KISHIELD

Security Audit

FGCA Token

May 23, 2022

Table of Contents

Audit Summary

This report has been prepared for FGCA Token on the Binance Chain network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Project Overview

Token Summary

Parameter	Result
Address	0x58ca2873c9091ad2eab4f00cc415b846a286c080
Name	FGCA
Token Tracker	FGCA (FGCA)
Decimals	18
Supply	10,000,000,000
Platform	Binance Chain
compiler	v0.8.12+commit.f00d7308
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x58ca2873c9091ad2eab4f00cc415b846a286c080#code
Url	https://www.fgd.ai

Main Contract Assessed

Name	Contract	Live
FGCA	0x58ca2873c9091ad2eab4f00cc415b846a286c080	Yes

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Griefing	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	Low / No Risk
Assert Violation	Complete	Complete	Low / No Risk
Reentrancy	Complete	Complete	Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	Low / No Risk
Unchecked Call Return Value	Complete	Complete	Low / No Risk
Outdated Compiler Version	Complete	Complete	Low / No Risk
Integer Overflow and Underflow	Complete	Complete	Low / No Risk
Function Default Visibility	Complete	Complete	Low / No Risk

Contract Ownership

The contract does not have an owner.

Having no owner means that all the ownable functions in the contract can not be called by anyone, this often leads to more trust on the project.

This contract has a PairManager that can call special functions:
0xe7b80ad1a73cec99eac142ccb4a6e6a913743cea

Important Notes To The Users:

- The owner cannot mint tokens after intial deployment.
- The owner cannot change the min tx amount.
- The owner cannot pause trading.
- There is no fee for transfer between wallets.
- Users than own LP tokens are added to the lpProviders group.
- If a user holds an NFT and are in the lpProviders group then they are rewarded with tokens proportional to the percentage of the LP supply they own.
- To be included in the lpProviders you need to have more than 0 LP tokens.
- If a user in the lpProviders sells or transfer all their LP tokens they are removed from the lpProviders group and will not receive rewards.
- Rewards tokens are distributed every day after the last distribution as long as the contract has at least 1000 tokens.
- Once the PairManager renounces ownership of the contract, none of the following are applicable.
- The PairManager can include/exclude addresses from fees.
- The PairManager can change the minPeriod for the rewards with no restrictions.
- No high-risk Exploits/Vulnerabilities Were Found in token Source Code.

Audit Passed

Technical Findings Summary

Classification of Issues

Severity	Description
High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency
Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited.Issues under this classification are recommended to be fixed as soon as possible.
Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Info	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

Findings

Severity	Found
High	0
Medium	0
Low	0
Info	4
Total	4

Findings

Contract locks BNB

ID	Severity	Contract	Function
01	Informational	FGCA	Function constructor()

Description

Contract with a payable function, but without a withdrawal capacity.

Recommendation

We recommend removing the payable attribute or add a withdraw function.

Variables could be declared as constant

ID	Severity	Contract	Function
02	Informational	FGCA	Variables burnFee, deadAddress, distributorGas, lpFee

Description

Gas Optimization. Variables that are never changed could be declared as constant.

Recommendation

We recommend declaring those variables as constant.

Public function that could be declared external

ID	Severity	Contract	Function
03	Informational	FGCA	Functions renounceOwnership, transferOwnership, renouncePairManager, transferPairManager, excludeMultipleAccountsFromFees.

Description

Gas Optimization. Public function that could be declared external

Recommendation

Public functions that are never called by the contract should be declared external to save gas.

Division before Multiplication

ID	Severity	Contract	Function
04	Informational	FGCA	function _transfer()

Description

Precision Loss. 'fees = amount * totalFee / 100 => burnAmount = fees * burnFee / totalFee'. Division before multiplication can result in truncation and less accurate results

Recommendation

Multiplication should be performed before division to not lose precision.

Priviliged Functions (onlyOwner & Others)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
renouncePairManager	none	public
transferPairManager	none	public
setMinPeriod	none	external
excludeFromFees	none	public
excludeMultipleAccountsFromFees	none	public
setAutomatedMarketMakerPair	none	public

Statistics

Liquidity Info

Parameter	Result
Pair Address	0x7a899F75Bdd868A12D2a94D30ecbCD4E39De7531
FGCA Reserves	522233112.78 FGCA
FGD Reserves	867226.82 FGD
Liquidity Value	$~ 4,791,870 USD

Token (FGCA) Holders Info

Parameter	Result
FGCA Percentage Burnt	0.00%
FGCA Amount Burnt	0 FGCA
Top 10 Percentage Own	96.37%
Top 10 Amount Owned	9,637,393,078.37 FGCA
Top 10 Aprox Value	$- USD

LP (FGCA/FGD) Holders Info

Parameter	Result
FGCA/FGD % Burnt	0.00%
FGCA/FGD Amount Burnt	0 FGCA/FGD
Top 10 Percentage Owned	83.44%
Top 10 Amount Owned	17,067,939.897 FGCA/FGD
Locked Tokens Percentage	72.37%
Locked Tokens Amount	14,803,643.455 FGCA/FGD

* All the data diplayed above was taken on-chain at block 18055810
* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 18055810

KISHIELD

Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit 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 may be pursued by the Project in question, and that 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 completely 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 in this report. Information is provided ‘as is’, and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD 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 and/or actions with regards to the information provided in this audit report.

The assessment services provided by KISHIELD is subject to dependencies and under continuing development. You agree that your access and/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 and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.