



Security Review For Byzantine Finance



Collaborative Audit Prepared For: **Byzantine Finance**
Lead Security Expert(s): [vinica_boy](#)
Date Audited: **October 15 - October 17, 2025**

Introduction

Byzantine vault-v2 is a new way to put company cash to work. Same safety, same compliance, just with returns that actually make CFOs smile - for the first time.

Byzantine offers a low-risk, institutional-grade digital credit product built for corporate cash. It combines the safety of traditional finance with the efficiency and returns of digital markets.

Scope

Repository: Byzantine-Finance/debt-fund-vault-v2

Audited Commit: 5e9135b94206d5610fca4cd45705126df1201a63

Final Commit: 3654b06f2f64d2133d85e4ccc4fd215ef50ca64d

Files:

- src/gate/GateWhitelist.sol

Final Commit Hash

3654b06f2f64d2133d85e4ccc4fd215ef50ca64d

Findings

Each issue has an assigned severity:

- High issues are directly exploitable security vulnerabilities that need to be fixed.
- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
- Low/Info issues are non-exploitable, informational findings that do not pose a security risk or impact the system's integrity. These issues are typically cosmetic or related to compliance requirements, and are not considered a priority for remediation.

Issues Found

High	Medium	Low/Info
0	0	1

Issues Not Fixed and Not Acknowledged

High	Medium	Low/Info
0	0	0

Issue L-1: Lost granularity of different gates when combined in a single contract [RESOLVED]

Source:

<https://github.com/sherlock-audit/2025-10-byzantine-finance-oct-15th/issues/2>

Summary

Morpho V2 Vaults provide ability to implement four different gates based on the exact needs of the vault - `receiveSharesGate`, `sendSharesGate`, `receiveAssetsGate`, `sendAssetsGate`. By having a single gate contract that has a general whitelisting, this granularity is lost as an address can only be allowed/disallowed for all actions.

Vulnerability Detail

The `GateWhitelist` contract has a single `whitelisted` mapping that is used for all related checks thus it is not possible to set an address being allowed for one action while not being allowed for another action.

Impact

Inability to cover some potential use cases.

Code Snippet

<https://github.com/sherlock-audit/2025-10-byzantine-finance-oct-15th/blob/182527794feaa44fdeee7cb76ad8b9bed6e24dc5/debt-fund-vault-v2/src/gate/GateWhitelist.sol#L113C5-L116C6>

Tool Used

Manual Review

Recommendation

Consider splitting the logic per each gate type into a separate contract.

Discussion

`spdimov`

Contracts were split into 4 separated child contract per each gate.

Additional changes:

- parent contract inherits from `Ownable2Step` and overrides `renounceOwnership()` function to always revert.
- `setWhitelisted()` now reverts on a no-op call (setting whitelisted value to the already set value).

Disclaimers

Sherlock does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.