STAYSAFU
AUDIT

June 11TH, 2022

Luna Inu

TABLE OF CONTENTS

AUDIT SUMMARY

This report was written for Luna Inu ($LINU) in order to find flaws and vulnerabilities in the Luna Inu 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 Luna Inu 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	Luna Inu
Description	The Luna Inu project, originally created to address the failures of LUNA by creating a token the community could rally around, a rebellion against the financial irresponsibility of Do Kwon and his whale cronies.
Platform	Binance Smart Chain
Language	Solidity
Codebase	https://etherscan.io/token/0x78132543d8e20d2417d8a07d9ae199d458a0d581

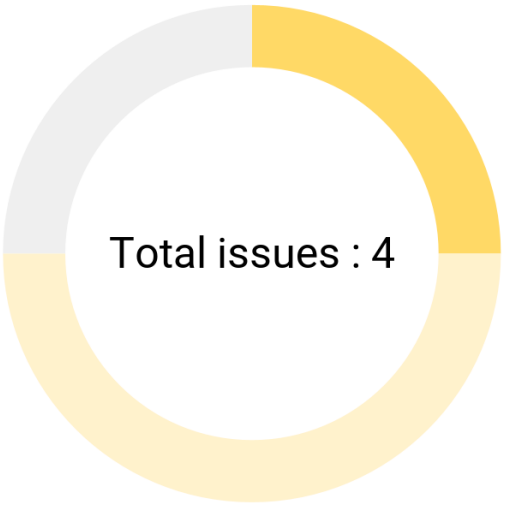
FINDINGS SUMMARY

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

EXECUTIVE SUMMARY

Luna Inu is an ERC20 that was originally created to compensate for the loss of the Terra Luna. It aims to be a fully community-driven token and project developed by an anonymous person. The liquidity is locked in for 100 years, and everything is being done to avoid a collapse like Terra Luna. No taxes are applied, and to finance itself the Luna Inu works on the basis of donations

There have been no major or critical issues related to the codebase and all findings listed here are minor or informational. The major security problem is the dependence on a decentralized exchange platform.



AUDIT FINDINGS

Code	Title	Severity
EXT-1	External protocol dependencies	Medium
COMP-2	Too old version of compiler	Minor
COMP-1	Unfixed version of compiler	Minor
MSG-3	Too long error message	Informational

MSG-3 | Too long error messages

Description

The smart contract has some error messages that are too long. The industry standards specify error messages must have a maximal length of 32 bytes. We recommend having the shortest possible error messages to optimize gas costs (see github.com/ethereum/solidity/issues/4588) and improve error handling. 6 issues of this type have been found in the smart contract.

Recommendation

We recommend shortening these error messages :

```
//Edited code with shortened error messages
//l 154
require(c / a == b, "Multiplication overflow");
//l 349
require(sender != address(0), "Transfer from the 0
address");
//350
require(recipient != address(0), "Transfer to the 0
address");
//l 386
require(account != address(0), "ERC20: burn from the 0
address");
//l 407
require(owner != address(0), "Approve from the 0
address");
```

```
//l 408
require(spender != address(0), "ERC20: approve to the 0
address");
```

COMP-1 | Unfixed version of compiler

Description

Luna Inu token's contract does not have locked compiler versions, meaning a range of compiler versions can be used. This can lead to differing bytecodes being produced depending on the compiler version, which can create confusion when debugging as bugs may be specific to a specific compiler version(s).

To rectify this, we recommend setting the compiler to a single version, the lowest version tested to be compatible with the code, an example of this change can be seen below.

Recommendation

We recommend fixing the compiler version to the most recent one :

```
//Edited code with fixed compiler version
//l 9
pragma solidity 0.5.0;
```

COMP-2 | Too old version of compiler

Description

The compiler version you used is quite old. It does not have any critical vulnerabilities but its use can cause problems (see https://solidity-fr.readthedocs.io/fr/v0.5.0/bugs.html).

Recommendation

We recommend you fix the compiler version to 0.8.0 or higher, since the project is fully compatible with newest versions.

EXT-1 | Dependence to an external protocol

Description

The contract serves as an underlying entity to interact with third party Uniswap protocols. The scope of the audit would treat this third party entity as black box and assume it is fully functional. However in the real world, third parties may be compromised and may have led to assets lost or stolen.

Recommendation

We encourage the team to constantly monitor the security level of the entire Uniswap project, as the security of the token is highly dependent on the security of the decentralized exchange platform.

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.