Smart Contract Final Audit Report for Volmex Finance

Document Properties

Client	Volmex Finance
Title	AMM Admin Fee Accural - Smart Contract Audit Report
Version (code freeze hash)	PR #9
Author	Manmeet Singh Parmar
Auditor	Manmeet Singh Parmar

Overview

The audited commit is `63cb5632d660b72bd2274cdf7af97939ab206300` and all Solidity contract diff in the volmexfinance/AMM-development/pull/9/files folder were in scope.

Project Status

Volmex Finance is a decentralised platform that implies the volatility of crypto assets using options contracts from multiple sources.
Currently, the team is planning to add Admin Fee Accrual functionality in AMM pools.

Timeline

From 2022-03-31 To 2022-04-08

Languages

Solidity

Audit Update

The Volmex team applied all fixes based on the recommendations. The audit fix is 91883a19c8f5abf77a400a9e2b5f1ce0ff5719e0 and contracts are good to deploy on the public Mainnet chain.

Security Assessment

The focus of the audit was to verify that the Smart Contract System is secure, resilient, and working according to the specifications. The audit activities can be classified as

Issues

1. CRITICAL: Bugs leading to Ether or token theft, fund access locking, or any other loss of Ether/tokens to be transferred to any party (for example, dividends)

2. HIGH: Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement

3. WARNINGS: Bugs that can break the intended contract logic or expose it to DoS attacks.

4. NOTES & ADDITIONAL INFORMATION: Other issues and recommendations

Security Assessment Methodology

Goals

- Testing the functionality of the Smart Contract to determine proper logic has been followed throughout the process.
- Analysing the complexity of the code in-depth and detailed, manual review of the code, line-by-line.
- Analysing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analysing the security of the on-chain data.
- A full review of the contract source code. The primary areas of focus include
    - Accuracy
    - Readability
    - Sections of code with high complexity
    - Quantity and quality of test coverage

Stages of audit

- Structural Analysis
- Static Analysis
- Code Review / Manual Analysis

General Feedback

Happy to see such a quality codebase of Volmex Finance. I didn’t find any critical vulnerability and glad to have robustness across the contracts even with novel designs.

Findings List

Level	Amount
CRITICAL	0

HIGH	0
WARNING	1 - Fixed
COMMENTS	1 - Fixed

Detected Issues

CRITICAL

Not Found

HIGH

Not Found

WARNING

[WA01] Storage layout mismatch

In previous version of contracts/VolmexPool.sol the gap of 10 slot were reserved and in new version one slot is been used by new mapping(accruedAdminFee) so in total 9 slot are left for gap.

Recommendation:

Make gap to be of 9 slot and maintain the same amount of slot.

uint256[9] private __gap;

Status: **Fixed**

NOTES & ADDITIONAL INFORMATION

[IN01] Gas optimisation

- The pre-increment operation is cheaper (about 5 GAS per iteration) so use ++i instead of i++ or i+= 1 in for loop. We recommend using pre-increment in all the for loops.
- In for loop the default value initialisation to 0 should not be there remove from all the for loops.

Status: **Fixed**

Conclusion

No critical, High, were found. Changes proposed for comments are implemented or acknowledged by Volmex team.