KISHIELD

Security Audit

FGD Airdrop

May 16, 2022

Table of Contents

Audit Summary

This report has been prepared for FGD Airdrop 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.

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	0x5E8922BE84b2fbA06B66E212D02ff1A35490475e
Name	FGD Airdrop
Platform	Binance Chain
compiler	v0.8.0+commit.c7dfd78e
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://testnet.bscscan.com/address/0x5E8922BE84b2fbA06B66E212D02ff1A35490475e#code
Url	https://www.fgd.ai

Main Contract Assessed

Name	Contract	Live
FGD Airdrop	0x5E8922BE84b2fbA06B66E212D02ff1A35490475e	No

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 ownership of FGD Airdrop is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x12380625f66f8775edad7bea937a30cf8f2d7fde which can be viewed from:
HERE

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

Important Notes To The Users:

- This airdrop contract rewards NFT holders with a token, the NFT has different tiers that give users different amount of tokens.
- The first time an user claims with their NFT they receive 40% of the allocated tokens for their NFT id.
- After that they can claim 10% of the allocated amount every month for 6 months.
- After the users claims all the tokens allocated for their NFT they cannot use the same NFT to claim again.
- Users can claim the airdrop for many NFTs ids at the same time.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- The owner can change the startTime without limitations.
- The owner can change the allocated tokens for each NFT tier without limitations.
- No High-risk Exploits/Vulnerabilities Were Found in token Source Code.

Audit Passed

Findings Summary

Classification of Issues

All Issues are of informational.

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

Check oneMonth Variable

ID	Severity	Contract	Function
01	Informational	FGD Airdrop	oneMonth = oneDay * 30;

Description

We conducted external testing using a python simulator for the claimId() and getAmount() functions. In our script using "oneMonth = oneDay * 30" results in a total amount claimed of 91.666 tokens based on the tokenAmount to be 100, also the Info.count variable moves from int to float.

Recommendation

We recommend double checking the distribution logic. In our research using 31 days for a month works out to 100 out of 100 tokens claimed and the count variable is always an int. The python script can be shared upon team request.

Division before Multiplication

ID	Severity	Contract	Function
02	Informational	FGD Airdrop	function getAmount()

Description

Precision Loss. 'day = (readTime - last) / oneMonth => amount = tokenAmount * day' Division before multiplication can result in truncation and less accurate results

Recommendation

Multiplication should be performed before division to not lose precision.

Uninitialized local variables

ID	Severity	Contract	Function
03	Informational	FGD Airdrop	Variable curAmount in _claimId(uint256)

Description

Variables 'curAmount' in _claimId function is uninitialized

Recommendation

Initialize all the variables. If a variable is meant to be initialized to zero, explicitly set it to zero to improve code readability.

Public function that could be declared external

ID	Severity	Contract	Function
04	Informational	FGD Airdrop	Functions renounceOwnership, transferOwnership

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.

Priviliged Functions (onlyMaster)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
setStartTime	uint256 _start	external
_setTokenAmount	none	internal
setTokenAmount	uint8 _type, uint256 _amount	external
setTokenAmountArr	calldata ts, calldata amounts	external

Only the contract owner has permission to use these functions.

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.