

Smart Contract Vulnerability Audit

Busd Land

April 26, 2022



Smart Contract – Audit Overview

Project Summary

| | |
|--------------|--|
| Project Name | Busd Land |
| Platform | Binance Smart Chain |
| Language | Solidity |
| Commits | 0x1422C78594b29B1B9E284E234E591beCd7DaDA6e |

Audit Summary

| | |
|---------------------|---------------------------------|
| Delivery Date | April 27, 2022 |
| Method of Audit | Human and AI |
| Consultants Engaged | Two |
| Timeline | April 26, 2022 – April 27, 2022 |

Vulnerability Summary

| Vulnerability Level | Total | Resolved |
|---------------------|-------|----------|
| Critical | 0 | ✓ |
| Major | 0 | ✓ |
| Medium | 0 | ✓ |
| Minor | 0 | ✓ |

Smart Contract - Contract Overview

All information is recorded as of 04/26/2022.

| | |
|----------------------|--|
| Contract Name | BUSDLAND |
| Contract Address | 0x1422C78594b29B1B9E284E234E591beCd7DaDA6e |
| Contract Creator | 0xcdeb20Ad5b4b4Ce6200E033491bBBbd291aee074 |
| Contract Ownership | Renounced Ownership |
| Compiler Version | v0.8.9+commit.e5eed63a |
| Source Code | Solidity |
| Optimization Enabled | Yes with 200 runs |
| Other Settings | default evmVersion, MIT license |
| Verification | Verified |

audits.finance

Smart Contract - Vulnerabilities

| Vulnerability Tested | Human Review | Ai Review | Line(s) Affected | Results |
|--------------------------------------|---|---|------------------|---|
| Function Default Visibility |  |  | |  |
| Integer Overflow and Underflow |  |  | |  |
| Outdated Compiler Version |  |  | |  |
| Unchecked Call Return Value |  |  | |  |
| Unprotected Ether Withdrawal |  |  | |  |
| Unprotected SELFDESTRUCT Instruction |  |  | |  |
| Unencrypted Private Data On-Chain |  |  | |  |

Smart Contract - Vulnerabilities

| Vulnerability Tested | Human Review | Ai Review | Line(s) Affected | Results |
|--------------------------------------|---|---|------------------|---|
| Reentrancy |  |  | |  |
| Uninitialized Storage Pointer |  |  | |  |
| Assert Violation |  |  | |  |
| Use of Deprecated Solidity Functions |  |  | |  |
| Delegatecall to Untrusted Callee |  |  | |  |
| DoS with Failed Call |  |  | |  |
| Code With No Effects |  |  | |  |

Smart Contract - Vulnerabilities

| Vulnerability Tested | Human Review | Ai Review | Line(s) Affected | Results |
|---|---|---|------------------|---|
| Missing Protection against Signature Replay Attacks |  |  | |  |
| Lack of Proper Signature Verification |  |  | |  |
| Requirement Violation |  |  | |  |
| Write to Arbitrary Storage Location |  |  | |  |
| Incorrect Inheritance Order |  |  | |  |
| Insufficient Gas Griefing |  |  | |  |
| Arbitrary Jump with Function Type Variable |  |  | |  |

Smart Contract - Vulnerabilities

| Vulnerability Tested | Human Review | Ai Review | Line(s) Affected | Results |
|---|---|---|------------------|---|
| DoS With Block Gas Limit |  |  | |  |
| Typographical Error |  |  | |  |
| Right-To-Left-Override control character |  |  | |  |
| Presence of unused variables |  |  | |  |
| Unexpected Ether balance |  |  | |  |
| Hash Collisions With Multiple Variable Length Arguments |  |  | |  |
| Message call with hardcoded gas amount |  |  | |  |

Smart Contract - Vulnerabilities

| Vulnerability Tested | Human Review | Ai Review | Line(s) Affected | Results |
|--|---|---|------------------|---|
| Transaction Order Dependence |  |  | |  |
| Block values as a proxy for time |  |  | |  |
| Signature Malleability |  |  | |  |
| Incorrect Constructor Name |  |  | |  |
| Shadowing State Variables |  |  | |  |
| Weak Sources of Randomness from Chain Attributes |  |  | |  |

Smart Contract - Code Analysis

We did not identify any minor or significant vulnerabilities within the contract code.



audits.finance

Smart Contract - Owner Functions

| Function | Description |
|-------------------|------------------------------|
| setDevAddress | Owner can set dev address |
| setDevFee | Owner can set dev fee |
| setBeansInCan | Owner can set miner |
| transferOwnership | Owner can transfer ownership |
| renounceOwnership | Owner can renounce ownership |

Ownership has been renounce

Smart Contract - Contract Functions

- + [Lib] SafeMath
 - [Int] tryAdd
 - [Int] trySub
 - [Int] tryMul
 - [Int] tryDiv
 - [Int] tryMod
 - [Int] add
 - [Int] sub
 - [Int] mul
 - [Int] div
 - [Int] mod
 - [Int] sub
 - [Int] div
 - [Int] mod
- + Context
 - [Int] _msgSender
 - [Int] _msgData
- + Ownable (Context)
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Int] _transferOwnership #
- + [Int] ERC20
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #
- + BUSDLAND (Context, Ownable)
 - [Pub] <Constructor> #
 - [Pub] hatchEggs #
 - [Pub] sellEggs #
 - [Pub] beanRewards
 - [Pub] buyEggs #
 - [Prv] calculateTrade
 - [Pub] calculateEggSell
 - [Pub] calculateEggBuy
 - [Pub] calculateEggBuySimple
 - [Prv] devFee
 - [Pub] seedMarket #
 - [Pub] getBalance
 - [Pub] getMyMiners
 - [Pub] getMyEggs
 - [Pub] getEggsSinceLastHatch
 - [Pub] setBeansInCan #
 - modifiers: onlyOwner
 - [Pub] setDevFee #
 - modifiers: onlyOwner
 - [Pub] setDevAddress #
 - modifiers: onlyOwner
 - [Prv] min

(S) = payable function

= non-constant function



audits.finance

DISCLAIMER

Audits.finance Inc. is in no way responsible or liable for any legal actions resulting from the use of this presentation. By reading this audit or any part of it, you agree to the terms of this disclaimer. If you do not agree to these terms, please stop reading now, and delete any duplicates of this report. Audits.finance Inc. is an official auditor utilizing the Solidity auditing industry standard. Audits.finance hereby excludes any liability and responsibility. Neither you nor any other person shall have any claim against Audits.finance for any economic loss or damages. Audits.finance Inc. does not guarantee the authenticity of a project, nor does it guarantee the project will not participate in one or any scamming including but not limited to, removing liquidity, selling off team supply, or exit scams. Audits.finance Inc. does not give investment advice in any way. Audits.finance Inc. supplies this presentation for information purposes only, and strongly suggests that none of this information be used as investment advice. Audits.finance in no way endorses or recommends any projects that it audits. Audits.finance is solely responsible for smart contract and project analysis of the projects that it is contracted to audit. Audits.finance may be contracted by teams, investors, or any other 3rd party in regard to a contract address or project. Audits.finance provides a full report for informational purposes only.



audits.finance

Contact information:

Website: audits.finance

Telegram: [auditsfinancegroup](https://t.me/auditsfinancegroup)

Twitter: [auditsfinance](https://twitter.com/auditsfinance)

Email: hello@audits.finance