STAYSAFU AUDIT

SECURITY ASSESSMENT: DECEMBER 5TH, 2021

KRINGLZ

TABLE OF CONTENTS

I) SUMMARY

II) OVERVIEW

III) FINDINGS

IV) DISCLAIMER

SUMMARY

*This report has been prepared for **Kringlz** to discover issues and vulnerabilities in the source code of the **Kringlz** project as well as any contract dependencies that were not part of an officially recognized library.*

The audit is based on the code of the following BSC smart-contract :

0x386BA29489Bf25b9d1d5862662E4b014A9e8959C

*A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and **Kringlz** Deployment techniques. The auditing process pays special attention to the following considerations:*

- Testing the smart contracts against both common and uncommon attack vectors
- Assessing the codebase to ensure compliance with current best practices and industry standards

- Ensuring contract logic meets the specifications and intentions of the client
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Thorough line-by-line manual review of the entire codebase by industry experts

OVERVIEW

VULNERABILITY SUMMARY

UNDERSTANDING

The **Kringlz** Protocol is a decentralized finance (**DeFi**) token deployed on the Binance smart chain (**BSC**)

Kringlz mainly employs four features in its protocol : reward for holders in **BNB**, LP acquisition mechanism, a buy-back fee and marketing-team fee :

Each **Kringlz** transaction is taxed by a **14%** fees. **8%** is sold to be redistributed as a reward to the holders in BUSD. **2%** is accumulated internally until a sufficient amount of capital has been amassed to perform an LP acquisition. When this number is reached, the total tokens accumulated are split with half being converted to BNB and the total being supplied to the **PancakeSwap** contract as liquidity. Finally, **2%** is sold and used for marketing and **2%** is sold and is used to buy-back **KRNGL**.

PRIVILEGED FUNCTIONS

The contract contains the following privileged functions that are restricted by **authorized** or **onlyOwner** modifiers. They are used to modify the contract configurations and address attributes. We grouped these functions below :

OWNERSHIP MANAGEMENT

- transferOwnership
- authorize
- unauthorize

ACCOUNTS MANAGEMENT

- setIsDividendExempt
- setIsFeeExempt
- setIsTxLimitExempt
- setFeeReceivers
- setIsBlacklisted

TAXES MANAGEMENT

- setFees
- setSwapBackSettings
- setDistributionCriteria
- setDistributorSettings

BUYBACK MANAGEMENT

- clearBuybackMultiplier
- triggerZeusBuyback
- setAutoBuybackSettings
- setBuybackMultiplierSettings
- setTargetLiquidity

TRADING MANAGEMENT

- launch
- setTxLimit

OWNERSHIP

Here is a non-exhaustive list of what the smart-contract owner can and cannot do.

Feature	Able to modify	Details
Transaction fees	**Yes**	100 %
Max transaction	**Partially**	0.1%
Blacklist	**Yes**	
Whitelist	**Yes**	
Mint	**No**	
Renounce	**Yes**	
Ownership	**Yes**	Can add auth

FINDINGS

Third-party dependencies

The contract is serving as the underlying entity to interact with third party **PancakeSwap** protocols. The scope of the audit would treat those third party entities as black boxes and assume it's functional correctness. However in the real world, third parties may be compromised that led to assets lost or stolen.

We understand that the business logic of the **Kringlz Protocol** requires the interaction PancakeSwap protocol for adding liquidity to **KRNGL/BNB** pool and swap tokens. We encourage the team to constantly monitor the statuses of those third parties to mitigate the side effects when unexpected activities are observed.

Centralization of major privileges

The owner of the smart-contract has major privileges over it (he can change fees, change the maximum transaction amount, blacklist addresses and modify only the sell fees to turn the token into honeypot). This can be a problem, and we recommend at least to use a multi-sig wallet as owner address, and at best to establish a community governance protocol to avoid such centralization.

Conclusion

No major issue has been found in the **Kringlz** smart-contract. The findings we reported are low severity issues, and are common to the majority of rewards smart-contracts. The overall security of the smart-contract is very good, the only point that should be improved is the centralization of the privileges.

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement.

This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement.

This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without **StaySAFU'**s prior written consent.This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts **StaySAFU** to perform a security assessment.

This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.This report should not be used in any way to make decisions around investment or involvement with any particular project.

This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk.

StaySAFU's position is that each company and individual are responsible for their own due diligence and continuous security. **StaySAFU**'s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.