Exactly Protocol Smart Contract Review | March 2024

by ChainSafe Systems | March 2024

Table of contents

1. Introduction

Date	Auditor(s)
March 2024	Oleksii Matiiasevych, Tanya Bushenyova, Anderson Lee

Exactly Protocol requested **ChainSafe Systems** to perform a review of the contracts update diff used for Interest Rate Model Upgrade. The contracts in scope can be identified as the following git diff:

`a91c85ab09c0c42b28332fd6dd33d4373163b40f original`
`d424a0758a877e95a9f21a3685c680e086dc2321 update`

Defining Severity

Each finding is assigned a severity level.

Note	Notes are informational 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.
Optimization	Optimizations are objective in nature but are not security vulnerabilities. These should be addressed unless there is a clear reason not to.
Minor	Minor issues are objective in nature but are not security vulnerabilities. These should be addressed unless there is a clear reason not to.
Major	Major issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
Critical	Critical issues are directly exploitable security vulnerabilities that need to be fixed.

Referencing updated code

Resolved	The finding has been acknowledged and the team has since updated the code.
Rejected	The team dismissed this finding and no changes will be made.

Disclaimer

The review makes no statements or warranties about the utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about the fitness of the contracts for any specific purpose, or their bug free status.

2. Executive Summary

All the initially identified high severity issues were fixed and are not present in the final version of the contract.

There are **no** known compiler bugs for the specified compiler version (0.8.23), that might affect the contracts' logic.

There were **0 critical**, **0 major**, **0 minor**, 1 informational/optimization issues identified in the initial version of the contracts. The critical issues found in the contracts were not present in the final version of the contracts, though new minor issues were found. They are described below for historical purposes. A number of substantial logic changes were introduced to the code which is out of scope of the verification step.

We are looking forward to future engagements with the Exactly Protocol team.

3. Line-by-line review

contracts/Market.sol

L909 Note

`totalFloatingBorrowAssets()` function is present in `Market.sol` and in `InterestRateModel.sol` contracts. It could be called from `InterestRateModel.sol` to avoid code duplication. An external call to `InterestRateModel.sol` is already present in `Market.sol` for calculating `floatingRate` so it's possible to pass the rest of the parameters to InterestRateModel's `totalFloatingBorrowAssets()` function for calculating the result.