KISHIELD

Security Audit

GrilledFist Game

April 25, 2022

Table of Contents

1 Audit Summary

2 Project Overview

2.1 Token Summary

2.2 Main Contract Assessed

3 Smart Contract Vulnerability Checks

4 Contract Ownership

4.1 Priviliged Functions

5 Important Notes To The Users

6 Findings Summary

6.1 Classification of Issues

6.1 Findings Table

01 Public function that could be declared external

02 Variables could be declared as constant

03 Access Control

04 Assigment with no effects

05 Too many digits

7 Statistics

7.1 Liquidity

7.2 Token Holders

7.3 Liquidity Holders

8 Liquidity Ownership

9 Disclaimer

Audit Summary

This report has been prepared for GrilledFist Game 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	0x1528bE1b680610Bd13CDe93542163D7B4f09e3Ef
Name	GrilledFist
Platform	Binance Chain
compiler	v0.8.6+commit.11564f7e
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x1528bE1b680610Bd13CDe93542163D7B4f09e3Ef
Url	https://www.grilledfist.top/

Main Contract Assessed

Name	Contract	Live
GrilledFist	0x1528bE1b680610Bd13CDe93542163D7B4f09e3Ef	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 GrilledFist has no 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.

Important Notes To The Users:

- The contract is different from other mining/hatching games because it uses the FIST tokens instead of BNB.
- There is NO mechanism to withdraw your entire investment, users can only withdraw the daily return out.
- When an user buys eggs there is a 3% fee sent to the ceoAddress.
- Users do not have the ability to decide how many eggs they can hatch, by default is the amount they buy.
- When eggs are hatched if an user enters their own address, the 0 address or the address have no miners, the referral address is set to the ceoAddress as long as they do not have a referral address already.
- When eggs are hatched the user referral address gets a bonus of 13% of the eggsUsed, and the ceoAddress gets a bonus of 2%.
- Upon hatching the amount of marketEggs increases with the goal of boosting the market to nerf miners hoarding.
- When eggs are sold there is a 3% fee sent to the ceoAddress.
- hatcheryMiners produce eggs based on the amount of seconds passed from the last hatch.
- There is not an ownable mechanism so the developers have no power to change any value or take out funds from the contract.
- The magic trade balancing algorithm allows users that buy normal amounts to get fair prices while users that buy huge values get a less favourable pricing.

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	1
Info	4
Total	5

Findings

Public function that could be declared external

ID	Severity	Contract	Function
01	Informational	GrilledFist	Functions sellEggs, buyEggs, calculateEggBuySimple, seedMarket, getBalance, getMyMiners

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.

Variables could be declared as constant

ID	Severity	Contract	Function
02	Informational	GrilledFist	Variables EGGS_TO_HATCH_1MINERS, PSN, PSNH

Description

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

Recommendation

We recommend declaring those variables as constant.

Access Control

ID	Severity	Contract	Function
03	Low	GrilledFist	Funcion seedMarket()

Description

Function visibility is set to public and there is no Ownable nor AccessControl contracts modifiers in place.

Recommendation

We recommend making use of Ownable contracts, otherwise do not do anything if this is by design.

Assigment with no effects

ID	Severity	Contract	Function
04	Informational	GrilledFist	bool public initialized=false

Description

bool variables in solidity are set to 0 by default.

Recommendation

We recommend deleting the initilization of the uint256 variable to 0

Too many digits

ID	Severity	Contract	Function
05	Informational	GrilledFist	Variables marketEggs

Description

Literals with many digits are difficult to read and review.

Recommendation

Make use of scientific notation, use underscores, and/or use ether suffix.

Priviliged Functions (onlyMaster)

Function Name	Parameters	Visibility

There are no functions that can be called by the owner of the contract because the contract has no ownership mechanism.

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.