expelee

Building the Futuristic Blockchain Ecosystem

Audit Report FOR

Qroniswap

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 with medium Risk
KYC Verification	Done
Audit Date	23 Sep 2022

Why Passed?

Because staking wallet is an EOA (externaly owner account) and not a contract address, and because there could be up to 20% tax on withdrawals, there are also couple of issues that can not disable the whole system but is better to be applied

-Team Expelee

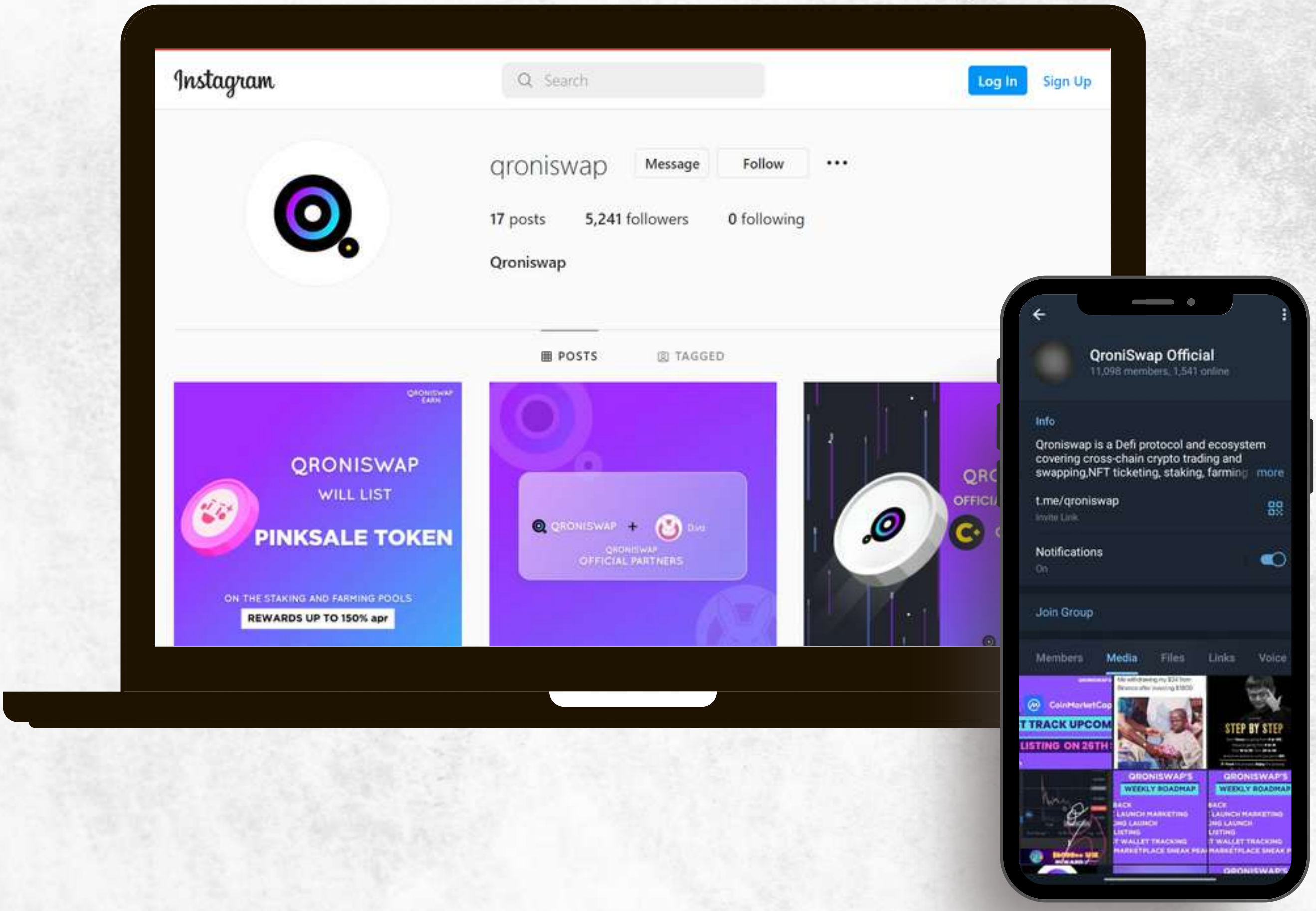
PROJECT DESCRIPTION

Qroniswap

Qroniswap is a DeFi protocol and ecosystem covering cross-chain crypto trading and swapping, NFT ticketings, and fiat on-ramp payments. Qroniswap's robust ecosystem is such that allows for deep liquidity and seamless crypto transactions, all spiced up with incentivized earning models which allow users' assets to create passive streams of income while they engage in other activities on the protocol.

Social Media Profiles

Qroniswap



qroniswap

17 posts 5,241 followers 0 following

Qroniswap

QroniSwap Official
11,098 members, 1,541 online

Info

Qroniswap is a Defi protocol and ecosystem covering cross-chain crypto trading and swapping,NFT ticketing, staking, farming more

t.me/qroniswap
Invite Link

Notifications
On

https://qroni.io

https://t.me/qroniswap

https://twitter.com/qroniswap

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

-Team Expelee

CONTRACT DETAILS

Contract Name

MasterChef

Token Type

Staking Contract

Network

BSC

Language

Solidity

Contract Address (Verified)

0x78E893603C7c481263C7a0CfD5fb49936576C9c1

Total Supply

-

Decimals

-

Compiler

v0.8.13+commit.abaa5c0e

License

MIT license

Contract SHA-256 Checksum:

02ec17a64e5efb69b592ec12e4ab86d8c12bd9368bc2abd176ed1f4b4140443a

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

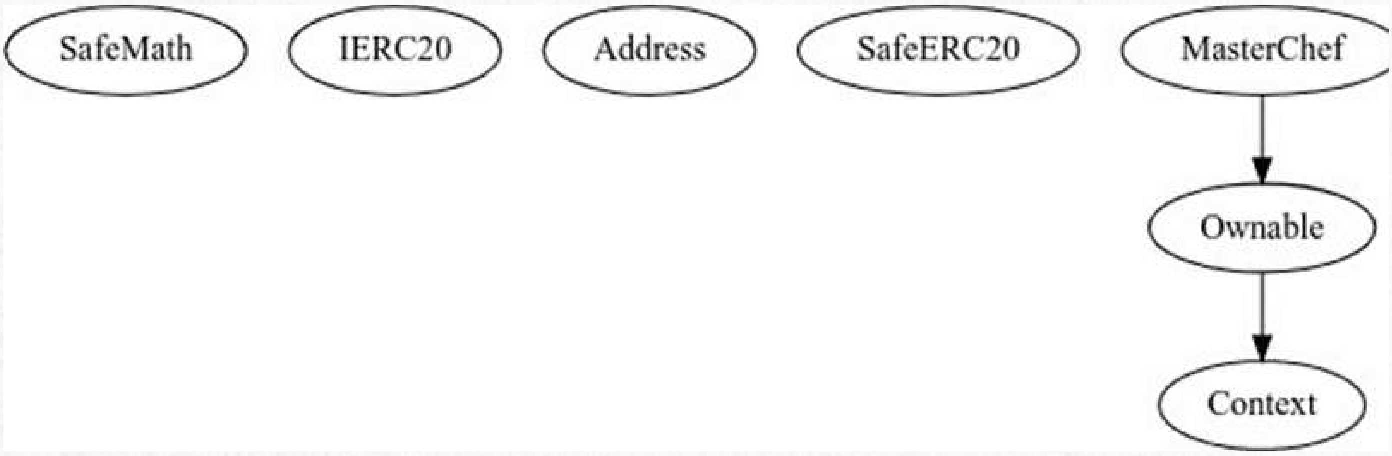
Ownership:

Current owner of MasterChef is:
0x53d5e8ade9f532bfaeff5ff1d86116def8968e79

Contracts & Inheritance Tree:

all of below contractsare in this audit scope

MasterChef.sol
Used libraries are SafeMath for uint256 and SafeERC20 for ERC20 typesAlso used IERC20 interface to handle ERC20 transfering operations



Summary

Staking contract dereived from Sushi Masterchef contract.
Owner can set up to 20% tax for deposits, this tax is deducted from deposited amount By staking a pool token, you receive QNI per block.
Rewards calculation:
there is a total amount of QNI rewards after N blocks considering that QNI per block is X (for sushi masterchef this number is 5, which means there would be totaly N * 5 sushi rewards after N blocks):

each pool takes a share of this total rewards based on its allocationpoint, sum of all this allocation points is total allocation points, so if we assume that:
allocation point = AP
total allocation points = ALP
the way this share is calculatedis:
PQS (Pool QNI Share) = TQR * (AP / ALP) (and this amount will be used to pay rewards for stakersof that pool.)
based on how much Staking tokens a pool has (for example;for a USDT pool Staking token is
USDT), the QNI Per Staking tokens is calculated in this formula:
TST = Total Staked Tokens

CQPS = Current Pool's QNI Per Share
a user rewardsare calculated in this way:

UST = User Staked Tokens

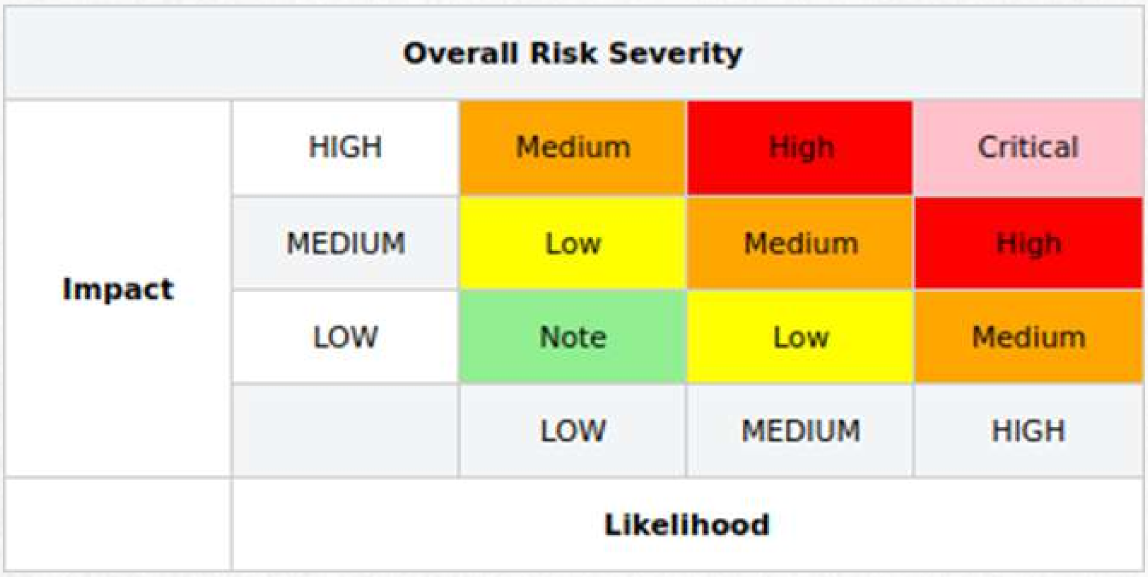
MANUAL AUDIT

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:1
- Medium Risk Findings:3
- Low Risk Findings:3
- Suggestions & discussion: 1
- Gas Optimizations : 2

High Risk Findings

- Centralization - staking wallet at
- 0x0a943fcb6ea7e0c7373ad95c82c8df37f5aa78b8 is an EOA, a privatekey leak or an attempfrom a malicious owner to access this token funds can affect the price very bad

Medium Risk Findings

- Centralization - a pool can charge up to 20% fee for deposit, this fee will be deducted from deposited amount
  Allevation:
- "therewas no limit for this amount of fee in Qroni previousstaking contract, after we awared them of this issue, they determineda 20% limit for fees"
- Validation - no address validationfor setStakingWallet and setFeeAddress, setting this addresses to address 0 leads to unexpected behaviours.

- **Logical - Accidently setting feeAddress to a wrong address(dead address) is irreversible since only feeAddress owner is able to change feeAddress, owners need to redeploy the contract in order to receive fee tokens if this happen.**
  Expelee:
  "allow owner to change feeAddress"

Low Risk Findings

- **Centralization - A maliciousowner is able to add a pool with any token (even a token with no liquditiy) to the staking contract**
- **Logical - stakingwallet at 0x0a943fcb6ea7e0c7373ad95c82c8df37f5aa78b8 currently holds only 750 QNI token, if there is not tokens in this wallet, then no one would be able to use withdraw function to withdraw his/her funds, we define this as a low risk issue because everyone can use emergency Withdraw function to remove their tokens from staking contract.**
- **Centralization - owner is able to set stakingWallet to any address even dead address. if owner set it to an addressthat doesn't hold any QNI token normal withdrawals will be disabled(if there is any rewards), this is a low risk issue, because everyone can use emergencywithdraw to withdrawhis/her tokens**

Optimizations

- no need to use SafeMathif compiler versionis more than 0.8.0
- define add functionas external, this function never been used inside the contract

Suggestions

- there are some event argumentsthat could have "indexed" keyword, as their size if fixed and you can use up to 3 indexed arguments: Deposit, Withdraw, EmergencyWithdraw, Add, Set

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.