Security Review

Cantina Managed

COINBASE: TOKENIZE PR 105

Cantina Managed review by:
Sujith Somraaj, Lead Security Researcher
0xhuy0512, Security Researcher

CANTINA

August 10, 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 Global `mintId` namespace allows cross-token key consumption . . . 4
  - 3.1.2 Empty mint IDs are accepted . . . 4
  - 3.1.3 No view function is available to query consumed mint IDs . . . 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

Base is a secure, low-cost, builder-friendly Ethereum L2 built to bring the next billion users onchain.

From Aug 10th to Aug 10th the Cantina team conducted a review of tokenize on commit hash 5d6800d9. The team identified a total of **3** issues:

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	3	1	2
Total	**3**	**1**	**2**

The Cantina Managed team reviewed Coinbase's tokenize holistically on commit hash 4d9b3b7a 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 tokenize on commit hash 5d6800d9:

```
src/TokenSupplyManager.sol
```

3 Findings

3.1 Informational

3.1.1 Global `mintId` namespace allows cross-token key consumption

Severity: Informational.

Context: TokenSupplyManager.sol#L402.

Description: `usedCreateIds` is shared globally across every registered token and caller. A whitelisted caller can consume an ID that another token's caller intended to use. This is informational because `create()` is only exposed to trusted whitelisted callers.

Recommendation: Document the global trust assumption, if it's intended.

Coinbase: Acknowledged.

Cantina Managed: Acknowledged.

3.1.2 Empty mint IDs are accepted

Severity: Informational.

Context: TokenSupplyManager.sol#L402.

Description: `create()` does not validate that `mintId` contains any data. The first call using `""` as `mintId` succeeds and consumes the global empty-string key.

Recommendation: Reject empty IDs with `if (bytes(mintId).length == 0) revert InvalidMintId();`

Coinbase: Acknowledged. There is no on-chain schema so these values will be opaque to the contract itself.

Cantina Managed: Acknowledged.

3.1.3 No view function is available to query consumed mint IDs

Severity: Informational.

Context: TokenSupplyManager.sol#L242.

Description: `usedCreateIds` is stored privately without an external getter. Integrations must scan `Created` logs or attempt a mint and handle `DuplicateCreateId`.

Recommendation: Consider adding a view function: `isCreateIdUsed(string calldata mintId) external view returns (bool)`.

Coinbase: Fixed in commit d809323.

Cantina Managed: Verified fix.