CANTINA

Sky: Spark ALM Controller

Security Review

Cantina Managed review by:

Christoph Michel, Lead Security Researcher
Mario.eth, Lead Security Researcher

September 11, 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

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

Sky Protocol is a decentralised protocol developed around the USDS stablecoin.

From Aug 26th to Sep 1st the Cantina team conducted a review of spark-alm-controller on commit hash cc8b6e30. The team identified a total of **2** issues:

Issues Found

Severity	Count	Fixed	Acknowledged
Critical Risk	0	0	0
High Risk	0	0	0
Medium Risk	0	0	0
Low Risk	1	1	0
Gas Optimizations	0	0	0
Informational	1	1	0
Total	**2**	**2**	**0**

The Cantina Managed team reviewed Sky's `spark-alm-controller`'s holistically on commit hash 8d06c0df (tag v1.7.0), concluding that all findings were addressed and no new vulnerabilities were identified.

3 Findings

3.1 Low Risk

3.1.1 Malicious relayer could `take` spark vault assets and `deposit` them back

Severity: Low Risk

Context: MainnetController.sol#L888-L897

Description: For Spark Vaults V2, the `taker` (the ALM proxy) can take out the vault's assets (without requiring the burning shares). An issue arises if the `taker` `deposit`s this amount again into the vault, receiving shares. The `totalAssets()` function will track a wrong value.

Recommendation: Ensure that whenever the `("LIMIT_SPARK_VAULT_TAKE", address(sparkVault))` rate limit is set, no ERC4626 deposits to the spark vault are possible, meaning, `("LIMIT_4626_DEPOSIT", address(sparkVault))` should **not** be set. In addition, `("LIMIT_ASSET_TRANSFER", sparkVault.asset(), sparkVault)` must be set to be able to repay the taken assets.

Sky: Fixed in PR 34.

Cantina Managed: This has been addressed in the `spark-vaults` code itself by disabling `deposit`/`mint` for the `TAKER` role. Verified.

3.2 Informational

3.2.1 The `superstateRedemption` and artifacts can be removed

Severity: Informational

Context: MainnetController.sol#L60-L64, MainnetController.sol#L141-L141

Description: The Superstate redemption function was removed from the `MainController`, the rest of the artifacts will not be needed anymore.

Recommendation: Consider removing any artifact that were left.

Sky: Fixed in PR 146.

Cantina Managed: Verified.