RAPID LABS

SMART CONTRACT SECURITY AUDIT

Final report

Plan: Simple

Aerarium Fi

August 2022

TABLE OF CONTENTS

INTRODUCTION

The report has been prepared for Aerarium Fi.
A Treasury-as-a-Service protocol on the Metis blockchain. Users can buy a part of the protocol by obtaining a so-called fractal. Which also brings them real-time payouts.

Name	Aerarium Fi
Audit date	2022-08-10 - 2022-08-16
Language	Solidity
Platform	Metis

ANALYZED CONTRACTS

Name	Address
IBaseV1Router.sol	
Aerarium.sol	

AUDIT PROCESS

Our audit structure consists of two stages:

Auto-analysis

- Our automated tools allow us to scan smart contract code and find potential issues
- We hand pick and verify all the issues found by the tools

Expert audit

- Manual analysis of potential issues and vulnerabilities

- Contract code is reviewed thoroughly

KNOWN ISSUES CHECKED

Title	Result
Unencrypted Private Data On-Chain	✓ passed
Code With No Effects	✓ passed
Message call with hardcoded gas amount	✓ passed
Typographical Error	✓ passed
DoS With Block Gas Limit	✓ passed
Presence of unused variables	✓ passed
Incorrect Inheritance Order	✓ passed
Requirement Violation	✓ passed
Weak Sources of Randomness from Chain Attributes	✓ passed
Shadowing State Variables	✓ passed
Incorrect Constructor Name	✓ passed

Block values as a proxy for time	✓	passed
Authorization through tx.origin	✓	passed
DoS with Failed Call	✓	passed
Delegatecall to Untrusted Callee	✓	passed
Use of Deprecated Solidity Functions	✓	passed
Assert Violation	✓	passed
State Variable Default Visibility	✓	passed
Reentrancy	✕	failed
Unprotected SELFDESTRUCT Instruction	✓	passed
Unprotected Ether Withdrawal	✓	passed
Unchecked Call Return Value	✓	passed
Floating Pragma	✓	passed
Outdated Compiler Version	✓	passed
Integer Overflow and Underflow	✓	passed
Function Default Visibility	✓	passed

ISSUE CLASSIFICATION

High risk	Issues leading to assets theft, locking or any other loss of assets or leading to contract malfunctioning.
Medium risk	Issues that can trigger a contract failure of malfunctioning.
Low risk	Issues that do now affect contract functionality. For example, unoptimised gas usage, outdated or unused code, code style violations, etc.

ISSUES

High risk issues

No issues were found

Medium risk issues

No issues were found

Low risk issues

1. Tokens are sent to an unknown user (IBaseV1Router.sol)

On L792, the called function has an unclear effect that potentially can be unsafe.

Recommendation: It's preferred to only call the function with a clear action.

2. Reentrancy vulnerability (Aerarium.sol)

Certain state variables can change after an external call. This can be the cause of a reentrancy attack.

Recommendation: State variables should be changed before external calls.

3. The stack is too deep (Aerarium.sol)

The EVM stack has 16 slots, which isn't always enough for all of the local and return variables, as well as parameters. A big number of declared variables in the contract fills the stack up. It's possible that performance or safety issues might be caused by this.

Recommendation: The code should be broken into parts by using structures.

CONCLUSION

Aerarium Fi IBaseV1Router.sol, Aerarium.sol contracts were audited. 3 low risk issues were found.

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, 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 RapidLabs 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 RapidLabs 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.

RAPID LABS

YOUR PROJECT SECURED

RL@RAPIDLABS.FINANCE

RAPIDLABS.FINANCE