Security Review

Cantina Managed

SKY: CCTPV2

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

CANTINA

October 28, 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 Mainnet deployment inputs still use CCTP V1 . . . 4
  - 3.1.2 A 100% maximum fee rate disables CCTP transfers . . . 4
  - 3.1.3 Inconsistent domain-configuration revert prefix . . . 4
  - 3.1.4 CCTP V1 and V2 interfaces reuse the same names . . . 5

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

From Oct 7th to Oct 10th the Cantina team conducted a review of spark-alm-controller on commit hash 899a8fd5. The team identified a total of **4** 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	4	4	0
Total	**4**	**4**	**0**

The Cantina Managed team reviewed Sky's spark-alm-controller holistically on commit hash 9c7dffe3 (tag v1.11.0) 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 spark-alm-controller on commit hash 899a8fd5:

```
src/MainnetController.sol
src/libraries/CCTPLib.sol
```

3 Findings

3.1 Informational

3.1.1 Mainnet deployment inputs still use CCTP V1

Severity: Informational.

Context: `mainnet-production.json#L5`, `mainnet-staging.json#L10`.

Description:

Both Mainnet deployment inputs still configure the CCTP V1 `TokenMessenger` address. The upgraded controller calls the CCTP V2 `depositForBurn` interface, which V1 does not implement, so CCTP transfers deployed with either configuration will revert. These inputs must be updated before deployment.

Recommendation:

Configure both inputs with the CCTP V2 `TokenMessenger` address, `0x28b5a0e9C621a5BadaA536219b3a228C8168cf5d`. The address registry already distinguishes the V2 and V1 addresses.

Sky: Fixed in PR 264.

Cantina Managed: Fix verified.

3.1.2 A 100% maximum fee rate disables CCTP transfers

Severity: Informational.

Context: `MainnetController.sol#L256-L259`, `CCTPLib.sol#L96-L98`.

Description:

`setCCTPMaxFeeRate` accepts `10_000` bps (100%). At this rate, each burn calculates `maxFee == amount`, but CCTP V2 requires `maxFee < amount`. All positive outbound CCTP transfers therefore revert until an administrator lowers the rate.

Recommendation:

Require `maxFeeRate < 10_000` instead of `maxFeeRate <= 10_000`, and update the boundary test to expect a revert at `10_000`.

Sky: Fixed in PR 264.

Cantina Managed: Fix verified.

3.1.3 Inconsistent domain-configuration revert prefix

Severity: Informational.

Context: `CCTPLib.sol#L85-L87`.

Description:

The unconfigured-domain check now reverts with `CCTPLib/domain-not-configured`, replacing the previous `MC/domain-not-configured` string. This departs from the existing controller error convention and unnecessarily changes the error returned to callers.

Recommendation:

Keep the existing `MC/domain-not-configured` revert string.

Sky: Fixed in PR 264.

Cantina Managed: Fix verified.

3.1.4 CCTP V1 and V2 interfaces reuse the same names

Severity: Informational.

Context: `CCTPLib.sol#L9-L29`, `CCTPInterfaces.sol#L4-L19`.

Description:

The new V2 interface reuses the name `ICCTPLike`, while the existing interface still represents V1 and is used by `ForeignController`. Their `depositForBurn` signatures and `localMinter` return types differ. Importing both without aliases causes a naming conflict, and the unversioned names make it easy to select the wrong ABI. `ICCTPTokenMinterLike` is also defined in both files.

Recommendation:

Rename the new messenger interface to `ICCTPv2Like`. Share the identical minter interface or give its new definition a versioned name.

Sky: Fixed in PR 264.

Cantina Managed: Fix verified.