expelee

Building the Futuristic Blockchain Ecosystem

Audit Report

FOR

CorgiSwap

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

Audit Result	Passed
KYC Verification	Not Done
Audit Date	2nd Nov 2022

-Team Expelee

PROJECT DESCRIPTION

CorgiSwap

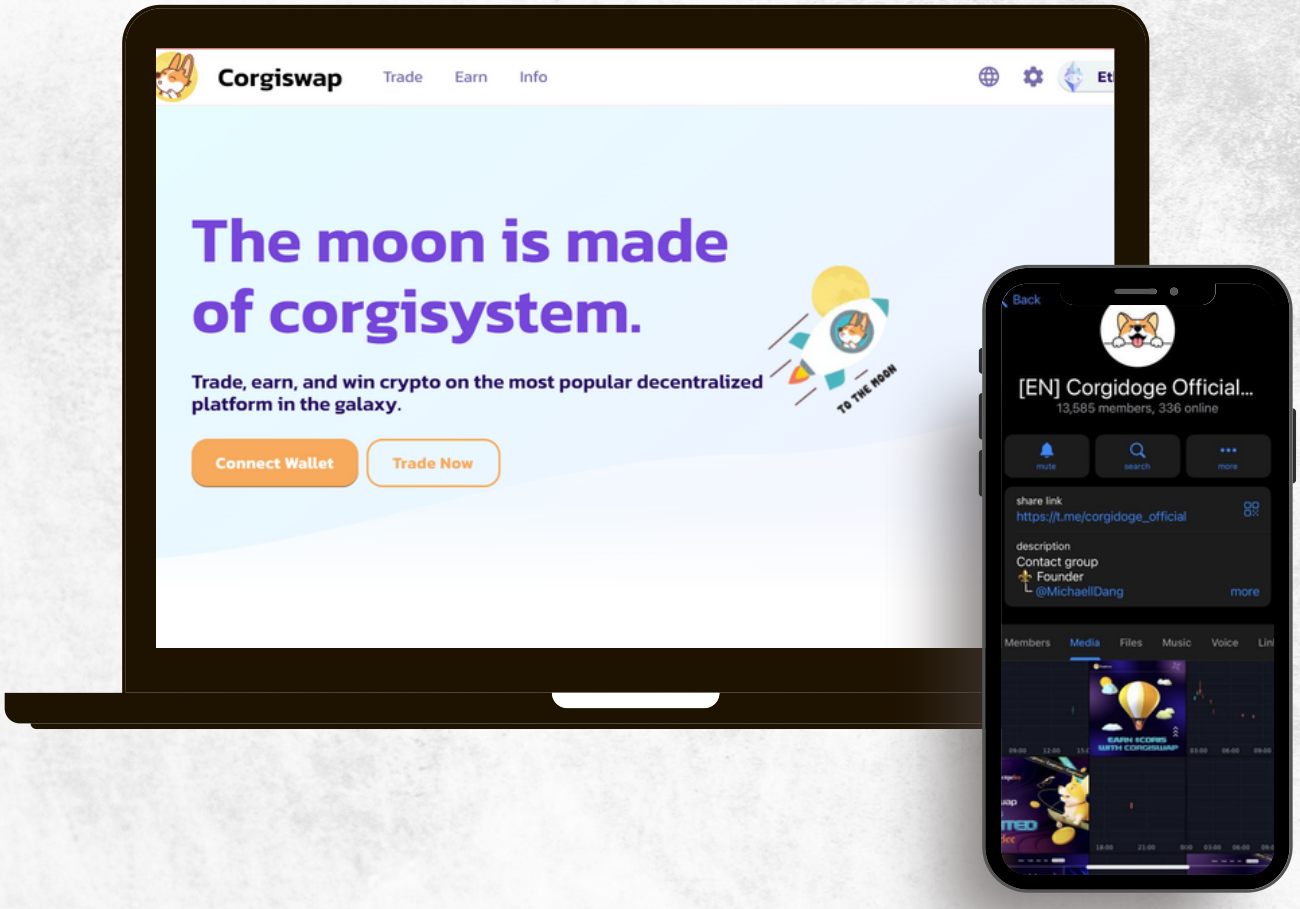
The moon is made of corgisystem.
Trade, earn, and win crypto on the most popular decentralized platform in the galaxy.
CorgiSwap has the most users of any decentralized platform, ever.
And those users are now entrusting the platform with over $6.1 billion in funds.

expelee

expelee.com

Social Media Profiles

CorgiSwap



http://beta.corgiswap.org/?chainId=10001

https://t.me/corgidoge_official

https://twitter.com/corgidogeestate

It's always good to check the social profiles of the project, before making your investment.

-Team Expelee

CONTRACT DETAILS

Name : CorgiSwap
Symbol: CORIS
Token: ERC20/ERC20Votes

- **Token Address:** 0x5187816A80A61B67b9879AEA87eA0890A493396b
- **Staking Contract Address:** 0x9A1B1F3585d905A159a37f9a091312EdD9dE2609
- **Token Owner:** 0x9A1B1F3585d905A159a37f9a091312EdD9dE2609
- **Staking Contract Owner:** 0x22240932f49dcd5b97797fc2f594d7e84061b642 **(EOA)**
- **Staking Contract SHA-256 Checksum:** b366b954a8c4a640c7683e277d1b8c1f1daee5f9766e74d8a4bd6e338bf293ed
- **Token Contract SHA-256 Checksum:** 3b6623b0930b2d31438956f013605227206470b54975363c14c1e2bf85b7108a

AUDIT METHODOLOGY

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Complier
- Hardhat

VULNERABILITY CHECKLIST

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

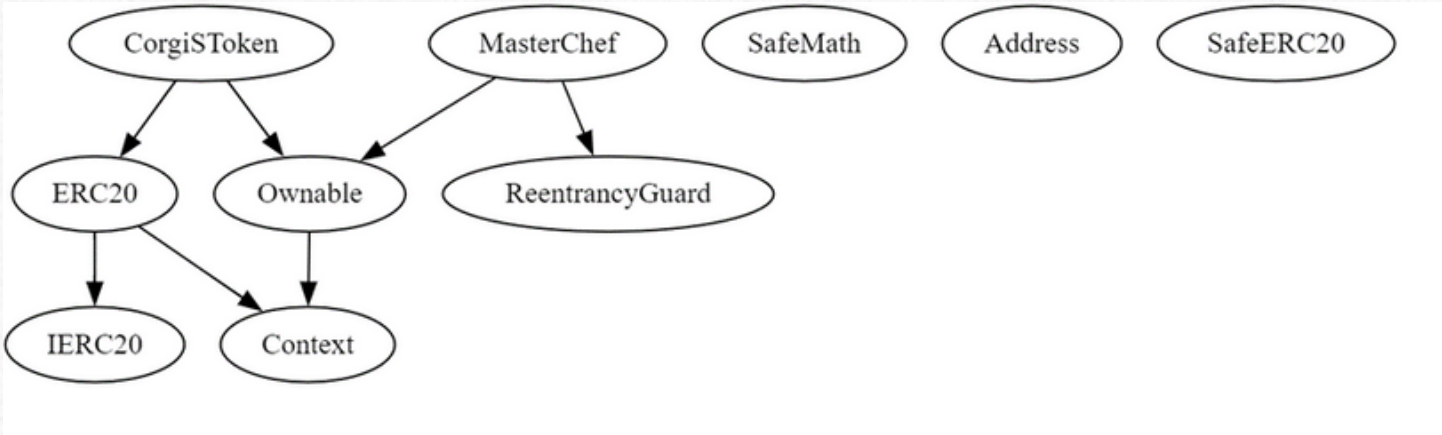
AUDIT SUMMARY

Audit Scope:

Staking Contract Owner:

0x22240932f49dcd5b97797fc2f594d7e84061b642 (EOA)

Contracts & Inheritance Tree:



Summary

- CorgiSwap is a ERC20 Token with voting and delegation functionality
- CorgiSwap is the reward token for Corgi's staking contract.
- There is 0% taxes on buys/sells/transfers
- Owner is not able to set taxes
- Owner is not able to blacklist an arbitrary address from buying/selling/transferring
- Owner is not able to disable trades
- Staking contract is derivied from Sushu MasterChef staking contract
- There are a certain number of CorgiSwap tokens per block, this tokens get accomulated in the contract and will be splitted between pools based on their allocation point.

MANUAL AUDIT

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to a methodology based on
OWASP standards.
Vulnerabilities are divided into three primary risk categories: high, medium, and low.

High-level considerations for vulnerabilities span the followingkey areas when conducting assessments:

- Malicious Input Handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Findings Summary

- High Risk Findings:2
- Medium Risk Findings:3
- Low Risk Findings:0
- Suggestions & discussion: 0
- Gas Optimizations : 2

High Risk Findings

Centralization- withdrawing can be reverted for some users:
this is issue is met when there is not enough tokens in the contract, i.e, owner should deposit some amount of staking tokens to the contract to cover rewards, otherwise rewards will be paid from staking amounts, and this means there wont be enough tokens in the contract for some users to withdraw.

Centralization - a malicous owner is able to set Corgi per block reward to an arbitrary number, in combination with last issue, owner is able to get all the new Corgi tokens to his own wallet. there is not a limit for Corgi per block rewards and also since rewards are minted and total supply is not static this issue is considered as a high centralization risk.

```
function setReward(uint256 _corgiSPerBlock) public onlyOwner {
corgiSPerBlock = _corgiSPerBlock;
}
```

Suggestion : set a limit for at setReward function for max corgiSPerBlock number.

Medium Risk Findings

Logical - Dev portion is not deducted from total rewards, as you can see in the code, we are minting +10% more rewards to devaddr

```
uint256 corgiSReward =
multiplier.mul(corgiSPerBlock).mul(pool.allocPoint).div(totalAllocPoint);
corgiS.mint(devaddr, corgiSReward.div(10)); //@audit minting +10%
corgiS.mint(address(this), corgiSReward);
```

Suggestion : we should reduce corgiSRewrad by 10% after sending that 10% to devaddr

Centralization -Corgi token has a mint function which is only callable by Corgi's Staking Contract, there are couple of ways for a malicious owner to mint new tokens & votes to himself which are discussed in "High Risk" section

Oudated Compiler Version -Corgi token has a mint function which is only callable by Corgi's Staking Contract, there are couple of ways for a malicious owner to mint new tokens & votes to himself which are discussed in "High Risk" section

Gas Optimizations

- update compiler version to > 0.8.0 to avoid using SafeMath library and also for other optimizations
- define StartBlock as immutable

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 Start-up. Coping up with numerous solutions for blockchain Security and constructing a Web3 Ecosystem from Deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

www.expelee.com

expeleeofficial

expelee

Expelee

expelee

expelee_official

expelee-co

expelee

Building the Futuristic **Blockchain Ecosystem**

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always Do your own research and protect yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.