CONTRACT WOLF

Blockchain Security - Smart Contract Audits

Security Assessment

April 10, 2022

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

Gongswap 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 **Gongswap.**

Network

Binance Smart Chain (BEP20)

Contract link

https://bscscan.com/address/0x9ff121A727F95E463370a75328dA2c0f705FF1b8

Website

https://gongswap.finance

Telegram

https://t.me/gongswap_chat

https://t.me/gongswap_official

Twitter

https://twitter.com/gongswap

YouTube

https://www.youtube.com/channel/UCmq7-zZOm0eDrdbwvTcaYMA

Facebook

https://www.facebook.com/GongSwap-109719595005903/

Medium

https://gongswap.medium.com/

Description

Gongswap is a decentralized cryptocurrency marketplace which is run on the Binance Smart Chain. It aims to be one of the most liquid markets when it comes to exchanging alt coins on a DEFI marketplace. This means that users will be able to swap almost any cryptocurrency immediately on the platform. GongSwap has a native token known as GONG.

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

- Context
- IERC20
- SafeMath
- Address
- Ownable
- IUniswapV2Factory
- IUniswapV2Pair
- IUniswapV2Router01
- IUniswapV2Router02
- GongSwap

Description

Optimization enabled: Yes

Decimal: 18

Symbol: GONG

Max / Total supply: 100,000,000,000

Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	2	2	5	1

Exposed Functions

Version	Public	Private	External	Internal
1.0	31	25	76	16

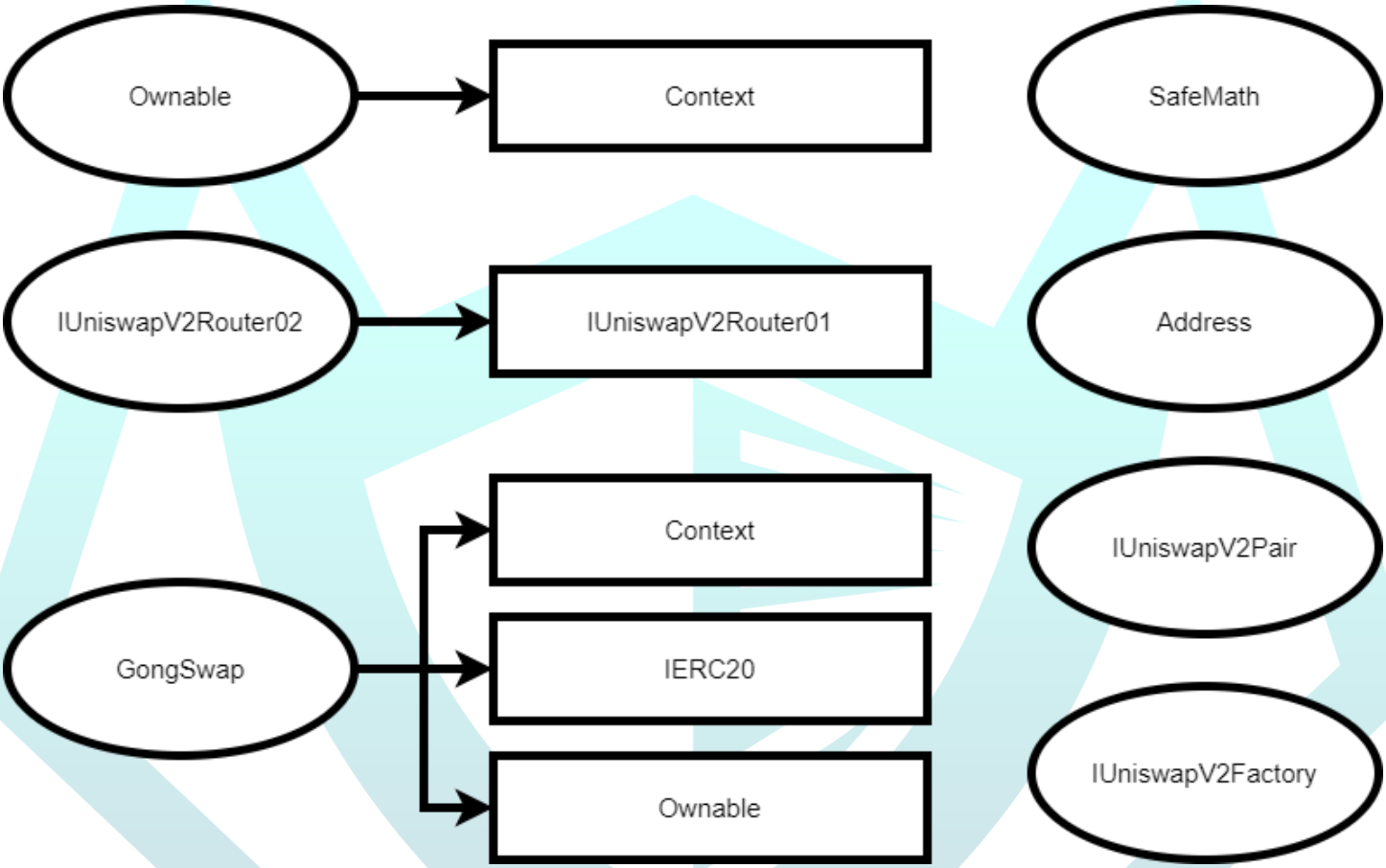
State Variables

Version	Total	Public
1.0	37	14

Capabilities

Version	Solidity Versions Observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	v0.8.5		Yes	Yes	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. decreaseAllowance
3. deliver
4. excludeFromFee
5. excludeFromReward
6. includeInFee
7. includeInReward
8. increaseAllowance
9. lock
10. presale
11. renounceOwnership
12. setBuyBackEnabled
13. setBuybackFee
14. setBuybackUpperLimit
15. setDevAddress
16. setMarketingAddress
17. setMarketingFee
18. setMaxTxAmount
19. setNumTokensSellToAddToLiquidity
20. setRouterAddress
21. setSwapAndLiquifyEnabled
22. setTaxFee
23. transfer
24. transferFrom
25. transferOwnership
26. unlock

AUDIT PASSED

Low Issues

A floating pragma is set (SWC- 103)	L: 20
State variable visibility is not set (SWC-108)	L: 479 C:9

Audit Comments

- Deployer can renounce ownership
- Deployer can transfer ownership
- Deployer can lock/pause contract
- Deployer can set fees with an indefinite amount
- Deployer can set max transaction amount
- Deployer can include/exclude addresses from rewards
- Deployer can include/exclude addresses from fees
- Deployer cannot burn
- Deployer cannot block users
- Deployer cannot mint after initial deployment

CONTRACTWOLF

Blockchain Security - Smart Contract Audits