



# Royalproof

## Security Audit Report



Completed on

**15,02,2023**



## OVERVIEW

This audit has been prepared for RioGreen to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal ”

**- RoyalProof Team -**



# TABLE OF CONTENTS

|                                     |    |
|-------------------------------------|----|
| OVERVIEW .....                      | 2  |
| TABLE OF CONTENTS .....             | 3  |
| PROJECT DESCRIPTION .....           | 4  |
| CONTRACT INFO .....                 | 5  |
| OUR CONTRACT REVIEW PROCESS .....   | 6  |
| CURRENT STATS .....                 | 7  |
| TOKEN TRANSFERS STATS .....         | 8  |
| SMART CONTRACT STATS .....          | 8  |
| FEATURED WALLETS .....              | 9  |
| VULNERABILITY CHECK .....           | 10 |
| THREAT LEVELS .....                 | 11 |
| TOKENOMICS: .....                   | 13 |
| WEBSITE .....                       | 14 |
| SOCIAL MEDIA& ONLINE PRESENCE ..... | 15 |
| DISCLAIMER .....                    | 17 |



## PROJECT DESCRIPTION

According to their website: Rgreen is a company that has made its mission to focus on clean energy and renewable energy. With the help of advanced technologies, Rgreen is committed to making the world a greener place. They are dedicated to creating innovative solutions that will help reduce emissions and pollution while providing sustainable energy solutions.

**Category: Energy Sector**



# CONTRACT INFO

|                         |  |
|-------------------------|--|
| <b>Token Name</b>       | RioGreen                                   |
| <b>Symbol</b>           | RGREEN                                     |
| <b>Contract Address</b> | 0x7661968f677A5D926a91785308BA029C6E9e60A6 |
| <b>Network</b>          | Binance Smart Chain                        |
| <b>Language</b>         | Solidity                                   |
| <b>Deployment Date</b>  | Dec-12-2022                                |
| <b>Verified?</b>        | Yes  |
| <b>Total Supply</b>     | 318,019,580                                |
| <b>Status</b>           | launched                                   |

## TAXES

|                 |    |
|-----------------|----|
| <b>Buy Tax</b>  | 0% |
| <b>Sell Tax</b> | 0% |



# Our Contract Review Process

The contract review process pays special attention to the following:

Testing the smart contracts against both common and uncommon vulnerabilities

- ❖ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ❖ Ensuring contract logic meets the specifications and intentions of the client.
- ❖ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ❖ Thorough line-by-line manual review of the entire codebase by industry experts.
  
- ❖ Blockchain security tools used:
  - ✓ Open Zeppelin
  - ✓ Mythril
  - ✓ Solidity Compiler
  - ✓ Hardhat



# CURRENT STATS

(As of Feb 14, 2023)

**Status:** Launched

**Liquidity:** 15\$

**Burn:** 0%

**MaxTxAmount:** No limit

**DEX:** Pancakeswap

**LP Address(es):** 0xd9DB8D92B1455b01C343162a09F1921af3802636



# TOKEN TRANSFERS STATS

|                         |                              |
|-------------------------|------------------------------|
| Transfer Count          | 34                           |
| Uniq Senders            | 1                            |
| Uniq Receivers          | 1                            |
| Total Amount            | 1,000                        |
| Median Transfer Amount  | 1,220,000                    |
| Average Transfer Amount | 3,197,351                    |
| First transfer date     | Dec 12,2022                  |
| Last transfer date      | Jan-30-2023 04:10:18 PM +UTC |
| Days token transferred  | 1                            |

# SMART CONTRACT STATS

|                       |   |
|-----------------------|---|
| Calls Count           | No data points found for the current time series. |
| External calls        | No data points found for the current time series. |
| Internal calls        | No data points found for the current time series. |
| Transactions count    | No data points found for the current time series. |
| Uniq Callers          | No data points found for the current time series. |
| Days contract called  | No data points found for the current time series. |
| Last transaction time | No data points found for the current time series. |
| Created               | No data points found for the current time series. |
| Create TX             | No data points found for the current time series. |
| Creator               | No data points found for the current time series. |





# FEATURED WALLETS

|                         |  |
|-------------------------|--|
| Owner address           | Oxb9c587517a2fefafcdc64e2d73e43bdd4eb83381 |
| *Marketing fee receiver | Ox7661968f677A5D926a91785308BA029C6E9e60A6 |
| Dev fee receiver        | Ox7661968f677A5D926a91785308BA029C6E9e60A6 |
| LP address              | Oxd9db8d92b1455b01c343162a09f1921af3802636 |

\*Address can be changed in future



# VULNERABILITY CHECK

|  |        |
|--|--------|
| Design Logic   | Passed |
| Compiler warnings.   | Passed |
| Private user data leaks  | Passed |
| Timestamp dependence   | Passed |
| Integer Overflow and Underflow                                 | Passed |
| Race conditions and 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 |



# THREAT LEVELS

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.



## Medium Risk

If any user use transferFrom Function to transfer tokens from a holder to his address it will throw error but the tokens will be transferred

```
function transferFrom(address sender, address recipient, uint256 amount) external returns (bool) {  
    _transfer(sender, recipient, amount);  
    _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount, "BEP20: transfer amount exceeds allowance"));  
    return true;  
}
```

Contract Owner Can mint unlimited Tokens

```
function mint(uint256 amount) public onlyOwner returns (bool) {  
    _mint(_msgSender(), amount);  
    return true;  
}
```



# Tokenomics:

**There is no tokenomics about initial tokens distribution on the project's whitepaper.**





# Website

|                    |   |
|--------------------|---|
| Website URL        | <a href="https://rgreen.riostaking.com/">https://rgreen.riostaking.com/</a> |
| Technical SEO Test | passed  |
| Security Test      | Passed, SSL certificate present   |

## Design

- Very nice color scheme and overall layout.

## Whitepaper

- Well written, explanatory.
- The information helps new investors understand what the product does right away. No grammar mistakes found..

## Content

## Roadmap

- Yes, goals set without time frames..

## Mobile-friendly?.

- Yes

<https://rgreen.riostaking.com>



# SOCIAL MEDIA& ONLINE PRESENCE

## ANALYSIS

Project's social media pages are very active with activity from organic users.



**Twitter:** @riostakinginc

- 1234 Followers
- Very active
- Posts few times a day



**Telegram:** @riostakingsupport

- 1139 members
- Active members
- Active mods



**Youtube:** @riostakingsupport

- 9 subscribers
- Active mods



**TikTok:** @riostakinginc

- 3177 Followers
- Active community
- Active mods



**Instagram:** @rio\_staking\_official

- 2171 followers
- Active members



# ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

## RoyalProof

### CRYPTO SECURITY

**Audits | KYCs | dApps  
Contract Development**

## FIND US ONLINE



<https://royalproof.net/>



@RoyalproofAudit



@RoyalProofOfficial



<https://github.com/Royal-Proof>



@RoyalProofAudit



@Royalproof\_Admin





# Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

## DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and Royal Proof and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Royal Proof) owe no duty of care towards you or any other person, nor does Royal Proof make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Royal Proof hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Royal Proof hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Royal Proof, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.