Sky

Security Review

Cantina Managed review by:

Christoph Michel, Lead Security Researcher

M4rio.eth, Lead Security Researcher

April 30, 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.

On Apr 17th the Cantina team conducted a review of sky's `src` and `deploy` directory contents on commit hash 893bccd6. The team identified a total of **2** issues in the following risk categories:

- Critical Risk: 0
- High Risk: 0
- Medium Risk: 0
- Low Risk: 0
- Gas Optimizations: 0
- Informational: 2

The Cantina Managed team reviewed Sky's sky holistically on commit hash 893bccd6 and concluded that no new vulnerabilities were identified.

3 Findings

3.1 Informational

3.1.1 Deprecating the Sky ⇒ MKR path will affect external integrators

Severity: Informational

Context: SkyInit.sol#L57

Description: In the new `MkrSky` deployment, users will only be able to convert in the `MKR` → `SKY` direction.

> The legacy `MkrSky` converter supported bi-directional conversions. Upon initialization of the new converter, only the `mkrToSky` path will be supported. It is expected that once the new converter fee becomes non-zero, the `mkrToSky` path in the old converter will also be disabled.

The `SKY` → `MKR` path will be disabled. After some on-chain analysis, we discovered that the following contracts have previously used this conversion path:

```
GPv2Settlement,0x9008d19f58aabd9ed0d60971565aa8510560ab41
CowExecutor,0x3913245cb9c636ef8904a7a863b332082f0c58b0
SwapExecutor,0xb2f72662ed42067ccce278f8462a0215b6adcabb
MainnetSettler,0x70bf6634ee8cb27d04478f184b9b8bb13e5f4710
GnosisSafeProxy,0xf10ef3dd809415b5084f76e6e7e46b7dbf9d05ad
SquidMulticall,0xad6cea45f98444a922a2b4fe96b8c90f0862d2f4
SafeProxy,0x6df12efc08304fd9b0b727d0ab7b07c8a5ddac72
EnsoShortcuts,0x7d585b0e27bbb3d981b7757115ec11f47c476994
GnosisSafeProxy,0x8bd038ff40acae302f39b530d43f3285d3dea7f8
MainnetSettler,0x0d0e364aa7852291883c162b22d6d81f6355428f
GnosisSafeProxy,0x19891541842162ad4311f14055e7221406213d67
SquidMulticall,0xea749fd6ba492dbc14c24fe8a3d08769229b896c
GnosisSafeProxy,0x3282a81912c7b61efd03630b11bfbffcde3df982
GnosisSafeProxy,0xe58918b65000a2b72e3186a99d1d07f5160c9d32
GnosisSafeProxy,0x496a3fc15209350487f7136b7c3c163f9204ee70
GnosisSafeProxy,0x3214b48fc628f33ed0034d66c634f72af3df6577
GnosisSafeProxy,0xbfc30a7b66d913c75c63ddcaaaa12e55821fc12d
```

As observed, some of these are multisigs, but many appear to be protocol contracts—likely used for swapping purposes.

Once the `SKY` → `MKR` path is disabled, these protocols will no longer be able to use it, which could lead to issues such as DoS for certain functionalities.

Recommendation: Coordinate with the affected protocols as early as possible so they can prepare for the deprecation of this path. Additionally, consider broadcasting an alert through appropriate channels to ensure that any party relying on this functionality can take the necessary measures in time.

Sky: Acknowledged.

Cantina Managed: Acknowledged.

3.1.2 `MKR` mint authorities can be removed

Severity: Informational

Context: README.md

Description: The `MkrSky` contract assumes no new MKR will be minted anymore as a fixed amount of SKY (equivalent to `MKR.totalSupply()`) is pre-minted for the conversion.

> Upon initialization, an amount of `Sky` equivalent to the total supply of `Mkr` is minted to it. It is then assumed that further minting of `Mkr` will not happen.

The `MKR` token's `authority` still allows the following contracts to mint:

1. Flopper.
2. DssVestMintable (`MCD_VEST_MKR`). I didn't dive deep into it but it looks old and was last used 4 years ago? What was this one used for?

3. `MCD_PAUSE_PROXY` as the authority's `root`.

Recommendation: Consider fully removing the mint authority for all contracts except the `MCD_PAUSE_PROXY` to ensure no automated MKR mints can happen.

Sky: Acknowledged. It will be considered as part of a general clean-up task in the future, which probably also involves removing the keys from the chainlog.

Cantina Managed: Acknowledged.