TechRate
September, 2023

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

basedrate

Deployer address

Not deployed

Client contacts:

basedrate team

Blockchain

Not deployed

Project website:

Not provided

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 basedrate to perform an audit of smart contracts on commit:
https://github.com/basedrate/contracts/commit/fe3aecffa52933c9f53adb8e9152c408e1f5f0a9

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.**	Low issues
19.	**Cross-function race conditions.**	Passed
20.	**Safe Open Zeppelin contracts implementation and usage.**	Passed
21.	**Fallback function security.**	Passed

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:

- (BaseShareRewardPool) add(uint256 _allocPoint, ...), set(uint256 _pid, ...) and updateEmissionRate(uint256 _sharesPerSecond) could invoke massUpdatePools() function, that can fail due to block gas limit if the pool size is too big.
- (presaleDistributor) getTotalValues(), updateUsers() and updateAllUsers()uses the loop to iterate through users list. Them could be aborted with OUT_OF_GAS exception if there will be a long user list.

Recommendation:
Check that the arrays length is not too big.

2. add() function issue (BaseShareRewardPool)

Issue:

- If some LP token is added to the contract twice using function add, then the total amount of reward in function updatePool() will be incorrect.

Recommendation:
Add the mapping from address to bool and check that same address will not be added twice.

Notes:

- BaseShareRewardPool has deposit and withdrawal fees.

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

- presaleDistributor
  - Owner can update a single user's data.
  - Owner can manually update a single user's data with specific values.
  - Owner can update data for multiple users within a specified range.
  - Owner can update data for all users.
  - Owner can withdraw ERC20 tokens.
- BaseRate
  - Tax manager can set the tax manager address.
  - Tax manager can set the TWAP value for a specific tax tier.
  - Tax manager can set the tax rate for a specific tax tier.
  - Tax manager can specify whether an address is an LP.
  - Tax manager can enable auto-calculation of tax.
  - Tax manager can disable auto-calculation of tax.
  - Tax manager can set the oracle address for BRATE price.
  - Tax manager can set a fixed tax rate (only if auto-calculation is disabled).
  - Tax manager can exclude an address from taxation.
  - Tax manager can include an address for taxation.
  - Operator can mint new BRATE tokens.
  - Owner can withdraw ERC20 tokens.
- BaseShare
  - Tax manager can set the tax manager address.
  - Tax manager can set the TWAP value for a specific tax tier.
  - Tax manager can set the tax rate for a specific tax tier.
  - Tax manager can specify whether an address is an LP.
  - Tax manager can enable auto-calculation of tax.
  - Tax manager can disable auto-calculation of tax.
  - Tax manager can set the oracle address for BSHARE price.
  - Tax manager can set a fixed tax rate (only if auto-calculation is disabled).
  - Tax manager can exclude an address from taxation.
  - Tax manager can include an address for taxation.
  - Operator can mint new BSHARE tokens.
  - Owner can withdraw ERC20 tokens.
- BaseBond
  - Operator can mint tokens.
  - Operator can burn tokens from any address.
- BaseShareRewardPool
  - Owner can add a new liquidity pool to the reward system.
  - Owner can update the allocation points and fees for an existing pool.
  - Owner can set a gauge for a pool and deposit LP tokens into it.

    - Owner can remove the gauge associated with a pool and withdraw LP tokens back to the contract.
    - Owner can claim external rewards from a gauge and transfer them to the fee address.
    - Owner can claim and transfer external swap fees from a liquidity pool.
    - Owner can change the address where fees are sent.
    - Owner can update the percentage of fees deducted from rewards.
    - Owner can change the address where developer rewards are sent.
    - Owner can update the percentage of rewards sent to the developer address.
    - Owner can set the referral rate, determining the portion of rewards given to referrers.
    - Owner can adjust the rate at which rewards are emitted per second.
- Boardroom
    - Operator can change the operator address.
    - Operator can set the lockup periods for withdrawal and claiming rewards.
    - Operator can allocate seigniorage rewards to the Boardroom.
    - Operator can withdraw ERC20 tokens.
- Treasury
    - Operator can change the Boardroom address.
    - Operator can change the Base Oracle address.
    - Operator can change the baseRatePriceCeiling.
    - Operator can change the maximum supply expansion percentage.
    - Operator can change the supply tiers entry.
    - Operator can change the maximum expansion tiers entry.
    - Operator can change the bond depletion floor percent.
    - Operator can change the maximum supply contraction percent.
    - Operator can change the maximum debt ratio percent.
    - Operator can change the bootstrap parameters (epochs and supply expansion percent).
    - Operator can change the DAO and Dev funds addresses and shared percent.
    - Operator can change the maximum discount rate.
    - Operator can change the maximum premium rate.
    - Operator can change the discount percent.
    - Operator can change the premium threshold.
    - Operator can change the premium percent.
    - Operator can change the minting factor for paying debt.
    - Operator can change the Boardroom operator.
    - Operator can change the Boardroom lockup periods.
    - Operator can allocate seigniorage to the Boardroom.
    - Operator can withdraw ERC20 tokens.
    - Operator can change the status of addresses in the excludedFromTotalSupply list.
    - Operator can buy/redeem bonds.

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: 78.

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.