EOCENE

Audit Report for Borabora V2

Document Properties

Project	Borabora V2		
Document Name	Audit Report for Borabora V2		
Document Number	Eocene-Bo-20220901-0005		
File type	Project Documentation		
Created by	Eugene	Version	1.0
Reviewed by	Arthur	Date reviewed	2022-09-01
Approved by	Arthur	Data Approved	2022-09-01
Receiver	Borabora Team	Date received	2022-09-01

Version Info

version	Description	Author(s)	Reviewed by	Date
1.0	Create report	Eugene	Arthur	2022-09-01

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, con fidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without Eocene's prior written consent.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Eocene to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Eocene's position is that each company and individual are responsible for their own due diligence and continuous security.

Eocene's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Contents

1 Summary

This report has been prepared for Borabora V2 to discover issues and vulnerabilities in the source code of the Borabora V2 project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques. Eocene examined Borabora V2's " source code " for syntactical, semantic, and logical errors with a methodology including "but not limited to":

- White box code review
- Static Analysis
- Expert Manual Review

The results of security assessments range from high to informational findings. We make the following recommendations to address these findings to ensure high levels of safety standards and industry practices:

- Use mutex and follow CEI pattern to prevent reentrancy attacks;
- Centralized privileges or roles in a protocol can be improved by decentralized mechanisms;
- Provide more comments per each function for readability;
- Add enough unit tests to cover the possible use cases;

2 Overview

2.1 Project info

Project name	Borabora V2
Platform	BSC
Language	Solidity
Codebase	https://github.com/boraboradao/BoraboraV2
Commit	3a9c8a7

2.2 Audit Scope

File	MD5
contracts/AgentRouter.sol	0b82207c9cf4ff1a3e4c132af1f15e17
contracts/Debt.sol	b77ef28a30bb48d420457e7a03c2bddb
contracts/Deployer01.sol	73db6700fb980401d278cee4d917ae2d
contracts/Deployer02.sol	b3b5c1c7f4c904857b59c2f520d19427
contracts/EventOut.sol	aa6ebf885646fe550192aa76a542d267
contracts/ExecutorManager.sol	82dfd8d31b63d9cd617cd6151ac73412
contracts/Pool.sol	a2706853cb841013afd2d7de4aa68888
contracts/PoolFactory.sol	9aebc5b4f8af3deb624b29b8ebc5e922
contracts/PoolSetting.sol	670d34a08a3127fd44b76c5311a4d303
contracts/Router.sol	937c4e6e3c480fa672eee9317a02a4ec
contracts/SManager.sol	c30670895d93b65dab268a9f89d57787
contracts/SystemSettings.sol	9883e099401a651e5dba2c1325d2df86

2.3 Findings

The risk distribution table is as follows:

Level	Number
Critical	0
High	1
Medium	0

Low	1
Informational	0

The key findings are as follows:

ID	Severity	Title	Category	Status
1	Low	Missing Zero Address Validation	Volatile Code	Acknowledged
2	High	Centralization Risks In SystemSettings.sol	Centralization /Privilege	Acknowledged

3 Detailed Results

3.1 Missing Zero Address Validation

ID	Category	Severity	Location	Status
1	Volatile Code	Low	contracts/SManager.sol:24	Acknowledged

Description

Addresses should be checked before assignment or external calls to make sure they are not zero addresses.

contracts/SManager.sol, line 24, function setEventOut ():

```
    function setEventOut(address eventOutAddress) public onlyOwner {
        _eventOut = eventOutAddress;
    }
```

Recommendation

We advise adding a zero-check for the passed-in address value to prevent unexpected errors.

Status

Borabora team acknowledged this finding.

3.2 Centralization Risks In SystemSettings.sol

ID	Category	Severity	Location	Status
2	Centralization /Privilege	High	contracts/SystemSettings.sol:354,360,366,372	Acknowledged

Description

In the contract SystemSettingsthe role owner has authority over the functions shown in the diagram below. Any compromise to the owner account may allow the hacker to take advantage of this authority.

- function setProtocolFee, to set protocol's fee;
- function setLiqProtocolFee, to set liqprotocol's fee;
- function setMarginRatio, to set margin ratio;
- function setClosingFee, to set closing fee;

Recommendation

We recommend the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism.

Status

Borabora team acknowledged this finding.

4 About us

Eocene is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in- class security, all whilst realizing our overarching vision: provable trust for all throughout all facets of blockchain.