TechRate
January, 2023

SMART CONTRACTS SECURITY AUDIT REPORT

Audit Details

Audited project

Staking

Deployer address

Not deployed

Client contacts:

Staking team

Blockchain

Not provided

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 Staking to perform an audit of smart contracts:

- staking.rtf

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.**	Medium 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

1. Abuse of authority

Issue:

- Main address can call `removeStakers()` function and remove user's stakes.

Recommendation:
Do not allow anybody to access users balances.

Low Severity Issues

2. Out of gas

Issue:

- The function `removeStakers()` uses the loop to remove stakers from the list. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.

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

Notes:

- *Previous* never set.

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

- Owner can transfer ownership.
- Owner can update staking limits.
- Owner can change maxTotal, maxWallets and minimumStakeTime.
- Owner can change resetTime.
- Owner can change emergencyRate.
- Owner can enable/disable emergencyRateEnabled.
- Owner can reset the contract.
- Owner can change TOKEN and REWARD addresses.
- Owner can enable/disable open value.
- Owner can start and finish distribution.
- Owner can top up contract reward balance.
- Owner can withdraw contract ERC20 and native tokens.
- Owner can change distribution period.
- Owner can change minPeriod.

Testnet deployment

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
BCBStaking	Implementation	IDistributor, ReentrancyGuard		
└	updateStakeLimits	External ❗	🛑	onlyMain
└	updateMaxTotal	External ❗	🛑	onlyMain
└	updateMaxWallets	External ❗	🛑	onlyMain
└	updateMinStakeTime	External ❗	🛑	onlyMain
└	updateResetTime	External ❗	🛑	onlyMain
└	updateEmergencyRate	External ❗	🛑	onlyMain
└	enableEmergencyRate	External ❗	🛑	onlyMain
└	setToken	External ❗	🛑	onlyMain
└	setReward	External ❗	🛑	onlyMain
└	setOpen	External ❗	🛑	onlyMain
└	startDistribution	External ❗	🛑	initialization onlyMain
└	topUp	External ❗	🛑	onlyMain
└	setDistributionPeriod	External ❗	🛑	onlyMain
└	setDistributionParameters	External ❗	🛑	onlyMain
└	relock	External ❗	🛑	nonReentrant
└	stake	External ❗	🛑	nonReentrant
└	claimReward	External ❗	🛑	nonReentrant
└	emergencyUnstake	External ❗	🛑	nonReentrant

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Conclusion

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

Security score: 73.

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.