Ondo RWA

Security Review

Cantina Solo review by:
Desmond Ho, Lead Security Researcher

December 6, 2025

Contents

1 Introduction

1.1 About Cantina

Cantina is a security services marketplace that connects top security researchers and solutions with clients. Learn more at cantina.xyz

1.2 Disclaimer

A security review is a detailed evaluation of the security posture of the code at a particular moment based on the information available at the time of the review. While the review endeavors to identify and disclose all potential security issues, it cannot guarantee that every vulnerability will be detected or that the code will be entirely secure against all possible attacks. The assessment is conducted based on the specific commit and version of the code provided. Any subsequent modifications to the code may introduce new vulnerabilities that were absent during the initial review. Therefore, any changes made to the code require a new security review to ensure that the code remains secure. Please be advised that a security review is not a replacement for continuous security measures such as penetration testing, vulnerability scanning, and regular code reviews.

1.3 Risk assessment

Severity level	Impact: High	Impact: Medium	Impact: Low
Likelihood: high	Critical	High	Medium
Likelihood: medium	High	Medium	Low
Likelihood: low	Medium	Low	Low

1.3.1 Severity Classification

The severity of security issues found during the security review is categorized based on the above table. Critical findings have a high likelihood of being exploited and must be addressed immediately. High findings are almost certain to occur, easy to perform, or not easy but highly incentivized thus must be fixed as soon as possible.

Medium findings are conditionally possible or incentivized but are still relatively likely to occur and should be addressed. Low findings are a rare combination of circumstances to exploit, or offer little to no incentive to exploit but are recommended to be addressed.

Lastly, some findings might represent objective improvements that should be addressed but do not impact the project's overall security (Gas and Informational findings).

2 Security Review Summary

Ondo's mission is to make institutional-grade financial products and services available to everyone.

From Dec 2nd to Dec 3rd the security researchers conducted a review of rwa-internal on commit hash 0e8bc196. A total of **5** issues were identified:

Issues Found

Severity	Count	Fixed	Acknowledged
Critical Risk	0	0	0
High Risk	0	0	0
Medium Risk	0	0	0
Low Risk	0	0	0
Gas Optimizations	4	4	0
Informational	1	1	0
Total	**5**	**5**	**0**

2.1 Scope

The security review had the following components in scope for rwa-internal on commit hash 0e8bc196:

```
contracts
├── globalMarkets
│   └── tokenManager
│       └── IGMTokenManager.sol
└── limit-order
    ├── GMTokenLimitOrder.sol
    └── IGMTokenLimitOrderErrors.sol
```

3 Findings

3.1 Gas Optimization

3.1.1 Redundant condition checked in `isOrderActive()`

Severity: Gas Optimization

Context: GMTokenLimitOrder.sol#L527

Description: The referenced condition is redundant because of the checks in place that results in a couple of state invariants:

- `OrderStatus.ACTIVE` (& `OrderStatus.CANCELLED`) ⇒ `order.filledQuantity < order.totalQuantity`.
- `OrderStatus.EXECUTED` ⇔ `order.filledQuantity == order.totalQuantity`.

As such, checking `order.status == OrderStatus.ACTIVE` will suffice in asserting the latter.

Recommendation: Remove the referenced condition.

Ondo Finance: Fixed in commit 0ce9b329.

Cantina Managed: Fix verified.

3.1.2 Cheaper conditional check for `isOrderFullyFilled()`

Severity: Gas Optimization

Context: GMTokenLimitOrder.sol#L551

Description/Recommendation: A cheaper check is `order.status == OrderStatus.EXECUTED`.

Ondo Finance: Fixed in commit 53e5cefc.

Cantina Managed: Fix verified.

3.1.3 `executorUserId` is checked per iteration for batch calls

Severity: Gas Optimization

Context: GMTokenLimitOrder.sol#L421-L425

Description/Recommendation: The compliance check on the executor should be refactored into a separate function because it's called every iteration for batch orders.

Ondo Finance: Fixed in commit ed9a4b92.

Cantina Managed: Fix verified.

3.1.4 `msg.sender` emission in `OrderCancelled` is redundant

Severity: Gas Optimization

Context: GMTokenLimitOrder.sol#L270

Description/Recommendation: Orders can only be cancelled by its creators, i.e. `order.user`, so emitting it in the `OrderCancelled` is redundant.

Ondo Finance: Fixed in PR 511. Another function for cancelling orders by authorized addresses was added, so the address emitted here becomes relevant.

Cantina Managed: Fix verified.

3.2 Informational

3.2.1 User may be removed from registry between order creation and execution

Severity: Informational

Context: GMTokenLimitOrder.sol#L226-L228

Description: A user may be removed from registry some time between order creation and execution.

Recommendation: Consider checking that the user is still registered upon order execution.

Ondo Finance: Fixed in PR 510.

Cantina Managed: Fix verified.