CANTINA

MakerDAO: Spark PSM

Security Review

Cantina Managed review by:

M4rio.eth, Security Researcher

Jonatas Martins, Associate Security Researcher

October 23, 2024

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

The Maker Protocol, also known as the Multi-Collateral Dai (MCD) system, allows users to generate Dai (a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar) by leveraging collateral assets approved by the Maker Governance, which is the community organized and operated process of managing the various aspects of the Maker Protocol.

From Oct 16th to Oct 18th the Cantina team conducted a review of spark-psm on commit hash 1e142338.

The Cantina team reviewed MakerDAO's spark-psm changes holistically on commit hash 6a5a579c and determined that all issues were resolved and no new issues were identified.

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

3 Findings

3.1 Informational

3.1.1 Typos in comments

Severity: Informational

Context: See below

Description:

- IPSM3.sol#L95 - `asset in the PSM (e.g., sUSDS).` should be `asset in the PSM.`
- README.md#L14 - `swap between USDC, USDS, and sSUDS,` should be `swap between USDC, USDS, and sUSDS,`
- README.md#L18 - `...held by the PSM` - While this is true now assets might be held by the PSM and the Pocket, even if the whole point of the pocket is that it's the PSM's pocket, no one should take assets out of it. Consider rephrasing it to include the Pocket functionality.

Recommendation: Consider fixing the comments.

Maker: Fixed in v1.0.0-rc.1.

Cantina Managed: Verified.

3.1.2 Increased risks of unwanted share price manipulation by manipulating the `pocket` USDC balance

Severity: Informational

Context: PSM3.sol#L286

Description: The `PSM3.sol` contract includes a `pocket` contract designed to store the `USDC` balance. By default, this `pocket` is set to the `PSM` address (`address(this)`), but it can be modified by invoking the setPocket function. This function transfers the current USDC balance to a new address, as shown below:

```
if (pocket_ == address(this)) {
    usdc.safeTransfer(newPocket, amountToTransfer);
} else {
    usdc.safeTransferFrom(pocket_, newPocket, amountToTransfer);
}
```

The new `Pocket` address is governed by the governance contract, meaning governance has the authority to move the USDC balance. This action could impact the `totalAssets`, subsequently affecting the share price.

Recommendation: To avoid unintended consequences, consider restricting interactions with the `Pocket` balance solely by the PSM.

Maker: Acknowledged. Agreed, this is something that we want to make very clear and known. Governance has control of the pocket and therefore has control over the USDC balance and corresponding totalAssets. This is a new trust assumption that was introduced with the pocket feature.

Cantina Managed: Acknowledged.