

Smart Contract Vulnerability Audit

Wolf Pack

April 25, 2022



Smart Contract – Audit Overview

Project Summary

Project Name	Wolf Pack
Platform	Binance Smart Chain
Language	Solidity
Commits	0x4460beAA64d1cE7840300a4f7b0F2b443a10fd5F

Audit Summary

Delivery Date	April 25, 2022
Method of Audit	Human and AI
Consultants Engaged	Two
Timeline	April 25, 2022 – April 25, 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 04/25/2022.

Contract Name	WolfPack
Contract Address	0x4460beAA64d1cE7840300a4f7b0F2b443a10fd5F
Contract Creator	0x4AcB95908B1de5Cf1F484774aD57930C2504EA28
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Outdated Compiler Version				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
CHANGE_OWNERSHIP	Admin can change ownership of contract
CHANGE_DEV1	Admin can change dev1 address
CHANGE_DEV2	Admin can change dev2 address
CHANGE_DEV3	Admin can change dev3 address
CHANGE_DEV	Admin can change dev address
CHANGE_MKT_WALLET	Admin can change marketing wallet
PRC_TAX	Admin can set prc tax (max 10%)
PRC_REFERRAL	Admin can set prc referral (max 10%)
PRC_MARKET_EGGS_DIVISOR	Admin can set market egg divisor
SET_WITHDRAWAL_TAX	Admin can set withdraw (max tax is 80%)
SET_COMPOUND_FOR_NO_TAX_WITHDRAWAL	Set compound with no tax
BONUS_DAILY_COMPOUND	Set daily bonus compound (900)
BONUS_DAILY_COMPOUND_BONUS_MAX_TIMES	Set daily compound times (30)
SET_MIN_INVEST_LIMIT	Admin can set min investment limit
SET_CUTOFF_STEP	Admin can cutoff step
SET_WITHDRAW_COOLDOWN	Admin can set withdraw cooldown
SET_WALLET_DEPOSIT_LIMIT	Admin can set wallet deposit limit

Smart Contract - Contract Functions

- + [Int] IToken
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #

- + [Lib] SafeMath
 - [Int] mul
 - [Int] div
 - [Int] sub
 - [Int] add
 - [Int] mod

- + WolfPack
 - [Pub] <Constructor> #
 - [Int] isContract
 - [Pub] hatchEggs #
 - [Pub] sellEggs #
 - [Pub] buyEggs #
 - [Int] payFees #
 - [Pub] getDailyCompoundBonus
 - [Pub] getUserInfo
 - [Pub] initialize #
 - [Pub] getBalance
 - [Pub] getTimeStamp
 - [Pub] getAvailableEarnings
 - [Pub] calculateTrade
 - [Pub] calculateEggSell
 - [Pub] calculateEggBuy
 - [Pub] calculateEggBuySimple
 - [Pub] getEggsYield
 - [Pub] calculateEggSellForYield
 - [Pub] getSiteInfo
 - [Pub] getMyMiners
 - [Pub] getMyEggs
 - [Pub] getEggsSinceLastHatch
 - [Prv] min
 - [Ext] CHANGE_OWNERSHIP #
 - [Ext] CHANGE_DEV1 #
 - [Ext] CHANGE_DEV2 #
 - [Ext] CHANGE_DEV3 #
 - [Ext] CHANGE_MKT_WALLET #
 - [Ext] PRC_EGGS_TO_HIRE_1MINERS #
 - [Ext] PRC_TAX #
 - [Ext] PRC_REFERRAL #
 - [Ext] PRC_MARKET_EGGS_DIVISOR #
 - [Ext] SET_WITHDRAWAL_TAX #
 - [Ext] SET_COMPOUND_FOR_NO_TAX_WITHDRAWAL #
 - [Ext] BONUS_DAILY_COMPOUND #
 - [Ext] BONUS_DAILY_COMPOUND_BONUS_MAX_TIMES #
 - [Ext] BONUS_COMPOUND_STEP #
 - [Ext] SET_MIN_INVEST_LIMIT #
 - [Ext] SET_CUTOFF_STEP #
 - [Ext] SET_WITHDRAW_COOLDOWN #
 - [Ext] SET_WALLET_DEPOSIT_LIMIT #



audits.finance

(\$) = payable function

= non-constant function

Smart Contract - Tokenomics

At the time of audit the transaction fees ("tax") listed below are the fees associated with trading. These fees are taken from every buy and sell transaction unless otherwise stated. Token taxes vary by each project. All tokenomics show below is what is shown on the token website.

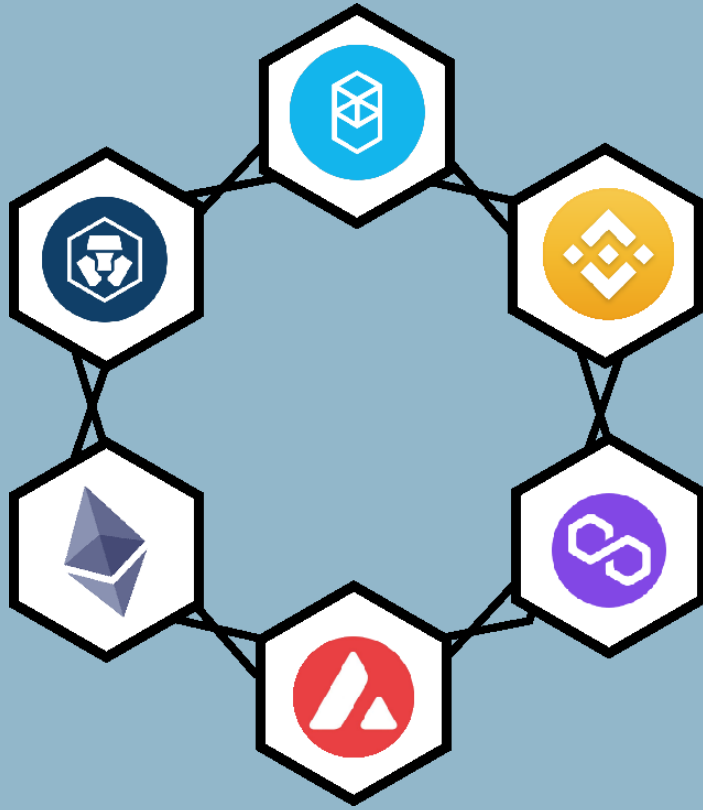


 **Join the Hunt!**

- 8% Daily ~ 2920% APR**
- 8% Referral Bonus**
- 5% Development/Marketing Fee**
- 2.5% Hunt Bonus**
- 12 Hours Compound Timer**
- 4 Hours Withdraw Cooldown**
- 48 Hours Rewards Accumulation Cut-Off**
- 5 Times Mandatory Compound Feature**

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