KISHIELD

Security Audit

FGD Staking

April 16, 2022

FGD

Table of Contents

Audit Summary

This report has been prepared for FGD Staking 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	0x8a8da57b532f567cfe2d2d7e411897a04875da18
Name	FGD Staking
Platform	Binance Chain
compiler	v0.8.10+commit.fc410830
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x8a8da57b532f567cfe2d2d7e411897a04875da18
Url	https://fgd.ai/

Main Contract Assessed

Name	Contract	Live
StakePool	0x8a8da57b532f567cfe2d2d7e411897a04875da18	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

FGD Staking has an admin and owner roles, all addresses set to either of these can trigger onlyMaster functions.

The current owner is the address 0x4394677869a6b3bcf943fc59cdc3f8e6d855f189
HERE

The current admin is the address
0x4394677869a6b3bcf943fc59cdc3f8e6d855f189
HERE

The wallets with roles have the power to call the function displayed on the priviliges function chart below. If the owner wallet is compromised this priviliges could be exploited.

Important Notes To The Users:

- The owner cannot stop users from withdraw.
- Users stake LP tokens for the pair FGD/WBNB.
- Users are rewarded with FGD tokens.
- Users need to wait 7 days to claim rewards and withdraw.
- Users can add up to one other address as their referral.
- Referred address "team" gains a teammate for every user that uses their address.
- Users cannot add themselves as their own referral.
- When a user claims their rewards they get 100% and the referral gains 20% of the amount.
- Rewards rates are calculated on base of periods.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- Owners can update the minLP, and minUsdt required to stake LP tokens.
- 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	2
Total	2

Findings

Public function that could be declared external

ID	Severity	Contract	Function
01	● Informational	FGD Staking	Functions renounceOwnership, transferOwnership, transferAdmin, validCount, userValid, getUserTime, getRewardInfo, getReferrer, getTeamLength, getTeam

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.

Assigment with no effects

ID	Severity	Contract	Function
02	● Informational	FGD Staking	periodFinish variable

Description

Uint variables in solidity are set to 0 by default.

Recommendation

We recommend deleting the initilization of the uint256 variable to 0

Priviliged Functions (onlyMaster)

Function Name	Parameters	Visibility
updateMinLp	uint256 _lp	public
updateMinUsdt	uint256 _usdt	public

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.