Overview

Project Summary

Name	Cygnus Finance - B2Vault
Platform	Bsquared Network
Language	Solidity
Repository	https://github.com/arks-labs/b2vault
Audit Range	See Appendix 1

Project Dashboard

Application Summary

Name	Cygnus Finance - B2Vault
Version	1.0
Type	Solidity
Dates	Sep 05 2024
Logs	Sep 03 2024; Sep 05 2024

Vulnerability Summary

High	0
Medium	0
Low	1
Informational	0
Total	1

Contact

E-mail: support@trustax.io

Risk Level Description

High	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for clients' reputations or serious financial implications for clients and users.
Medium	The issue puts a subset of users' sensitive information at risk, would be detrimental to the client's reputation if exploited, or is reasonably likely to lead to a moderate financial impact.
Low	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
Informational	The issue does not pose an immediate risk, but is relevant to security best practices or defense in depth.

Content

Introduction

1.1 About Trustax

At Trustax Security, we are in the business of trust.

We are dedicated to tackling the toughest security challenges facing the industry today. By building foundational trust in technology and infrastructure through security, we help clients to lead their respective industries and unlock their full Web3 potential.

Our team of security experts employ industry-leading proof-of-concept (PoC) methodology for demonstrating smart contract vulnerabilities, coupled with advanced red teaming capabilities and a stereoscopic vulnerability detection service, to deliver comprehensive security assessments that allow clients to stay ahead of the curve.

1.2 Audit Breakdown

The objective was to evaluate the repository for security-related issues, code quality, and adherence to specifications and best practices. Possible issues we looked for included (but are not limited to):

- Risky external calls
- Integer overflow/underflow
- Transaction-ordering dependence
- Timestamp dependence
- Access control
- Call stack limits and mishandled exceptions
- Number rounding errors
- Centralization of power
- Logical oversights and denial of service
- Business logic specification
- Code clones, functionality duplication

1.3 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release and does not give any warranties on finding all possible security issues with the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues.

Findings

2.1 Summary of Findings

ID	Title	Severity	Category	Status
1	Zero Amount	Low	Business Logic	Resolved

2.2 Notable Findings

Significant flaws that impact system confidentiality, integrity, or availability are listed below.

1. Zero Amount	
Severity	Low
Category	Business Logic
Target	-Vault.sol

Description

When the amount is 0, it should revert.

Recommendation

```
require(amount>0,"Zero amount");
```

Status

This issue has been resolved by the team with commit bd6c7ff.

Appendix

Appendix 1 - Files in Scope

This audit covered the following files in commit 71cf514 of the B2Vault repo:

File	SHA-1 hash
contracts/Vault.sol	94cc29f06c50f81204bdcfec9769878c39930b29