Security Review

Cantina Managed

SKY: L2 PAS DEPLOYER

Cantina Managed review by:
Christoph Michel, Lead Security Researcher
M4rio.eth, Lead Security Researcher

CANTINA

October 26, 2026

Contents

1 Introduction **2**
- 1.1 About Cantina . . . 2
- 1.2 Disclaimer . . . 2
- 1.3 Risk assessment . . . 2
  - 1.3.1 Severity Classification . . . 2

2 Security Review Summary **3**
- 2.1 Scope . . . 3

3 Findings **4**
- 3.1 Informational . . . 4
  - 3.1.1 Full deployment config may exceed the initcode size limit . . . 4

1 Introduction

1.1 About Cantina

Cantina is a security platform that pairs a world-class network of security researchers with agentic AI to help teams building onchain find and fix real risk. Through managed reviews, competitions, and bounties, Cantina secures protocols before vulnerabilities can be exploited.
Learn more at cantina.security

1.2 Disclaimer

Cantina Managed provides 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 Cantina Managed 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 the Cantina Managed 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

On Oct 1st the Cantina team conducted a review of pas on commit hash 5263f260. The team identified **1** issue:

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	0	0	0
Informational	1	0	1
Total	**1**	**0**	**1**

The Cantina Managed team reviewed Sky's pas holistically on commit hash 5263f260 and concluded that all findings were addressed and no new vulnerabilities were identified.

2.1 Scope

The security review had the following components in scope for pas on commit hash 5263f260:

```
deploy/L2PASDeployer.sol
```

3 Findings

3.1 Informational

3.1.1 Full deployment config may exceed the initcode size limit

Severity: Informational.

Context: L2PASDeployer.sol#L63.

Description: Deployment and configuration is performed as part of the `L2PASDeployer` contract's constructor. It receives the full configuration through its constructor, so the creation code and encoded configuration must fit within the EIP-3860 initcode limit of 49,152 bytes.

The existing size test uses arrays of length one; for example, a full configuration with 120 rate-limit entries exceeds the limit and cannot be deployed.

Recommendation: Check the final deployment initcode size against the limit before deployment. If the required configuration does not fit, deploy with a smaller configuration and submit the remaining rate-limit instructions or other settings through governance as a second update.

Sky: Acknowledged.

Cantina Managed: Acknowledged.