CFG NINJA AUDITS

Security Assessment

BFCToken Token

September 17, 2023

Audit Status: Fail

Audit Edition: Pinksale

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
Critical	Danger or Potential Problems.
High	Be Careful or Fail test.
Low	Pass, Not-Detected or Safe Item.
Informational	Function Detected

Manual Code Review Risk Results

Contract Priviledge	Description
Buy Tax	4%
Sale Tax	4%
Cannot Sale	Pass
Cannot Sale	Pass
Max Tax	100%
Modify Tax	Yes
Fee Check	Pass
Is Honeypot?	Detected
Trading Cooldown	Not Detected
Can Pause Trade?	Not Detected.

Contract Priviledge	Description
Pause Transfer?	Not Detected
Max Tx?	Pass
Is Anti Whale?	Not Detected
Is Anti Bot?	Not Detected
Is Blacklist?	Not Detected
Blacklist Check	Pass
is Whitelist?	Not Detected
Can Mint?	Fail
Is Proxy?	Not Detected
Can Take Ownership?	Not Detected
Hidden Owner?	Not Detected
Owner	0x502e1A4eCA726C185D8bdbBa120Dc8Ac189e9d01
Self Destruct?	Not Detected
External Call?	Not Detected
Other?	Detected
Holders	1
Auditor Confidence	High Risk

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Project Overview

Token Summary

Parameter	Result
Address	0x6cb2Fa05765288d90E708F7e152c64c43FeE8A6e
Name	BFCToken
Token Tracker	BFCToken (BFC)
Decimals	18
Supply	100,000
Platform	Binance Smart Chain
compiler	v0.8.19+commit.7dd6d404
Contract Name	BFCToken
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/token/0x6cb2Fa05765288d90E708F7e152c64c43FeE8A6e#code
Payment Tx	Corporate

Main Contract Assessed Contract Name

Name	Contract	Live
BFCToken	0x6cb2Fa05765288d90E708F7e152c64c43FeE8A6e	Yes

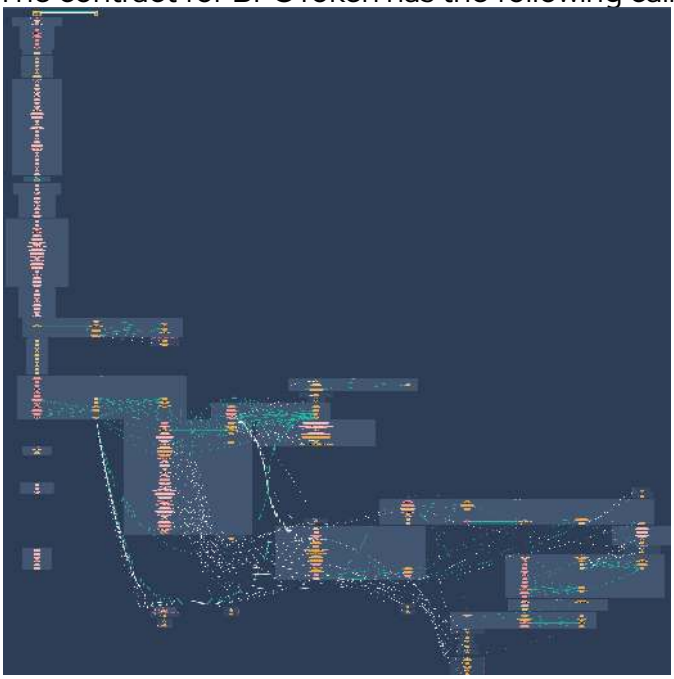
TestNet Contract was Not Assessed

Solidity Code Provided

SolID	File Sha-1	FileName
BFC	02fa809a406315b4955d1d7211e0ba0f89f5cfed	BFCToken.sol
BFC		
BFC		
BFC		
BFC		
BFC		

Call Graph

The contract for BFCToken has the following call graph structure.



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	BFCToken.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	BFCToken.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	BFCToken.sol	L: 0 C: 0
SWC-103	Fail	A floating pragma is set.	BFCToken.sol	L: 15 C: 0
SWC-104	Pass	Unchecked Call Return Value.	BFCToken.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	BFCToken.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	BFCToken.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	BFCToken.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	BFCToken.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	BFCToken.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	BFCToken.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	BFCToken.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	BFCToken.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	BFCToken.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	BFCToken.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	BFCToken.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	BFCToken.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	BFCToken.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	BFCToken.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	BFCToken.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	BFCToken.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	BFCToken.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	BFCToken.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	BFCToken.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	BFCToken.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	BFCToken.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	BFCToken.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	BFCToken.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	BFCToken.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	BFCToken.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	BFCToken.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	BFCToken.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	BFCToken.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	BFCToken.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	BFCToken.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	BFCToken.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	BFCToken.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

Smart Contract Vulnerability Details

SWC-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

References:

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen.

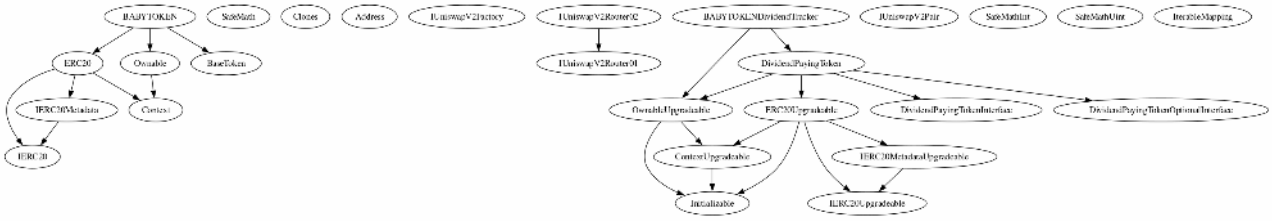
Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.

Inheritance

The contract for BFCToken has the following inheritance structure.



Smart Contract Advance Checks

ID	Severity	Name	Result	Status
BFC-01	Low	Potential Sandwich Attacks.	Pass	Not Detected
BFC-02	Informational	Function Visibility Optimization	Pass	Not Detected
BFC-03	Low	Lack of Input Validation.	Fail	Detected
BFC-04	High	Centralized Risk In addLiquidity.	Fail	Detected
BFC-05	Low	Missing Event Emission.	Fail	Detected
BFC-06	Low	Conformance with Solidity Naming Conventions.	Pass	Not Detected
BFC-07	Low	State Variables could be Declared Constant.	Pass	Not Detected
BFC-08	Low	Dead Code Elimination.	Pass	Not Detected
BFC-09	High	Third Party Dependencies.	Pass	Not Detected
BFC-10	High	Initial Token Distribution.	Pass	Not Detected
BFC-11	High	claimStuckTokens can claim own tokens.	Pass	Not Detected
BFC-12	High	Centralization Risks In The X Role	Pass	Not Detected
BFC-13	Informational	Extra Gas Cost For User..	Pass	Not Detected
BFC-14	Medium	Unnecessary Use Of SafeMath	Fail	Detected
BFC-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not Detected

ID	Severity	Name	Result	Status
BFC-16	Medium	Taxes can be up to 100%	Fail	Detected
BFC-17	Logical Issue	Highly Permissive Role Access.,`	Pass	Not Detected
BFC-18	Critical	Stop Transactions by using Enable Trade.	Pass	Not Detected

BFC-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	Low	BFCToken.sol: L: 1055 C: 14	Detected

Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the .

Remediation

We advise the client to add the check for the passed-in values to prevent unexpected errors as below:

```
...
 require(receiver != address(0), "Receiver is the zero address");
...
...
require(value X limitation, "Your not able to do this function");
...
```

We also recommend customer to review the following function that is missing a required validation. .

BFC-04 | Centralized Risk In addLiquidity.

Category	Severity	Location	Status
Coding Style	High	BFCToken.sol: L: 1464 C: 14	Detected

Description

uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this), tokenAmount, 0, 0, owner(), block.timestamp);

The addLiquidity function calls the uniswapV2Router.addLiquidityETH function with the to address specified as owner() for acquiring the generated LP tokens from the BFC-WBNB pool.

As a result, over time the _owner address will accumulate a significant portion of LP tokens.If the _owner is an EOA (Externally Owned Account), mishandling of its private key can have devastating consequences to the project as a whole.

Remediation

We advise the to address of the uniswapV2Router.addLiquidityETH function call to be replaced by the contract itself, i.e. address(this) , and to restrict the management of the LP tokens within the scope of the contract's business logic. This will also protect the LP tokens from being stolen if the _owner account is compromised. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or via smart-contract based accounts with enhanced security practices, f.e. Multisignature wallets.

1. Indicatively, here are some feasible solutions that would also mitigate the potential risk:
2. Time-lock with reasonable latency, i.e. 48 hours, for awareness on privileged operations;
3. Assignment of privileged roles to multi-signature wallets to prevent single point of failure due to the private key;

Introduction of a DAO / governance / voting module to increase transparency and user involvement

Project Action

BFC-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	Low	BFCToken.sol: L: 1055 C: 14	Detected

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.The linked code does not create an event for the transfer.

Remediation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

BFC-14 | Unnecessary Use Of SafeMath

Category	Severity	Location	Status
Logical Issue	Medium	BFCToken.sol: L: 802 C: 14	Detected

Description

The SafeMath library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations
will automatically revert in case of integer overflow or underflow.
library SafeMath {
An implementation of SafeMath library is found.
using SafeMath for uint256;
SafeMath library is used for uint256 type in contract.

Remediation

We advise removing the usage of SafeMath library and using the built-in arithmetic operations provided by the
Solidity programming language

Project Action

BFC-16 | Taxes can be up to 100%.

Category	Severity	Location	Status
Logical Issue	Medium	BFCToken.sol: L: 1078 C: 20	Detected

Description

The current definition of taxes can be set up to 100% for specific wallets, we suggest to modify the function not to be dynamic but to be a static resolution.

```
function setSniperFee(address[] memory account, uint8 _sellFee, uint8 _buyFee) public
onlyOwner {
  for (uint256 i = 0; i < account.length; i++) {
    if (_sellFee > 0) {
      sellSniperFee[account[i]] = _sellFee;
    }
    if (_buyFee > 0) {
      buySniperFee[account[i]] = _buyFee;
    }
  }
}
```

due to the logic written in here may results in a honeypot.

Remediation

We advise the team to review the following logic..

Project Action

Technical Findings Summary

Classification of Risk

Severity	Description
Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
High	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
Low	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
Critical	1	0	0
High	1	0	0
Medium	1	0	0
Low	2	0	0
Informational	0	0	0
Total	5	0	0

Social Media Checks

Social Media	URL	Result
Twitter		Fail
Other		Fail
Website		Fail
Telegram	Fail	Fail

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

Assessment Results

Score Results

Review	Score
Overall Score	42/100
Auditor Score	50/100
Review by Section	**Score**
Manual Scan Score	-12/33
SWC Scan Score	35 /37
Advance Check Score	19 /30

The Following Score System Has been Added to this page to help understand the value of the audit, the maximun score is 100, however to attain that value the project most pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Fail

Assessment Results

Important Notes:

- No issues or vulnerabilities were found.
- This is a Pinksale Generated BabyToken.
- Please DYOR on the project.
- The contract gives Ethereum https://bscscan.com/address/0x2170ed0880ac9a755fd29b2688956bd959f933f8
- this contract depends on volume and buy/sale then distribution of rewards may happen.
- This type of contract may fail if the fees are set to 0.

Auditor Score =50
Audit Fail

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that actagainst the nature of decentralization, such as explicit ownership or specialized access roles incombination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code,such as a constructor assignment imposing different require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.

Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocation for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.