

0x00NINJA AUDITS



Security Assessment

TegridyFarms miner

April 30, 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**
- 6 Important Notes To The Users**
- 7 Social Media Check(Informational)**
- 8 Disclaimer**



Audit Summary

This report has been prepared for TegrityFarms miner on the Binance Smart Chain network. CFGNINJA 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:

- 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.



Project Overview

Token Summary

Parameter	Result
Address	0x066c3c870f30e7B2de58Ad0854bAE87a3c5C07bE
Name	TegridyFarms
Token Tracker	TegridyFarms (TegridyFarms)
Decimals	0
Supply	0
Platform	Binance Smart Chain
compiler	v0.8.11+commit.d7f03943
Contract Name	TegridyFarms
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x066c3c870f30e7b2de58ad0854bae87a3c5c07be#code
Payment Tx	0xd9634997111fcc6818b53042cc7793da8c5a77a7e773b72646ffa08ec64bf8fc



Main Contract Assessed Contract Name

Name	Contract	Live
TegridyFarms	0x066c3c870f30e7B2de58Ad0854bAE87a3c5C07bE	Yes

TestNet Contract Assessed Contract Name

Name	Contract	Live
TegridyFarms	0x07d846d037f9e22a532b2b56a2ce9863b5e07956	Yes

Solidity Code Provided

SolID	FileNameMD5	FileName
TegridyFarms	a0c90bc601ef74fb4ee26307be4d93f86fef9749	TegridyFarms.sol



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



Contract Ownership

The contract ownership of TegrifyFarms has been renounced.

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.



KYC Information

The Project Owners of TegrityFarms is not KYC. .

The owner wallet has the power to call the functions displayed on the privileged 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.

KYC Information Notes:

Auditor Notes: Asked project owner about KYC.

Project Owner Notes: Costumer have plans to do KYC at a Later time.



Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-100	Pass	Function .	TegridyFarms.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	TegridyFarms.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	TegridyFarms.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	TegridyFarms.sol	L: 1 C: 1
SWC-104	Pass	Unchecked Call Return Value.	TegridyFarms.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	TegridyFarms.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	TegridyFarms.sol	L: 0 C: 0
SWC-107	PASS	Read of persistent state following external call.	TegridyFarms.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	TegridyFarms.sol	L: 114 C: 30
SWC-108	Pass	State variable visibility is not set.	TegridyFarms.sol	L: 185 C: 9
SWC-108	Pass	State variable visibility is not set.	TegridyFarms.sol	L: 195 C: 14
SWC-109	Pass	Uninitialized Storage Pointer.	TegridyFarms.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	TegridyFarms.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	TegridyFarms.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	TegridyFarms.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	TegridyFarms.sol	L: 1180 C: 8
SWC-114	Pass	Transaction Order Dependence.	TegridyFarms.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	TegridyFarms.sol	L: 25 C: 4127
SWC-116	Low	A control flow decision is made based on The block.timestamp environment variable.	TegridyFarms.sol	L: 1205 C: 8
SWC-117	Pass	Signature Malleability.	TegridyFarms.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	TegridyFarms.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	TegridyFarms.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randomness.	TegridyFarms.sol	L: 608 C: 47
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	TegridyFarms.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	TegridyFarms.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	TegridyFarms.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	TegridyFarms.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-125	Pass	Incorrect Inheritance Order.	TegridyFarms.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	TegridyFarms.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	TegridyFarms.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	TegridyFarms.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	TegridyFarms.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	TegridyFarms.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	TegridyFarms.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	TegridyFarms.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	TegridyFarms.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	TegridyFarms.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	TegridyFarms.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	TegridyFarms.sol	L: 0 C: 0

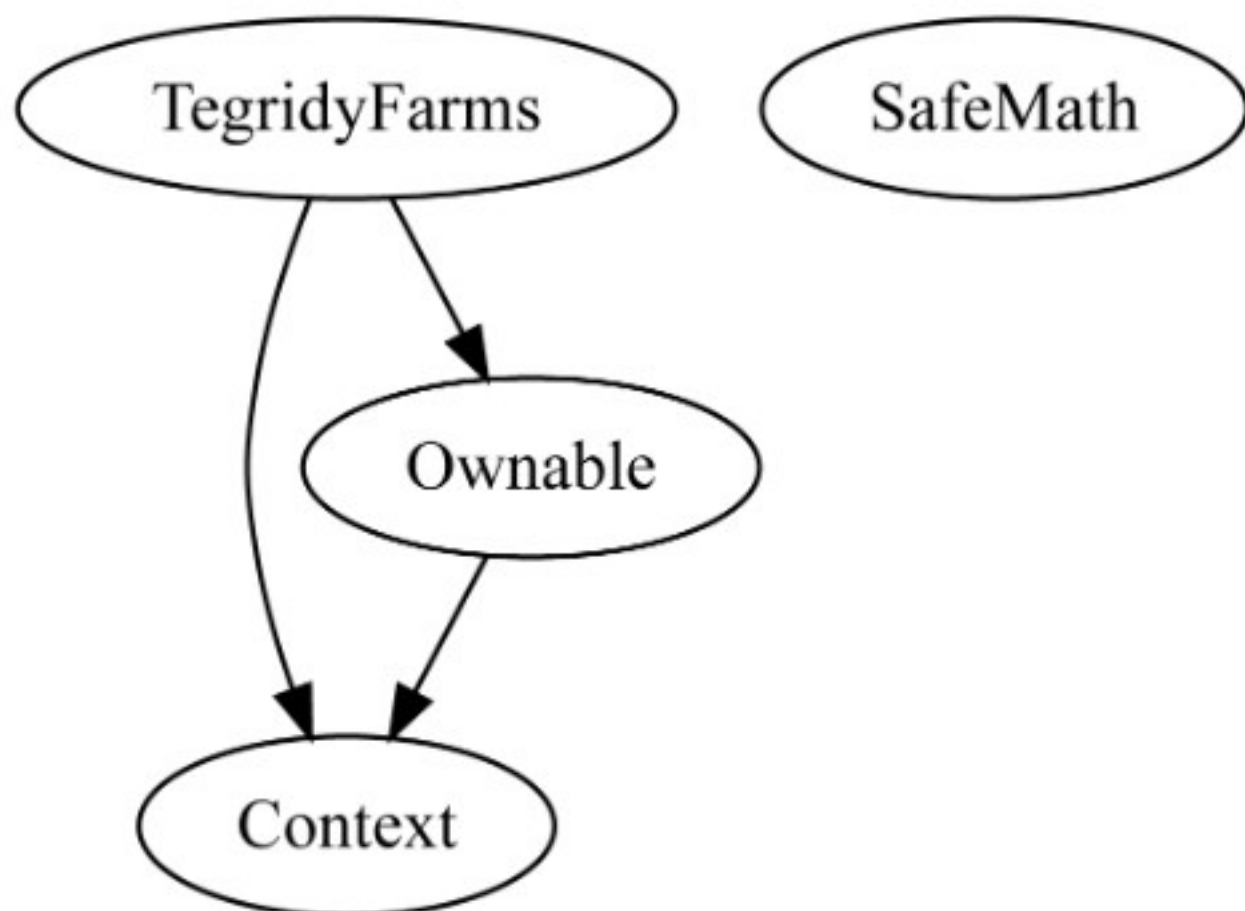
We scan the contract for additional security issues using MYTHX and industry standard security scanning tool



Call Graph and Inheritance

The contract for TegriddyFarms has the following call graph structure

The Project has a Total Supply of 0 and has the following inheritance



Privileged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
seedMarket		public
setFee	_fee (uint256)	public



Important Notes To The Users:

- The Farming Collective team is currently not KYC with Pinksale or with CFG NINJA.
- Contract is currently renounced:
- <https://bscscan.com/tx/0x19a8e4163ff9e02a6fdb988ffebf56123fd57d024597414905699de1ae4c19ec>
- We gave feedback to the Farming Collective team around the miners contract and how to potentially improve it in the future.
- Contract did not show any issues on their code, or any concerns of hidden information or functions.
- We tested the dapp on a limited basis and did not encounter any issues.
- During the test of the dapp, we water plants and grow 16 plants.
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.

Audit Passed



Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/TheFarmingCo	Pass
Medium	https://medium.com/@TheFarmingCollective	Pass
Website	https://bsc.tegridy.app	Pass
Telegram	https://t.me/TheFarmingCollective	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: The Farming Collective has an outstanding social media reach

Project Owner Notes: Gitbook: <https://docs.thefarmingcollective.io/> YouTube: <https://www.youtube.com/channel/UC-BOW44odbgKKhAm6clZOSQ>



Disclaimer

CFGNINJA 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 advocacy 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 CFGNINJA is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will CFGNINJA 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 CFGNINJA 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.

