YO Protocol Security Audit

Report Version 1.0

August 20, 2025

Conducted by **Aether Labs**

Table of Contents

1 About Aether

Aether is an industry-leading smart contract security company. Having conducted over 100+ security assessments protecting over $3B in TVL, we deliver high-signal security reviews to emerging and established DeFi protocols. For security audit inquiries, visit aethersecurity.io.

2 Disclaimer

Audits are a time-, resource-, and expertise-bound effort where trained experts evaluate smart contracts using a combination of automated and manual techniques to identify as many vulnerabilities as possible. Audits can reveal the presence of vulnerabilities, but cannot guarantee their absence.

3 Risk classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	High	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

3.1 Impact

- **High** - leads to a significant loss of assets in the protocol or significantly harms a group of users.
- **Medium** - involves a small loss of funds or affects a core functionality of the protocol.
- **Low** - encompasses any unexpected behavior that is non-critical.

3.2 Likelihood

- **High** - a direct attack vector; the cost is relatively low compared to the potential loss of funds.
- **Medium** - only a conditionally incentivized attack vector, with a moderate likelihood.
- **Low** - involves too many or unlikely assumptions; offers little to no incentive.

3.3 Actions required by severity level

- **High** - client **must** fix the issue.
- **Medium** - client **should** fix the issue.
- **Low** - client **could** fix the issue.

4 Findings

4.1 Medium

4.1.1 An attacker can manipulate users' redeem parameters via front-running

Severity: Medium

Description: When redeeming through the gateway, the shares are taken from the passed receiver parameter which is not always the msg.sender.

A user could grant allowance to the gateway and then have their redeem transaction (if separate) be frontrun by an attacker who changes other parameters such as shares, minAssetsOut, and partnerId.

Recommendation: Consider using the msg.sender instead of receiver on line 91 or implement a signature verification logic.

Resolution: Resolved.

4.2 Informational

4.2.1 Non-critical issues and suggestions

Severity: Informational

Description: The contracts contain one or more non-critical issues. In an effort to keep the report size reasonable, we enumerate these below:

1. Instant redeem is assumed when the returned value is > 0. However, a zero-amount redeem is also a possible edge case which should be considered.
2. getShareAllowance does not check whether the passed vault is whitelisted.
3. .redeem could be used instead of .requestRedeem
4. The newly implemented redeem method does not have standard EIP4626 behaviour.

Recommendation: Consider fixing the above non-critical issues and suggestions.

Resolution: Partially resolved (2).