STAYSAFU
AUDIT

NOVEMBER 23RD, 2022

TEGRO

TABLE OF CONTENTS

AUDIT SUMMARY

This report was written for Tegro(TGR) in order to find flaws and vulnerabilities in the Tegro(TGR) 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 Tegro(TGR) 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

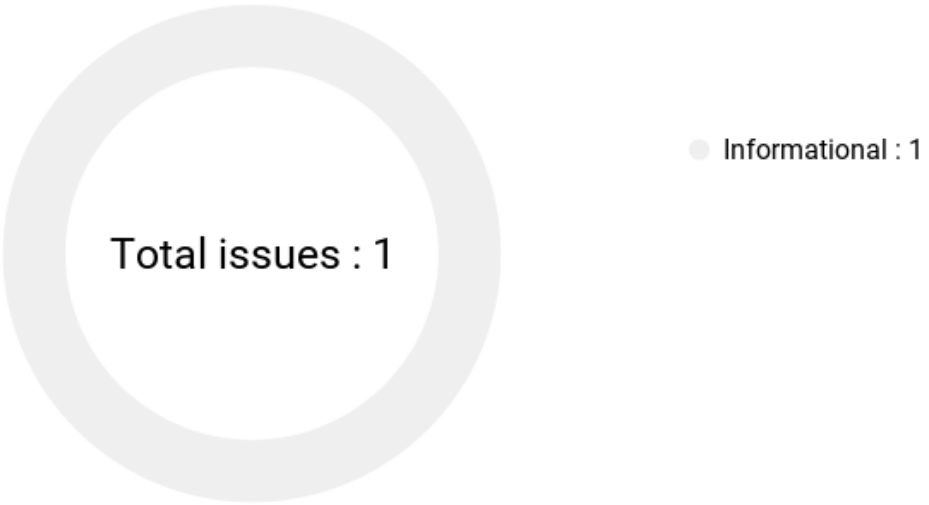
AUDIT OVERVIEW

PROJECT SUMMARY

Project name	Tegro
Description	Tegro – A Cross-Chain Platform for Decentralized Finance. Band Protocol – Secure and scalable decentralized oracle for Web3.0. The token is integrated with the connected stores of the TegroMoney payment system and integration with TON blockchain.
Platform	Binance Smart Chain
Language	Solidity
Codebase	https://bscscan.com/token/0xd9780513292477c4039dfda1cfcd89ff111e9da5#code

FINDINGS SUMMARY

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



AUDIT FINDINGS

Code	Title	Severity
MINT-1	mint limit not imposed	Informational

MINT-1 | mint limit not imposed

Description

The totalSupply for the token is initialized in the constructor but there is also a mint function that can be called by the owner to increase supply. If you would like to cap the total supply at an amount then you may want to add a require statement that checks the added supply does not exceed max supply.

Recommendation

Add supply check if a supply cap is desired:

```
require(_totalSupply.add(amount) < _maxSupply, “MAX_SUPPLY”);
```

Add a max supply state variable:

```
uint256 private constant _maxSupply = <value>;
```

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.