CANTINA

Maple inance
Security Review

A Cantina Managed review by:

Christoph Michel, Lead Security Researcher

Riley Holterhus, Lead Security Researcher
Jonatas Martins, Associate Security Researcher

June 5, 2023

Contents

1 Introduction

1.1 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.

1.2 Risk assessment

Severity	Description
Critical	*irectly* exploitable security vulnerabilities that need to be fixed.
High	Security vulnerabilities that may not be directly exploitable or may *require certain conditions* in order to be exploited. All high issues should be addressed.
Medium	Objective in nature but are not security vulnerabilities. Should be addressed unless there is a clear reason not to.
Low	Subjective in nature. They are typically suggestions around best practices or readability. Code maintainers should use their own judgment as to whether to address such issues.
Gas	Suggestions around gas saving practices
Informational	Suggestions around best practices or readability.

1.2.1 Severity Classification

The severity of security issues found during the security review is categorized based on the above table. When determining the severity one first needs to determine whether the finding is subjective or objective. All subjective findings are considered of Minor severity.

Next it is determined whether the finding can be regarded as a security vulnerability. Some findings might be objective improvements that need to be fixed, but do not impact the project's security overall (Medium).

Finally, objective findings of security vulnerabilities are classified as either critical or major. Critical findings should be directly vulnerable and have a high likelihood of being exploited. Major findings on the other hand may require specific conditions that need to be met before the vulnerability becomes exploitable.

2 Security Review Summary

Maple Finance is an institutional crypto-capital network built on Ethereum and Solana. Maple provides the infrastructure for credit experts to efficiently manage and scale crypto lending businesses and connect capital from institutional and individual lenders to innovative, blue-chip companies. Built with both traditional financial institutions and decentralized finance leaders, Maple is transforming capital markets by combining industry-standard compliance and due diligence with the frictionless lending enabled by smart contracts and blockchain technology.

From April 24th to May 5th the Cantina team conducted a review of maple-core-v2-private on commit hash d3409c29.

The reviewed code is a new release of Maple V2 that implements Open Term Loans. It also includes enhancements to global contracts to allow for greater flexibility in the allowlist, improvements to incident response, and protection for deployments. Finally, it includes adjustments to Fixed Term Loan contracts to work with the new architecture.

Submodule	Commit hash
fixed-term-loan-private	v5.0.0-rc.1
fixed-term-loan-manager-private	v3.0.0-rc.1
globals-v2-private	v1.1.0-rc.1
liquidations-private	v2.0.0
open-term-loan-private	v1.0.0-rc.1
open-term-loan-manager-private	v1.0.0-rc.1
pool-v2-private	v2.0.0-rc.1
withdrawal-manager-private	v1.0.0

The team identified a total of **18** issues in the following risk categories:

- Critical Risk: 0
- High Risk: 1
- Medium Risk: 1
- Low Risk: 6
- Gas Optimizations: 1
- Informational: 9