CFG NINJA
AUDITS

Security Assessment

Stake Token Token

May 9, 2022

Table of Contents

Audit Summary

This report has been prepared for Stake Token Token on the Ethereum 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	0xe55bd75d7cE7bfDe26A347A748d080D3ACdA7FFE
Name	Stake Token
Token Tracker	Stake Token (STAKE)
Decimals	18
Supply	750,000
Platform	Ethereum
compiler	v0.8.12+commit.f00d7308
Contract Name	StakeToken
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/token/0xe55bd75d7ce7bfde26a347a748d080d3acda7ffe
Payment Tx	0xd9b4ae240866d84b664bc5786bb0708e45fd41e08f164be58787f954bcf11f36

Main Contract Assessed
Contract Name

Name	Contract	Live
Stake Token	0xe55bd75d7cE7bfDe26A347A748d080D3ACdA7FFE	Yes

TestNet Contract Assessed
Contract Name

Name	Contract	Live
Stake Token	0x6ac54FbA9C1aeF23714c67f2cE44f87B0929405D	Yes

Solidity Code Provided

SolID	FileNameMD5	FileName
StakeToken	9a5e218aec98b02dfb91bd4b98904222ade1f66b	StakeToken.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

Mint Check

The Project Onwers of Stake Token has the ability to Mint New Tokens.

We Recommend the team to create a new contract without a Mint Function.

Mint Notes:

Auditor Notes: Customer added mint limit and only allow to pool to mint 5%, the max supply is 5,000,000.

Project Owner Notes: only minter is the faucet/pool and the maximum it could mint is of 5% total supply every day.

Fees Check

The Project Owners of Stake Token does not have the ability to set fees higher than 25% .

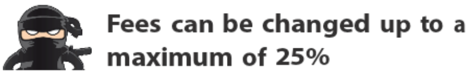
Team May have fees defined, however they dont have the ability to set those fees higher than 25%.

.

Tax Fee Notes:

Auditor Notes: We informed the customer of the fees configuration, they hVe a 11% buy and 18% Sale. We recommended not only increase it higher than 25

Project Owner Notes: Customer implemented requires changes to all fees including external al contracts.



Fees can be changed up to a maximum of 25%

MaxTx Check

The Project Onwers of Stake Token does not has the ability to set max tx amount

The Team allow any investors to swap, transfer or sale their total amount if needed.

Pause Trade Check

The Project Onwers of Stake Token Owner can pause trading but he can't move tokens (Owner can't pause trading)

The Team has done a great job to avoid stop trading, and investors has the ability to trade at any given time without any problems

Pause Trade Notes:

Auditor Notes:

Project Owner Notes:

Contract Ownership

The contract ownership of Stake Token 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 0x3cc6a3fa5bECF00B585E4575537F03d24891bD70 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.

We recommend the team to use a Multisignature Wallet if contract is not going to be renounced, this will give the ability to the team to have more control over the contract.

Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 17670820

KYC Information

The Project Onwers of Stake Token has provided KYC Documentation.

KYC Certificated can be found on the Following:
KYC Data

KYC Information Notes:

Auditor Notes: Asked project owner about KYC.

Project Owner Notes: Project owner is in the process of getting PinkSale KYC Approved

Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-100	Pass	Function .	StakeToken.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	StakeToken.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	StakeToken.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	StakeToken.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	StakeToken.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	StakeToken.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	StakeToken.sol	L: 0 C: 0
SWC-107	PASS	Read of persistent state following external call.	StakeToken.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	StakeToken.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	StakeToken.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	StakeToken.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	StakeToken.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	StakeToken.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-113	Pass	Multiple calls are executed in the same transaction.	StakeToken.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	StakeToken.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	StakeToken.sol	L: 474 C: 15
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	StakeToken.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	StakeToken.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	StakeToken.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	StakeToken.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	StakeToken.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	StakeToken.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	StakeToken.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	StakeToken.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	StakeToken.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	StakeToken.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	StakeToken.sol	L: 0 C: 0

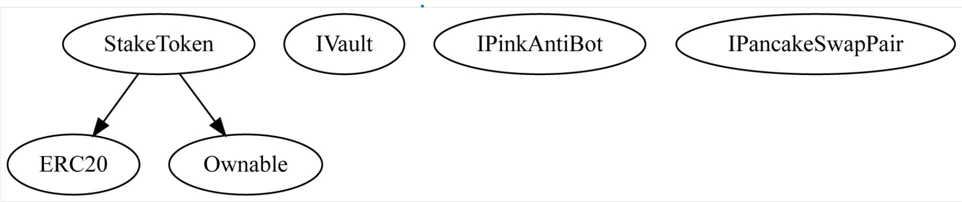
ID	Severity	Name	File	location
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	StakeToken.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	StakeToken.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	StakeToken.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	StakeToken.sol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

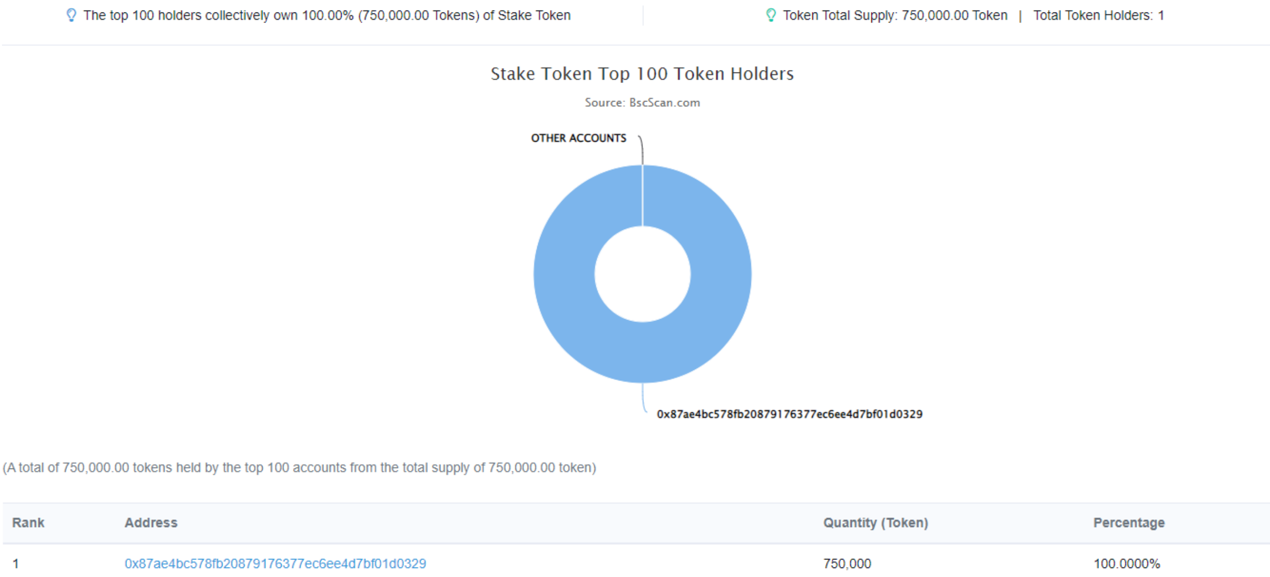
The contract for Stake Token has the following call graph structure

The Project has a Total Supply of 750,000 and has the following inheritance



Top Token Holders

The contract for Stake Token has the following top token holders



The top 100 holders collectively own 100.00% (750,000.00 Tokens) of Stake Token

Token Total Supply: 750,000.00 Token | Total Token Holders: 1

Stake Token Top 100 Token Holders

Source: BscScan.com

(A total of 750,000.00 tokens held by the top 100 accounts from the total supply of 750,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x87ae4bc578fb20879176377ec6ee4d7bf01d0329	750,000	100.0000%

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
setEnableAntiBot	_enable bool	external
setPool	_pool(address)	external
setAllTaxes	_transferTax uint256, _sell uint256, _buy uint256	external
setCustomTax	_contract address, _tax uint256	external
setCustomTaxStatus	_contract address, _status bool	external
excludeAddress	_address (address), _all (bool), _isReceive (bool)	public
excludeMultiple	_addresses (address), _all (bool), _isReceive _all (bool)	external
removeExclusions	_addresses (address), _all (bool), _isReceive _all (bool)	public
removeMultiple	_addresses (address), _all (bool), _isReceive _all (bool)	public
updateVault	_vault (address), _isContract (bool)	external
mint	amount (uint256), onlyPool	public
addLiquidityPair	_pair (address)	external

Important Notes To The Users:

- Stake Protocol team is very responsive, we have asked the team to do several revisions of their contract and they have made those improvements.
- The team will complete the KYC Process with PinkSale.
- A Mint function was found, the customer has updated the requirements around the mint and has limited the mint to 5% of the total supply every 30 minutes by the pool.
- The Project owner states since this is a rebase protocol they will have a mint function to generate new tokens and a burn function to burn functions.
- Initial Supply is 750,000 and the Max Supply is 5,000,000. There are limits to avoid the token from going beyond this rate.
- Owner can charge fees up to 25%, they also can set different fees for specific addresses.
- Owner can't set max tx amount.
- Owner can't pause trading.
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.

Audit Passed

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/Stake_Protocol	Pass
Reddit	https://www.reddit.com/u/StakeProtocol	Pass
Website	https://stakeprotocol.app/	Pass
Telegram	http://T.me/stakeprotocolportal	Pass

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

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

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 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 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.

CFG NINJA AUDITS