Smart Contract Audit Report

AIBRA

2023-01-27

BiPOLE Labs
Email: team@bipole.org

CONTENTS

Summary

This report was created for AIBRA in order to identify bugs and vulnerabilities in the contract dependencies that were not a part of an officially recognized library as well as project's source code.
Static Analysis and Manual Review approaches have been used to conduct a thorough examination.

The following factors receive extra consideration during the auditing process:
testing the smart contracts for both typical and unusual attack vectors.

* evaluating the codebase to make sure it adheres to the most recent industry standards and best practices.
* ensuring that contract logic adheres to the client's requirements and goals.
* Cross-referencing contract design and execution with related smart contracts created by top industry producers.
* Complete manual line-by-line review of the complete codebase by specialists in the field.

Findings from the security evaluation ranged from important to informative. To guarantee a high degree of security standards and industry practices, we advise taking action on these results. We offer suggestions that, from a security standpoint, could benefit the project.:

* Improve general coding techniques for improved source code organization;
* Include sufficient unit tests to cover all potential use cases.;
* For improved readability, include extra comments for each function, especially for contracts that are publicly verifiable;

* Once the protocol is active, provide additional transparency on privileged operations.

Project Introduction

AIBRA is a decentralized application that transforms the recruitment. AIBRA decentralizes the typical recruitment paradigm creating an ecosystem where recruiters, job seekers and recruitment agencies are united thereby providing more value for the future of recruitment.

Audit Scope

ID	Filename	SHA256 CHECK SUM
FIL-1	https://brisescan.com/address/0x9F7Bb6E8386ac9ad5e944d66fBa80F3F7231FA94	7a4ae0b8db044e5ef86e58df8b34b39795b2c46ecbd1e68e0c104a4478f3227d

Audit Methodology

Step	Operations	Description
1	Backgroud	Reading the descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated Testing	Automated detection tools will be mainly used to scan the source code to find common potential vulnerabilities
3	Manual Review	The code will be thoroughly reviewed line by line by engineers to find potential vulnerabilities
4	Logic Proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the white paper information.
5	Test Cases	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization	Items Review the project from the aspects of maintainability, security and operability according to the application scenarios, call methods and the latest research results.

Risk Levels

Risk Level	Issue Description
Critical	Fatal risks and hazards that need to fixed immediately.
Major	Some high risks and hazards that will lead to related problems that must be solved.
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed.
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being.
Informational	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution.

Vulnerability Summary

ID	Title	Category	Severity	Status
RISK-01	Unused return	Improvement	Informational	Acknowledged
RISK-02	State variables that could be declared constant	Improvement	Informational	Acknowledged
RISK-03	Centralization Risk	Improvement	Informational	Acknowledged
RISK-04	Redundant Statements	Improvement	Informational	Acknowledged

RISK-01 | Unused return

Category	Severity	Location	Status
Improvement	Informational	FIL-1:addLiquidity(uint256 tokenAmount, uint256 ethAmount) #758-771	Acknowledged

Description:

The function ignores return value by uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp).

Recommendation:

Ensure that all the return values of the function calls are used.

RISK-02 | State variables that could be declared constant

Category	Severity	Location	Status
Improvement	Informational	FIL-1: #404-406	Acknowledged

Description:

Constant state variables should be declared constant to save gas.

Recommendation:

Add the constant attributes to state variables _decimals■_name■_symbol that never change.

RISK-03 | Centralization Risk

Category	Severity	Location	Status
Improvement	Informational	FIL-1:onlyOwner #160	Acknowledged

Description:

Risk due to privilege control or key contract operations controlled by a single private key. Once the private key is lost, the key management functions of the contract will not be available, while the private key leakage will cause more serious financial risks.

Recommendation:

It is generally recommended that contract management functions use multi-signature or timelock for external calls, while project owners are required to establish instant alarm system to deal with unpredictable permission control

RISK-04 | Redundant Statements

Category	Severity	Location	Status
Improvement	Informational	FIL-1:_msgData #15	Acknowledged

Description:

Detect the usage of redundant statements that have no effect.

Recommendation:

Remove redundant statements if they congest code but offer no value.

Disclaimer

1 Only the audit types mentioned in the final report published are the subject of this audit report. This audit does not cover any other undiscovered security flaws, and we disclaim all liability for them. ii. A report on an audit may only be based on an attack or vulnerability that existed or had already taken place at the time the report was issued.br/>

2 We are not liable for any new attacks or vulnerabilities that may be launched or arise in the future, and we are unable to predict their likely effects on the security posture of our projects.

3 Prior to the publication of the audit report, the Project Party gave us with certain papers and materials, including but not limited to contract codes, on which we based our security audit analysis and other audit report components. Such documents and materials shall not be false, inaccurate, uninformative, changed, deleted, or concealed, and if the Project Party's documents and materials are false, inaccurate, uninformative, changed, deleted, or concealed, or if the Project Party's documents and materials are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if the Project Party's documents and materials. We shall not be responsible for any loss or negative consequences resulting from any discrepancy between the reflected and actual conditions if the records and information provided by the Project Party are false, inaccurate, uninformative, altered, deleted, or concealed, or if changes are made to such documents and information after the audit report is issued.

4 The Project Parties are aware that our audit report depends on currently available technology and is based on information and documents supplied by the Project Parties. However, there is a chance that our audit report might not fully identify all hazards due to the technical limits of any business. The project development team and any other interested parties are urged to carry out further testing and audits of the project by our audit team.

5 The project owner guarantees that the project is legitimate, compliant, and does not break any laws in the country where the audit or testing is being performed. The audit report is just for the project owner's reference; it should not be used for investment, tax, legal, regulatory, or advisory reasons of any sort, and we will not be held responsible for the contents,

method of acquisition, use, or any services or resources included in the audit report. Without our prior written consent, the Project Party shall not make any references to, quotations from, displays of, or transmissions of the Audit Report, in whole or in part, to any third party. Any damage or liabilities caused by that location is the responsibility of the project party. We disclaim all liability for any reliance or use of the audit report, regardless of its intended use.

6 The compiler of the contract or any other topics outside of the Smart Contract's programming language are not covered in this audit report. The project party is solely responsible for the risk and liability of the audited Smart Contract resulting from references to off-chain data or resources.

About BiPOLE Labs

Through the provision of market-leading smart contract auditing services, BiPOLE Labs, a leading blockchain security company, aims to conduct security and vulnerability research on current blockchain ecosystems. Please contact us for more information at (www.bipole.org) or Email (team@bipole.org)