RETRO BRIDGE

Audit Report by Yevhenii Bezuhlyi

@BezuglyiE

Date:

November 2023

Table of Contents

About Retrobridge

Retrobridge is an advanced cross-chain bridging solution designed to simplify the transfer of assets between blockchain networks.
By utilizing concentrated liquidity on each chain, we ensure rapid and direct asset cross-chain transfers, bypassing the
complexities of smart contracts and consequently reducing bridging costs. This efficiency is further emphasized through its direct transfer mechanisms.

Disclaimer

This document presents the findings of a security audit conducted on the specified backend application. The audit was performed based on the information provided by the client and the state of the application at the time of the audit.

- **Scope Limitation**

  The findings are confined to the scope agreed upon with the client and may not cover all potential security risks. The audit was conducted on the application's version as provided, and any changes made to the application post-audit may affect the validity of these findings.

- **No Guarantee of Security**

  While this audit aims to identify security vulnerabilities and provide recommendations for mitigation, it does not guarantee that the application is free from security risks. New vulnerabilities may emerge, and existing vulnerabilities may be exploited in ways not identified in this audit.

- **Limitation of Liability**

  The auditor is not liable for any direct, indirect, incidental, consequential, or any other damages resulting from using the information provided in this audit. The client is responsible for the final decision on implementing the recommendations provided.

Yevhenii Bezuglyi

@BezuglyiE

Yevhenii Bezuhlyi boasts an extensive background in cybersecurity, specializing in web3 security since 2018. As the former head of Hacken's Smart Contracts Audit Department, he has audited over 150 web3 projects, underscoring his deep expertise in the field.

Starting his professional journey in 2013 as a Java developer on a military project, Yevhenii quickly demonstrated a knack for embracing new challenges. By 2016, he had climbed the ranks to become a senior developer at Epam, sharpening his skills in reverse engineering and code auditing. His entry into the blockchain space came in 2018 with his first smart contract audit. That same year, he launched Tabia, a software outsourcing firm that caters to high-load, fintech, and web3 projects, counting Hacken, a pioneer in web3 cybersecurity, among its first clients.

Yevhenii's leadership at Tabia involved not only overseeing project development but also personally conducting smart contract audits for Hacken. In 2019, he ventured into the advertising and marketing arena by co-founding an agency, although this was short-lived, wrapping up operations in 2020. Despite the venture's brief duration, Yevhenii continued to refine his technical acumen, engaging in extensive bug-hunting for both traditional web2 systems and cutting-edge technologies.

His tenure at Hacken, beginning in January 2022, was marked by significant achievements. As the head of the smart contracts audits department, he was instrumental in setting up its foundational structure, facilitating departmental growth, and training a new generation of professional auditors. His commitment to comprehensive auditing processes catered to a wide array of client security needs, extending beyond simple code review.

In July 2023, Yevhenii transitioned to an independent role, offering his expertise as a cybersecurity consultant and auditor. He now serves as the Security Advisor at RetroBridge, where he continues to ensure the integrity of the company's infrastructure and the security of new feature releases through regular audits.

Severities Definition

Risks Classification

Impact / Likelihood	High	Medium	Low
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Impact

High	leads a significant financial losses or irrecoverable data consistency issues.
Medium	leads a financial losses to only a subset of users, but still unacceptable.
Low	leads to low financial losses or easily recoverable data consistency issues.

Likelihood

High	easy to prepare and execute or are always executing within the system during the regular flow.
Medium	requires additional preparations and specific conditions.
Low	requires very specific conditions and most likely will never be executed during the regular flow of the app.

Summary

The audited code contains:

Critical — **1** critical issue

Medium — **2** medium issue

Low — **1** low severity issue

Informational and architectural issues are omitted.

№	Title	Severity	Status
1	Order content substitution	Critical	✅ Fixed
2	Double-spending during an order fulfillment process	Medium	✅ Fixed
3	Insufficient number of confirmations	Medium	✅ Fixed
4	Non-validated response from the prices provider	Low	✅ Fixed

Findings

Critical Risk Findings (1)

1. Order content substitution

Impact	Allows third parties to substitute order information such as the receiving party.	High
Likelihood	Easy to execute	High
Description	The description has been intentionally withheld to ensure the security and confidentiality of the app's architecture and codebase.	
Recommendation	Sessions management should be added to validate a request origin. Authentication could be done by the **eip-4361** or its variations.	
Resolution	✅ Fixed	

Medium Risk Findings (2)

1. Double-spending during an order fulfillment process

Impact	Can lead to multiple fulfillment of the same order.	High
Likelihood	The service execution must be aborted at its very specific stage of execution	Low
Description	The description has been intentionally withheld to ensure the security and confidentiality of the app's architecture and codebase.	

Recommendation	Order execution flow should follow the principles of transactional systems. All the external calls should be made in an async mode with the possibility to verify whether the same request has been sent and/or processed before.
Resolution	✅ Fixed

2. Insufficient number of confirmations

Impact	Orders that are not funded might be considered as funded.	High
Likelihood	The chances of a network reordering are low-to-impossible within the supported networks.	Low
Description	The description has been intentionally withheld to ensure the security and confidentiality of the app's architecture and codebase.	
Recommendation	Add the recommended number of confirmations for each network where it's required.	
Resolution	✅ Fixed	

Low Risk Findings (1)

1. Non-validated response from the provider of the price

Impact	Outdated prices can be used, leading to the platform's financial losses.	Low
Likelihood	Likely to happen if the price provider experiences issues or shuts down.	Medium
Description	The description has been intentionally withheld to ensure the security and confidentiality of the app's architecture and codebase.	

Recommendation	Implement fallback prices provider. Constantly evict the cache on timeout. Add correct procession for cases when the cache is empty.
Resolution	✅ Fixed