RAPID LABS

SMART CONTRACT SECURITY AUDIT

Final report **Plan: Simple**

Regard

May 2024

RL@RAPIDLABS.FINANCE

RAPIDLABS.FINANCE

TABLE OF CONTENTS

1. Introduction 3

2. Analyzed Contracts 3

3. Audit Process 4

3.1 Auto-analysis 4

3.2 Expert audit 4

4. Known issues checked 4

5. Issue Classification 7

6. Issues 7

6.1 High risk issues 7

6.2 Medium risk issues 7

6.3 Low risk issues 7

7. Conclusion 8

8. Disclaimer 9

9. Static analysis 10

INTRODUCTION

The report has been prepared for Regard.
Regard project description:
Are you tired of the endless parade of copycat animals, cats, dogs and frogs? If you're searching for a meme token that truly gets and represents your chaotic, risk-loving, diamond-handed heart, you've finally found your tribe. REGARD Token is the cryptocurrency built by regards, for regards – the wild ones, the YOLO enthusiasts, the ones who laugh in the face of conventional wisdom.

We're not here to promise you overnight riches or a cushy retirement plan. We're here for the thrill of the ride, the adrenaline rush of a perfectly timed (or spectacularly mistimed) trade, and the camaraderie born from shared victories and legendary losses.
REGARD Token fuels the rocket ship of dreams... dreams filled with rockets, moons, and lambos paid for with those sweet, sweet tendies. Embrace the absurdity, harness the power of the meme, and join the ranks of the most gloriously reckless regards in the cryptosphere.

Name	Regard
Audit date	2024-05-15 - 2024-05-15
Language	Solidity
Platform	Binance Smart Chain

ANALYZED CONTRACTS

Name	Address
AntiBotStandardToken	0x66addb3204359821d7b854da9574b6fafe4331c1

AUDIT PROCESS

Our audit structure consists of two stages:

Auto-analysis

- Our automated tools allow us to scan smart contract code and find potential issues
- We hand pick and verify all the issues found by the tools

Expert audit

- Manual analysis of potential issues and vulnerabilities
- Contract code is reviewed thoroughly

KNOWN ISSUES CHECKED

Title	Result
Unencrypted Private Data On-Chain	✓ passed
Code With No Effects	✓ passed
Message call with hardcoded gas amount	✓ passed
Typographical Error	✓ passed
DoS With Block Gas Limit	✓ passed
Presence of unused variables	✓ passed

Incorrect Inheritance Order	✓ passed
Requirement Violation	✓ passed
Weak Sources of Randomness from Chain Attributes	✓ passed
Shadowing State Variables	✓ passed
Incorrect Constructor Name	✓ passed
Block values as a proxy for time	✓ passed
Authorization through tx.origin	✓ passed
DoS with Failed Call	✓ passed
Delegatecall to Untrusted Callee	✓ passed
Use of Deprecated Solidity Functions	✓ passed
Assert Violation	✓ passed
State Variable Default Visibility	✓ passed
Reentrancy	✓ passed
Unprotected SELFDESTRUCT Instruction	✓ passed
Unprotected Ether Withdrawal	✓ passed

Unchecked Call Return Value	✓ passed
Floating Pragma	✓ passed
Outdated Compiler Version	✓ passed
Integer Overflow and Underflow	✓ passed
Function Default Visibility	✓ passed

ISSUE CLASSIFICATION

High risk	Issues leading to assets theft, locking or any other loss of assets or leading to contract malfunctioning.
Medium risk	Issues that can trigger a contract failure of malfunctioning.
Low risk	Issues that do now affect contract functionality. For example, unoptimised gas usage, outdated or unused code, code style violations, etc.

ISSUES

High risk issues

No issues were found

Medium risk issues

No issues were found

Low risk issues

No issues were found

CONCLUSION

Regard AntiBotStandardToken contract was audited. No risk issues were found.

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 RapidLabs 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 RapidLabs 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.

STATIC ANALYSIS

```
Downloading compiler 0.8.4
Generating typings for: 7 artifacts in dir: typechain-types for target: ethers-v5
Successfully generated 14 typings!
Compiled 1 Solidity file successfully (evm target: istanbul).

INFO:Detectors:
AntiBotStandardToken.allowance(address,address).owner (contracts/contract.sol#590)
shadows:
 - Ownable.owner() (contracts/contract.sol#150-152) (function)
AntiBotStandardToken._approve(address,address,uint256).owner (contracts/
contract.sol#795) shadows:
 - Ownable.owner() (contracts/contract.sol#150-152) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-
variable-shadowing
INFO:Detectors:
AntiBotStandardToken.constructor(string,string,uint8,uint256,address,address,uint25
6).serviceFeeReceiver_ (contracts/contract.sol#491) lacks a zero-check on :
  - address(serviceFeeReceiver_).transfer(serviceFee_) (contracts/
contract.sol#510)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-
zero-address-validation
INFO:Detectors:
Reentrancy in AntiBotStandardToken._transfer(address,address,uint256) (contracts/
contract.sol#716-736):
 External calls:
 - pinkAntiBot.onPreTransferCheck(sender,recipient,amount) (contracts/
contract.sol#725)
 State variables written after the call(s):
 - _balances[sender] = _balances[sender].sub(amount,ERC20: transfer amount exceeds
balance) (contracts/contract.sol#730-733)
 - _balances[recipient] = _balances[recipient].add(amount) (contracts/
contract.sol#734)
Reentrancy in AntiBotStandardToken.transferFrom(address,address,uint256)
(contracts/contract.sol#630-645):
 External calls:
 - _transfer(sender,recipient,amount) (contracts/contract.sol#635)
   - pinkAntiBot.onPreTransferCheck(sender,recipient,amount) (contracts/
contract.sol#725)
```

```
▐State variables written after the call(s):
▐- _approve(sender,_msgSender(),_allowances[sender]
[_msgSender()].sub(amount,ERC20: transfer amount exceeds allowance)) (contracts/
contract.sol#636-643)
▐▐- _allowances[owner][spender] = amount (contracts/contract.sol#802)
Reference: https://github.com/crytic/slither/wiki/Detector-
Documentation#reentrancy-vulnerabilities-2
INFO:Detectors:
Reentrancy in AntiBotStandardToken._transfer(address,address,uint256) (contracts/
contract.sol#716-736):
▐External calls:
▐- pinkAntiBot.onPreTransferCheck(sender,recipient,amount) (contracts/
contract.sol#725)
▐Event emitted after the call(s):
▐- Transfer(sender,recipient,amount) (contracts/contract.sol#735)
Reentrancy in AntiBotStandardToken.transferFrom(address,address,uint256)
(contracts/contract.sol#630-645):
▐External calls:
▐- _transfer(sender,recipient,amount) (contracts/contract.sol#635)
▐▐- pinkAntiBot.onPreTransferCheck(sender,recipient,amount) (contracts/
contract.sol#725)
▐Event emitted after the call(s):
▐- Approval(owner,spender,amount) (contracts/contract.sol#803)
▐▐- _approve(sender,_msgSender(),_allowances[sender]
[_msgSender()].sub(amount,ERC20: transfer amount exceeds allowance)) (contracts/
contract.sol#636-643)
Reference: https://github.com/crytic/slither/wiki/Detector-
Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
AntiBotStandardToken._burn(address,uint256) (contracts/contract.sol#768-779) is
never used and should be removed
AntiBotStandardToken._setupDecimals(uint8) (contracts/contract.sol#813-815) is
never used and should be removed
Context._msgData() (contracts/contract.sol#110-112) is never used and should be
removed
SafeMath.div(uint256,uint256) (contracts/contract.sol#324-326) is never used and
should be removed
SafeMath.div(uint256,uint256,string) (contracts/contract.sol#380-389) is never
used and should be removed
SafeMath.mod(uint256,uint256) (contracts/contract.sol#340-342) is never used and
should be removed
SafeMath.mod(uint256,uint256,string) (contracts/contract.sol#406-415) is never
```

```
used and should be removed
SafeMath.mul(uint256,uint256) (contracts/contract.sol#310-312) is never used and
should be removed
SafeMath.sub(uint256,uint256) (contracts/contract.sol#296-298) is never used and
should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/contract.sol#211-217) is never used
and should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/contract.sol#253-258) is never used
and should be removed
SafeMath.tryMod(uint256,uint256) (contracts/contract.sol#265-270) is never used
and should be removed
SafeMath.tryMul(uint256,uint256) (contracts/contract.sol#236-246) is never used
and should be removed
SafeMath.trySub(uint256,uint256) (contracts/contract.sol#224-229) is never used
and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version=0.8.4 (contracts/contract.sol#461) allows old versions
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-
versions-of-solidity
INFO:Detectors:
Parameter AntiBotStandardToken.setEnableAntiBot(bool)._enable (contracts/
contract.sol#513) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-
Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable AntiBotStandardToken._totalSupply (contracts/contract.sol#480) is too
similar to AntiBotStandardToken.constructor(string,string,uint8,uint256,address,add
ress,uint256).totalSupply_ (contracts/contract.sol#489)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-
names-too-similar
INFO:Detectors:
AntiBotStandardToken.pinkAntiBot (contracts/contract.sol#482) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-
variables-that-could-be-declared-immutable
INFO:Slither:. analyzed (7 contracts with 85 detectors), 26 result(s) found
```

RAPID LABS

YOUR PROJECT SECURED

RL@RAPIDLABS.FINANCE

RAPIDLABS.FINANCE