KISHIELD

Security Audit

StrikeCrypto Token

May 4, 2022

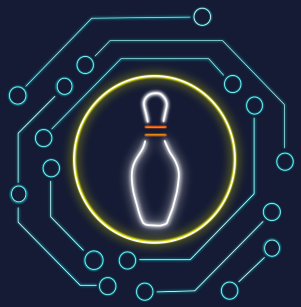

Table of Contents

Audit Summary

This report has been prepared for StrikeCrypto Token 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 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:

- 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	0x5A6AE66e9AE7c70540B9DAe6d69B338bB06b6d89
Name	StrikeCrypto
Token Tracker	StrikeCrypto (STR)
Decimals	18
Supply	100,000,000
Platform	Binance Chain
compiler	v0.8.7+commit.e28d00a7
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x5A6AE66e9AE7c70540B9DAe6d69B338bB06b6d89
Url	strikecryptobsc.com

Main Contract Assessed

Name	Contract	Live
StrikeCrypto	0x5A6AE66e9AE7c70540B9DAe6d69B338bB06b6d89	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 ownership of StrikeCrypto 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 0x03ee7D17a358c39618cdEAFb719Ef94D512E6a8F 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:

- The owner cannot mint tokens after intial deployment.
- Users added to exemptOperatePausedToken mapping can trade even when the transfer are paused.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- The owner can change the feePool tax to 100%
- The owner can pause/unpause transfer.
- The owner can change the max tx amount without restrictions.
- The owner can change the max account amount without restrictions.
- The owner of the contract can withdraw all the BNB from the contract.
- The owner can add/remove addresses from fees and tx limits.
- No high-risk Exploits/Vulnerabilities Were Found in token Source Code Other than owner priviliges.
- The contract makes heavy use of optimizations techniques with Yul, these fall outside the scope of the audit.

Technical Findings Summary

Classification of Issues

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

Public function that could be declared external

ID	Severity	Contract	Function
01	Informational	StrikeCrypto	Functions setExemptFee, setExemptFeeReceiver, setExemptTxLimit, setExemptAmountLimit, setExemptStaker, setAdministrationWallet, setDevelopingWallet

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.

Missing events arithmetic

ID	Severity	Contract	Function
02	Informational	StrikeCrypto	Missing events for setWBNB_TOKEN_PAIR, setMaxAccountAmountWithDecimals, setMaxTxAmountWithDecimals, setFeePool, setFeeDevelopmentWallet, setFeeAdministrationWallet

Description

Functions that change critical arithmetic parameters should emit an event.

Recommendation

Emit corresponding events for critical parameter changes.

Assigment with no effects

ID	Severity	Contract	Function
03	Informational	StrikeCrypto	Variables pausedToken, pausedStake

Description

Bools variables in solidity are set to false by default.

Recommendation

We recommend deleting the initilization of the boolean variable to false

Code with no effects

ID	Severity	Contract	Function
04	Informational	StrikeCrypto	exemptStaker mapping

Description

exemptStaker mapping has information but is never used in contract logic outside of set/remove

Recommendation

We recommend deleting the statement

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
enableToken	none	external
togglePauseStake	none	external
setFeeAdministrationWallet	none	external
setFeeDevelopmentWallet	none	external
setFeePool	none	external
setMaxTxAmountWithDecimals	none	public
setMaxTxAmount	none	external
setMaxAccountAmountWithDecimals	none	public
setMaxAccountAmount	none	external
setExemptOperatePausedToken	none	public
setExemptFee	none	public
setExemptFeeReceiver	none	public
setExemptTxLimit	none	public
setExemptAmountLimit	none	public
setExemptStaker	none	public
setAdministrationWallet	none	public

Function Name	Parameters	Visibility
setDevelopingWallet	none	public
buyBackAndHold	none	external
buyBackAndHoldWithDecimals	none	public
buyBackAndBurn	none	external
buyBackAndBurnWithDecimals	none	public
setWBNB_TOKEN_PAIR	none	external
setWBNB_BUSD_Pair	none	external

Statistics

Liquidity Info

Parameter	Result
Pair Address	0xcb0DBe1e27277b14C95D46050E2dDadF74AFf600
STR Reserves	0.00 STR
BNB Reserves	0.00 BNB
Liquidity Value	$0 USD

Token (STR) Holders Info

Parameter	Result
STR Percentage Burnt	0.00%
STR Amount Burnt	0 STR
Top 10 Percentage Own	100.00%
Top 10 Amount Owned	100,000,000 STR
Top 10 Aprox Value	$NaN USD

LP (STR/BNB) Holders Info

Parameter	Result
STR/BNB % Burnt	0.00%
STR/BNB Amount Burnt	0 STR
Top 10 Percentage Owned	0.00%
Top 10 Amount Owned	0 STR
Locked Tokens Percentage	0.00%
Locked Tokens Amount	0 STR

* All the data diplayed above was taken on-chain at block 17518826
* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 17518826

KISHIELD

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.