TECH
RATE

SMART CONTRACTS SECURITY

AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

Outer Ring

Deployer address

Not deployed

Client contacts:

Outer Ring team

Blockchain

BNB Smart Chain (Not deployed)

Project website:

https://dapp.outerringmmo.com

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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 alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by Outer Ring to perform an audit of smart contracts on commit:

https://github.com/NexxyoLabs/OR.Blockchain.Crafting/commit/8934c4ac0532d1bb9d7c336d8dd5827461e779e2

Audit scope:

- LandStaking.sol
- ArmorsController.sol
- RarityController.sol
- WeaponsController.sol
- CraftingSharedStorage.sol
- BaseStep.sun
- CraftingAssembly.sol
- CraftingCreation.sol
- CraftingStyling.sol
- ResourcesController.sol

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.

- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Issues Checking Status

Issue description	Checking status
1. **Compiler errors.**	Passed
2. **Race conditions and Reentrancy. Cross-function race conditions.**	Passed
3. **Possible delays in data delivery.**	Passed
4. **Oracle calls.**	Passed
5. **Front running.**	Passed
6. **Timestamp dependence.**	Passed
7. **Integer Overflow and Underflow.**	Passed
8. **DoS with Revert.**	Passed
9. **DoS with block gas limit.**	Low issues
10. **Methods execution permissions.**	Passed
11. **Economy model of the contract.**	Passed
12. **The impact of the exchange rate on the logic.**	Passed
13. **Private user data leaks.**	Passed
14. **Malicious Event log.**	Passed
15. **Scoping and Declarations.**	Passed
16. **Uninitialized storage pointers.**	Passed
17. **Arithmetic accuracy.**	Passed
18. **Design Logic.**	Passed
19. **Cross-function race conditions.**	Passed
20. **Safe Open Zeppelin contracts implementation and usage.**	Passed
21. **Fallback function security.**	Passed

TECH
RATE

Security Issues

⊘ High Severity Issues

No high severity issues found.

⊘ Medium Severity Issues

No medium severity issues found.

⊗ Low Severity Issues

1. Out of gas

Issue:

- (LandStaking) Functions changePoolRewards(), getUserPendingRewards(), _computePendingRewards() uses the loop to iterate through pools list. Function will be aborted with OUT_OF_GAS exception if there will be a long list of pools.
- (ArmorsController) Contract uses even triple loops to iterate through lists. Function will be aborted with OUT_OF_GAS exception if there will be a long list.
- (WeaponsController) Contract uses even triple loops to iterate through lists. Function will be aborted with OUT_OF_GAS exception if there will be a long list.

Recommendation:
Check that the array length is not too big and be careful about nested loops.

Notes:

- LandStaking stakeLand() function no longer need to be payable.

Owner privileges (In the period when the owner is not renounced)

- LandStaking
  - PAUSER can pause the contract.
  - PAUSER can unpause the contract.
  - MANAGER can change the land contract address.
  - MANAGER can change the staking token.
  - MANAGER can change the staking fee.
  - MANAGER can change the fee receiver address.
  - MANAGER can change the oracle prices address.
  - MANAGER can change crafting cost reduction per pool.
  - MANAGER can change crafting time reduction per pool.
  - MANAGER can change pool rewards.
  - MANAGER can add a land type.
  - BLOCKER can set the block duration for a specific size.
  - BLOCKER can set the block duration for the top land size.

- ArmorsController
  - MANAGER can set the description of an armor piece.
  - MANAGER can set descriptions for multiple armor pieces.
  - MANAGER can set the number of aesthetics for an armor piece.
  - MANAGER can set the number of aesthetics for multiple armor pieces.
  - MANAGER can set resources for a specific tier and step of an armor piece.
  - MANAGER can set resources for all steps of an armor piece.
  - MANAGER can set the crafting time for a specific tier and step of an armor piece.
  - MANAGER can set the crafting time for multiple armor pieces.
  - MANAGER can set the crafting time for multiple armor pieces across tiers and steps.
  - MANAGER can set the skip time price for a specific tier and step of an armor piece.
  - MANAGER can set the skip time price for multiple armor pieces.
  - MANAGER can set the skip time price for multiple armor pieces across tiers and steps.
  - MANAGER can set the address of the armor piece contract.

- RarityController
  - MANAGER can set rarity description.
  - MANAGER can set rarity probability.
  - MANAGER can set rarity booster price.
  - MANAGER can set rarity booster token.

- WeaponsController
  - MANAGER can set weapon pieces aesthetics.
  - MANAGER can set weapon pieces type.
  - MANAGER can set weapon pieces aesthetic elements.
  - MANAGER can set weapon types description.
  - MANAGER can set weapon types pieces.
  - MANAGER can set weapon type all steps resources.
  - MANAGER can set weapon types crafting time.
  - MANAGER can set weapon types all tiers crafting time.
  - MANAGER can set weapon types skip time price.
  - MANAGER can set weapon types all tiers skip time price.
  - MANAGER can set weapon type address.

- CraftingSharedStorage
  - MANAGER can set the collection ID.
  - MANAGER can set the collection name.
  - MANAGER can set the default URI for NFTs.
  - MANAGER can set the crafting token address.
  - MANAGER can set the crafting fee.
  - MANAGER can set the payment recipient address.
  - MANAGER can set the fee recipient address.
  - MANAGER can set the ArmorsController contract address.
  - MANAGER can set the WeaponsController contract address.
  - MANAGER can set the RarityController contract address.
  - MANAGER can set element descriptions.
  - STYLING can set crafting item aesthetics.
  - ASSEMBLY can set crafting item rarity boosters.
  - ASSEMBLY can set crafting item rarity.

- BaseStep
  - MANAGER can change the oracle address.
  - MANAGER can change the craftingSharedStorage address.
  - MANAGER can change the landStaking contract address.

- CraftingAssembly
  - PAUSER can pause the contract.
  - PAUSER can unpause the contract.
  - MANAGER can change the resourcesController address.
  - CREATION can add an item to the assembly pools.

- CraftingCreation
  - PAUSER can pause the creation process.
  - PAUSER can unpause the creation process.
  - MANAGER can change crafted items by tier.
  - MANAGER can change the ResourcesController contract address.

- MANAGER can change the CraftingStyling contract address.
- MANAGER can change the price of a specific pool.
- MANAGER can update the state of item creation.

- CraftingStyling
  - PAUSER can pause the contract.
  - PAUSER can unpause the contract.
  - MANAGER can change the ResourcesController contract address.
  - MANAGER can change the CraftingAssembly contract address.
  - MANAGER can change the price of optional weapon pieces.
  - CREATION can add an item to the styling pools.

- ResourcesController
  - BURNER can burn user resources.

Conclusion

Smart contracts contain low severity issues! The further transfers and operations with the funds raise are not related to this particular contract.

Security score: 80.

TechRate note:
Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.