# BMX Contracts

## Security Review


Cantina Managed review by:

**Om Parikh**, Security Researcher
**Chinmay Farkya**, Associate Security Researcher



August 1, 2025

# 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

BMX provides innovative trading solutions for all assets through various product offerings. One such product is Classic for spot and margin trading, built upon the GMX v1 pool model.

On Jul 22nd the Cantina team conducted a review of morphex-contracts on commit hash ea9d16b9. The team thoroughly examined the PR 1 update to core BMX contracts (GMX fork) and have concluded that the re-entrancy bug in `Orderbook.sol` via native ETH transfer, that resulted in the GMX V1 exploit on the 9th of July 2025, has been patched in the BMX contracts, on commit hash 55b03683, by replacing with WETH transfer in case of returning collateral after `executeDecreaseOrder` and paying keeper fees.

**Issues Found**

| Severity | Count | Fixed | Acknowledged |
|---|---|---|---|
| Critical Risk | 0 | 0 | 0 |
| High Risk | 0 | 0 | 0 |
| Medium Risk | 0 | 0 | 0 |
| Low Risk | 1 | 1 | 0 |
| Gas Optimizations | 0 | 0 | 0 |
| Informational | 0 | 0 | 0 |
| **Total** | **1** | **1** | **0** |

# 3 Findings

## 3.1 Low Risk

### 3.1.1 `ShortsTracker` can be temporarily out of sync due to direct `vault.decreasePosition`

**Severity:** Low Risk

**Description:** When placing and executing orders via `Orderbook`, shorts tracker is updated by `updateGlobalShortData` call in `PositionRouter`. However, user can decrease position directly on vault which doesn't update shorts tracker data. This leads to temporary mispricing of BLT as global shorts average price is lagging until some other user interacts via `PositionRouter` or shorts data is updated externally by some other means. This scenario is currently not exploitable in practice because of fees on trades, fees on minting and burning BLT, various imposed caps and can't be executed atomically requiring to take positional risk. This also requires large uninterrupted price movements (i.e no other user/s except malicious trader is opening/closing positions while large price movement takes place).

**Recommendation:**

- Since `Vault.sol` can't be upgraded, add additional strict checks in `VaultUtils.sol` and replace address in vault contract to newly deployed vault utils, or...
- Shorts tracker's global short average price should be monitored externally and if any discrepancies are found, it should be updated/adjusted to correct value.

**BMX:** Fixed in PR 1

**Cantina Managed:** Fix verified.