CANTINA

Sky: Grove ALM Controller

Security Review

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

August 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	Description
Critical	*Must* fix as soon as possible (if already deployed).
High	Leads to a loss of a significant portion (>10%) of assets in the protocol, or significant harm to a majority of users.
Medium	Global losses <10% or losses to only a subset of users, but still unacceptable.
Low	Losses will be annoying but bearable. Applies to things like griefing attacks that can be easily repaired or even gas inefficiencies.
Gas Optimization	Suggestions around gas saving practices.
Informational	Suggestions around best practices or readability.

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 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 Jul 28th to Aug 8th the Cantina team conducted a review of grove-alm-controller on commit hash 1e12d824. The team identified a total of **3** issues in the following risk categories:

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	3	0
Total	**3**	**3**	**0**

The Cantina Managed team reviewed Sky's `grove-alm-controller` holistically on commit hash 1658e203 and concluded that all the issues were addressed and no new vulnerabilities were identified.

3 Findings

3.1 Informational

3.1.1 Relayer can choose `remoteExtraGasLimit` for `transferSharesCentrifuge`

Severity: Informational

Context: MainnetController.sol#L403

Description: The `transferSharesCentrifuge` allows the relayer to specify a `uint128 remoteExtraGasLimit` parameter. However, this parameter is currently not used in Centrifuge V3 (both cases of `MessageDispatcher.sendExecuteTransferShares` end up ignoring it).

Recommendation: Consider removing the parameter from the `transferSharesCentrifuge` function arguments and hardcode it to `0` for the `crosschainTransferShares` Centrifuge V3 call. To avoid any future complications with a malicious relayer specifying a high gas limit and potentially locking up funds.

Sky: Fixed in commit 96a8986b following the recommendations.

Cantina Managed: Fix verified.

3.1.2 Minor Issues

Severity: Informational

Context: *(See each case below)*

Description:

1. ForeignController.sol#L509: Wrong message prefix, should be `ForeignController/centrifuge-id-not-configured`
2. ForeignController.sol#L20, MainnetController.sol#L18: Consider importing just the necessary interfaces from `CentrifugeInterfaces` same as we do for the other import, e.g `import { ICCTPLike } from "./interfaces/CCTPInterfaces.sol";` In this way we can just clean the `CentrifugeInterfaces` and keep only the necessary functions/contracts. If any of the functions are needed for testing, consider creating a more extended version of this interface file just for testing.
3. CentrifugeInterfaces.sol#L6-L31: The `ICentrifugeToken` and `ICentrifugeV3VaultLike` are both used for Centrifuge's V3 vaults (not the vault's share token). Consider merging the interfaces into `ICentrifugeV3VaultLike`.

Recommendation: Consider fixing the aforementioned issues.

Sky: Fixed 1 and 2 in commit 967da971 and 3 in commit 4dc999e0.

Cantina Managed: Fix verified.

3.1.3 Deployment scripts don't set Centrifuge bridge recipients

Severity: Informational

Context: deploy/MainnetControllerInit.sol#L161-L171, deploy/ForeignControllerInit.sol#L152-L160

Description: The init deployment scripts set the controller's `mintRecipients` for CCTP bridge transfers and `layerZeroRecipients` for LayerZero bridges. However, the `centrifugeRecipients` for the similar Centrifuge V3 bridge transfers are not set.

Recommendation: Consider initializing the Centrifuge recipients by calling `setCentrifugeRecipient` in the init scripts after `setMintRecipient`. The same issue applies to `ForeignControllerInit`.

Sky: Fixed in commit fb4c2408.

Cantina Managed: Fix verified.