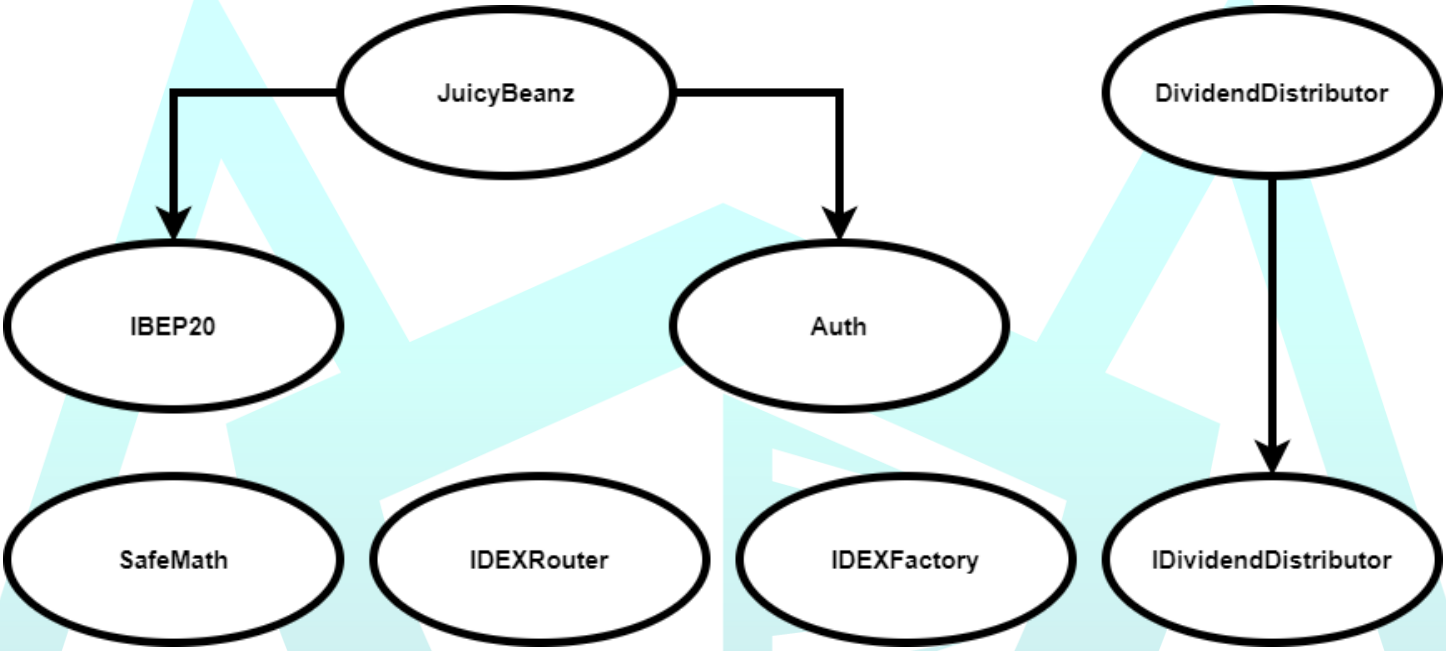
State Variables

Version	Total	Public
1.0	32	31

Capabilities

Version	Solidity Versions Observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	v0.8.4		Yes	No	No

Inheritance Graph



Correct implementation of Token Standard

Tested	Verified
✓	✗

Overall Checkup (Smart Contract Security)

Tested	Verified
✓	✓

Function	Description	Exist	Tested	Verified
TotalSupply	Information about the total coin or token supply	✓	✓	✓
BalanceOf	Details on the account balance from a specified address	✓	✓	✓
Transfer	An action that transfers a specified amount of coin or token to a specified address	✓	✓	✓
TransferFrom	An action that transfers a specified amount of coin or token from a specified address	✓	✓	✓
Approve	Provides permission to withdraw specified number of coin or token from a specified address	✓	✓	✓

Verify Claims

Statement	Exist	Tested	Deployer
Renounce Ownership	–	–	–
Mint	–	–	–
Burn	–	–	–
Block	–	–	–
Pause	–	–	–

Legend

Attribute	Symbol
Verified / Can	✓
Verified / Cannot	✗
Unverified / Not checked	⚑
Not Available	–

Write Functions of Contract

1. approve
2. approveMax
3. authorize
4. claimDividend
5. clearBuybackMultiplier
6. cooldownEnabled
7. manualSend
8. setAutoBuybackSettings
9. setBuyFees
10. setBuyTxLimitInPercent
11. setBuybackMultiplierSettings
12. setDistributionCriteria
13. setDistributorSettings
14. setFeeReceivers
15. setIsDividendExempt
16. setIsFeeExempt
17. setIsTimelockExempt
18. setIsTxLimitExempt
19. setMaxWalletPercent
20. setSellFees
21. setSellTxLimitInPercent
22. setSwapBackSettings
23. setTargetLiquidity
24. setTokenDistributor
25. tradingStatus
26. transfer
27. transferFrom
28. transferOwnership
29. triggerManualBuyback
30. unauthorize

AUDIT PASSED

Low Issues

A floating pragma is set (SWC - 103)	L: 61 C: 59
State variable visibility is not set (SWC - 108)	L: 224 C: 12, L: 233 C: 11, L: 234 C: 12, L: 235 C: 15, L: 237 C: 14, L: 238 C: 33, L: 239 C: 33, L: 252 C: 12, L: 254 C: 9, L: 393 C: 12, L: 394 C: 12, L: 395 C: 12, L: 396 C: 12, L: 397 C: 12, L: 399 C: 12, L: 411 C: 12, L: 419 C: 33, L: 420 C: 54, L: 421 C: 30, L: 422 C: 30, L: 423 C: 30, L: 424 C: 30, L: 428 C: 12, L: 431 C: 12, L: 436 C: 12, L: 439 C: 12, L: 443 C: 12, L: 444 C: 12, L: 445 C: 12, L: 446 C: 12, L: 447 C: 12, L: 448 C: 12, L: 449 C: 12, L: 455 C: 12, L: 456 C: 12, L: 459 C: 12, L: 460 C: 12, L: 461 C: 12, L: 462 C: 12, L: 466 C: 12, L: 467 C: 12, L: 468 C: 12, L: 469 C: 12, L: 470 C: 12, L: 472 C: 24, L: 473 C: 12, L: 487 C: 9,
Potential use of "block.number" as source of randonmness (SWC - 120)	L: 698 C: 19, L: 798 C: 22, L: 825 C: 15, L: 854 C: 14, L: 874 C: 15

Audit Comments

- Deployer cannot renounce ownership
- Deployer cannot mint after initial deployment
- Deployer cannot burn tokens
- Deployer cannot block user
- Deployer cannot pause contract
- Deployer can transfer ownership
- Deployer can set max wallet percentage
- Deployer can set trading status
- Deployer can set trading cooldown
- Deployer can set authorized/unauthorized address
- Authorized can set token distributor
- Authorized can set buybacks
- Authorized can set buyback settings
- Authorized can set max transaction limit with an indefinite amount
- Authorized can set fees with an indefinite amount
- Authorized can set fee receivers
- Authorized can set target liquidity
- Authorized can send BNB to marketing wallet
- Authorized can set distribution criteria
- Authorized can set gas for distributor
- Authorized can include/exclude address from fees
- Authorized can include/exclude address from transaction limit
- Authorized can include/exclude address from trading cooldown
- Authorized can include/exclude address from dividends

CONTRACTWOLF

Blockchain Security - Smart Contract Audits