Security Review

Cantina Managed

SKY: DSSEXECLIB V0.1.1

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 Add max line `_amount` value check to `setIlkAutoLineDebtCeiling` . . . 4
  - 3.1.2 Implicit `AutoLine` execution makes debt-ceiling updates order-dependent . . . 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

From Oct 8th to Oct 10th the Cantina team conducted a review of dss-exec-lib on commit hash de6b715c. 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	0	0	0
Gas Optimizations	0	0	0
Informational	2	2	0
Total	**2**	**2**	**0**

The Cantina Managed team reviewed Sky's dss-exec-lib holistically on commit hash 4206c58c 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 dss-exec-lib on commit hash de6b715c:

```
src/DssExecLib.sol
```

3 Findings

3.1 Informational

3.1.1 Add max line `_amount` value check to `setIlkAutoLineDebtCeiling`

Severity: Informational.

Context: DssExecLib.sol#L803.

Description: This `setIlkAutoLineDebtCeiling(bytes32 _ilk, uint256 _amount)` variant lacks the `_amount < WAD` check used by the other variants to reject amounts with incorrect precision.

Recommendation: Consider also adding it to this variant:

```
require(_amount < WAD); // "LibDssExec/incorrect-auto-line-amount-precision"
```

Sky: Fixed in PR 110.

Cantina Managed: Fix verified.

3.1.2 Implicit `AutoLine` execution makes debt-ceiling updates order-dependent

Severity: Informational.

Context: DssExecLib.sol#L808, DssExecLib.sol#L1079-L1082.

Description: AutoLine setters now call `exec`, which can update both the ilk debt ceiling and global `Vat.Line`. If a spell configures AutoLine before calling `addNewCollateral`, this execution can increase `Vat.Line` first. Onboarding then adds its own ceiling and overwrites the ilk ceiling without reversing the earlier global increase, leaving `Vat.Line` higher than intended. Subsequent spell operations must account for both an actual update and a no-op from `exec`.

Recommendation: Document that collateral onboarding must precede AutoLine configuration, and test both `exec` outcomes when composing debt-ceiling changes. Alternatively, keep `exec` separate so spells explicitly control when live ceilings change.

Sky: Fixed by documenting the ordering dependency in commit 9968b371.

Cantina Managed: Fix verified.