Sky: LZ EVM Token Bridge
Security Review

Cantina Managed review by:

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

October 28, 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 Sep 22nd to Sep 26th the Cantina team conducted a review of sky-oapp-oft on commit hash c4e4f8ca. 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	1	0
Total	**1**	**1**	**0**

The Cantina Managed team reviewed Sky's `sky-oapp-oft` holistically on commit hash b044009d and concluded that all findings were addressed and no new vulnerabilities were identified.

3 Findings

3.1 Informational

3.1.1 Minor issues, Typos & Documentation

Severity: Informational

Context: See each case below

Description:

- SkyRateLimiter.sol#L2: The min pragma version must be increased to `0.8.22`.
- SkyRateLimiter.sol#L15: Comment is inaccurate because we don't implement `Ownable` in this contract.
- SkyOFTAdapterMintBurn.sol#L16: Wrong comment `extends the DoubleSidedRateLimiter contract` ⇒ `extends the SkyOFTCore contract which extends SkyRateLimiter contract`.
- SkyOFTAdapterMintBurn.sol#L117: Missing space `if (_to == address(0) || _to == token())_to = address(0xdead);` ⇒ `if (_to == address(0) || _to == token()) _to = address(0xdead);`.
- SkyOFTAdapter.sol#L89, SkyOFTAdapter.sol#L122-L123, SkyOFTAdapter.sol#L139: Consider describing the way things work in the current implementation, instead of referring to abstract default and non-default implementations. In the current implementation, tokens with irregular transfer balance behavior (like fee-on-transfer tokens) are not supported.

Recommendation: Consider addressing the mentioned issues.

Sky: Fixed in PR 27.

Cantina Managed: Fix verified.