STAYSAFU AUDIT

September 2nd, 2022

Readify Chain

TABLE OF CONTENTS

I. SUMMARY

II. OVERVIEW

III. FINDINGS

A. CENT-3 | Centralization of initial token distribution

B. FUNC-1 | Unused functions

C. GAS-3 | Unoptimized function type

VI. DISCLAIMER

AUDIT SUMMARY

This report was written for Readify Chain ($RDC) in order to find flaws and vulnerabilities in the Readify Chain project's source code, as well as any contract dependencies that weren't part of an officially recognized library.

A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Readify Chain 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
- Through line-by-line manual review of the entire codebase by industry expert

AUDIT OVERVIEW

PROJECT SUMMARY

Project name	Readify Chain
Description	READIFY CHAIN is a blockchain read to earn revolutionary project. Readify intends to bring passion and purpose to readers, where you can read and earn while doing it. Nft marketplace, Readland verse and a unique blockchain ecosystem
Platform	BNB Chain
Language	Solidity
Codebase	https://bscscan.com/address/0x00967254d6B6DB3d10DA7dE99095cA71aBBB38c5

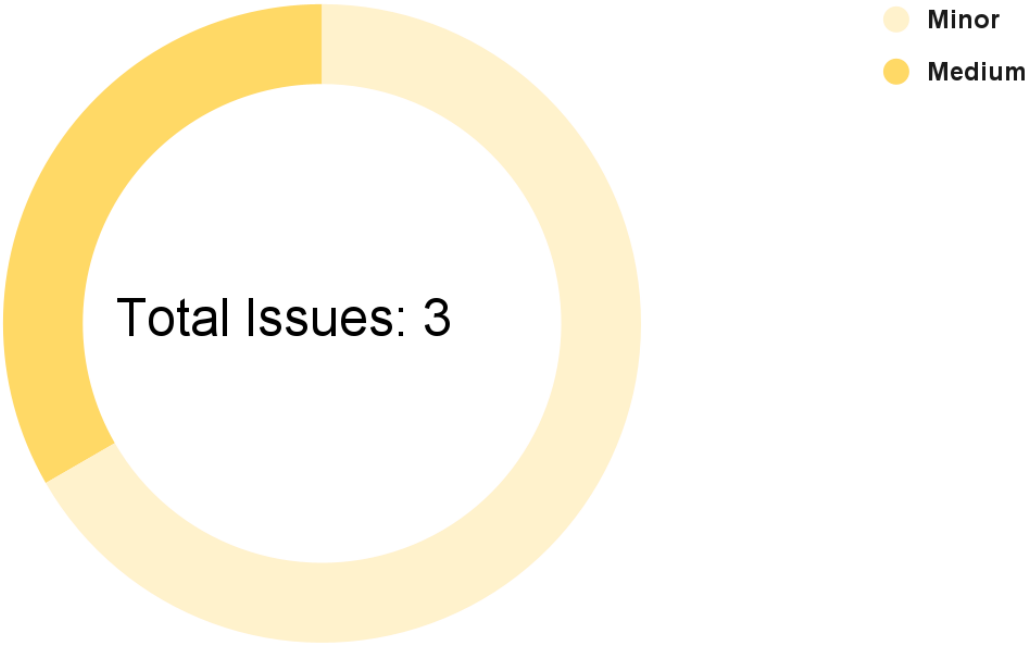
FINDINGS SUMMARY

Vulnerability	Total
Critical	0
Major	0
Medium	1
Minor	2
Informational	0

EXECUTIVE SUMMARY

There have been no major or critical issues related to the codebase and all findings listed here range from informational to medium. The medium security issues are the: centralisation of initial token supply.

AUDIT FINDINGS



Code	Title	Severity
CENT-3	Centralization of initial token distribution	Medium
FUNC-1	Unused functions	Minor
GAS-3	Unoptimized function type	Minor

CENT-3 | Centralization of initial token distribution

Description

A constructor within the contract mints the initial token supply to the deployer address (msg.sender). This initially centralizes token supply to the deployer address.

Recommendation

We recommend decentralizing tokens as soon as possible, matching the project's intentions. Examples of this are burning tokens or adding tokens to a liquidity pool (locked). We also recommend being fully transparent with the community about token distribution.

FUNC-1 | Unused functions

Description

Multiple functions within Readify Chain's contract are defined as private or internal but are never called within the contract. This wastes contract space as there is a maximum size a contract can have. Functions found with this issue have been listed below:

- _setupDecimals -> Line 776
- _burn -> Line 731
- trySub -> Line 224
- tryMul -> Line 236
- tryMod -> Line 265
- tryDiv -> Line 253
- tryAdd -> Line 211
- sub -> Line 296
- mul -> Line 310
- mod -> Line 406
- mod -> Line 340
- div -> Line 380
- div -> Line 324
- _msgData -> Line 110

Recommendation

We recommend safely removing these functions from the contract.

GAS-3 | Unoptimized function type

Description

Throughout Readify Chain's contracts some functions are of type public although they are never called within the contract. External functions require significantly less gas to call. Such found functions are listed below:

- decreaseAllowance -> Line 653
- increaseAllowance -> Line 626
- transferFrom -> Line 597
- approve -> Line 574
- allowance -> Line 557
- transfer -> Line 544
- balanceOf -> Line 526
- totalSupply -> Line 519
- decimals -> Line 512
- symbol -> Line 495
- name -> Line 487
- transferOwnership -> Line 177
- renounceOwnership -> Line 169

Recommendation

We recommend reviewing each of the functions listed above and where possible switch their type from public to external.

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 fun.