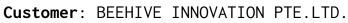


SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Date: September 27th, 2021



This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

Document

Name	Smart Contract Code Review and Security Analysis Report for BEEHIVE INNOVATION PTE.LTD.		
Approved by	Andrew Matiukhin CTO Hacken OU		
Туре	Balancer		
Platform	Ethereum / Solidity		
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review		
Repository	https://github.com/beehive-innovation/rain-protocol		
Commit	0a05312f706bfaf9458277516b0a13cba31cefcd		
Technical Documentation	YES		
TO	VEC		
JS tests	YES		
Timeline	22 JULY 2021 - 27 SEPTEMBER 2021		
Changelog	30 JULY 2021 - INITIAL AUDIT		
	06 AUGUST 2021 - Second Review		
	27 SEPTEMBER 2021 - THIRD REVIEW		

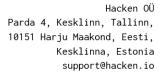




Table of contents

Introduction	
Scope	4
Executive Summary	5
Severity Definitions	6
Audit overview	7
Conclusion	7
Disclaimers	9



Introduction

Hacken OÜ (Consultant) was contracted by BEEHIVE INNOVATION PTE.LTD. (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contract and its code review conducted between July $22^{\rm nd}$, 2021 - July $30^{\rm th}$, 2021. The second code review conducted on August $6^{\rm th}$, 2021. The third code review conducted on September $27^{\rm th}$, 2021.

Scope

The scope of the project is smart contracts in the zip archive:

Repository:

https://github.com/beehive-innovation/rain-protocol

Commit:

0a05312f706bfaf9458277516b0a13cba31cefcd

Technical Documentation: Yes

JS tests: Yes Contracts:

Cooldown.sol Phased.sol

RedeemableERC20.sol

RedeemableERC20Pool.sol

SeedERC20.sol Trust.sol

We have scanned this smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item	
Code review	Reentrancy	
	Ownership Takeover	
	Timestamp Dependence	
	Gas Limit and Loops	
	DoS with (Unexpected) Throw	
	DoS with Block Gas Limit	
	 Transaction-Ordering Dependence 	
	Style guide violation	
	Costly Loop	
	ERC20 API violation	
	Unchecked external call	
	Unchecked math	
	Unsafe type inference	
	Implicit visibility level	
	Deployment Consistency	
	Repository Consistency	
	Data Consistency	



Functional	review

- Business Logics Review
- Functionality Checks
- Access Control & Authorization
- Escrow manipulation
- Token Supply manipulation
- Assets integrity
- User Balances manipulation
- Data Consistency manipulation
- Kill-Switch Mechanism
- Operation Trails & Event Generation

Executive Summary

According to the assessment, the Customer's smart contracts are well-secured.

Insecure	Poor secured	Secured	Well-secured
		You are here	

Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

As a result of the audit, security engineers found 2 low severity issues which were addressed before the second review.

After the second review security engineers found all issues were resolved.

After the third review security engineers found a new function added together with two immutable state variables. No new issues were detected.



Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution



Audit overview

■ ■ ■ Critical

No critical issues were found.

High

No high severity issues were found.

■ Medium

No medium severity issues were found.

Low

1. **Issue**: Maximum line length.

Solidity declares <u>maximum line length</u> that should be followed.

Recommendation: Please follow the solidity <u>Code Layout</u> recommendations.

Fixed before the second review

2. **Issue**: State variable that could be immutable.

State variable which value is initialized in the constructor and never changes should be declared immutable to save gas.

Fixed before the second review



Conclusion

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

As a result of the audit, security engineers found **2** low severity issues which were addressed before the second review.

After the second review security engineers found all issues were resolved.

After the third review security engineers found a new function added together with two immutable state variables. No new issues were detected.



Hacken Disclaimer

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.