CANTINA

MakerDAO: Arbitrum Token Bridge

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 14th to Oct 15th the Cantina team conducted a review of arbitrum-token-bridge on commit hash aedb60f1. 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 Mutable `escrow` increases the risk of creating unbacked l2Tokens

Severity: Informational

Context: L1TokenGateway.sol#L127-L132

Description: In the previous version, the `Escrow` contract was immutable for the bridge. With the introduction of the `file`-able Escrow, the risk of breaking the invariant that the `Escrow` contract must contain sufficient L1 tokens to back the L2 tokens has increased.

Recommendation: Ensure that within the transition spell the full balance of the old `escrow` is moved to the new `escrow` along with granting the required approval for the bridge to pull from the new escrow.

Maker: Acknowledged. When changing the escrow the backing funds are to be moved to the new escrow in the same spell and the bridge is to be approved to pull out funds from the new escrow. Governance is assumed to be fully trusted and set params / execute actions in an extremely careful manner, which covers also this case.

Cantina Managed: Acknowledged.

3.1.2 Missing comment for `maxWithdraws` functionality in documentation

Severity: Informational

Context: README.md

Description: The update in `arbitrum-token-bridge` now includes a limit on withdrawals. However, comments explaining this new feature are still missing from the `README`.

Recommendation: Add information about the new withdrawal limit to the `L2 to L1 withdrawals` section. Specify that each token now has a maximum withdrawal limit set by `maxWithdraws`.

Maker: Acknowledged.

Cantina Managed: Acknowledged.