Wakehacker Report

Contract address	0xbe58fda3bcf03b6bbc821d1f0e6b764c86709227
Chain ID	8453
Report version	1.0
Last edit	November 25, 2025

"Static analysis or stay rekt"

Document Revisions

1.0	Wakehacker Report - 0xBE58fdA3Bcf03B6bbc821D1f0E6b764C86709227 on chain 8453	November 25, 2025

Contents

Overview

This report was generated using Wakehacker, an automated vulnerability analysis tool. Wakehacker utilizes Wake with additional detectors to perform comprehensive AI and static analysis.

To identify potential vulnerabilities and issues in smart contracts Wake framework utilizes:

- Code structure and patterns
- Control flow graph
- Data flow graph
- Common vulnerability patterns
- Contract interactions

The findings presented in this report are based on automated analysis optimized for precision, aiming for a low false-positive rate. The detection is not optimized for recall—it doesn't target finding all issues (which come at the cost of a high false-positive rate). This code review should be complemented with additional manual code review for a complete security assessment.

Disclaimer

The best effort has been put into finding known vulnerabilities in the system, however automated findings shouldn't be considered as a complete list of all existing issues. The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them.

Finding Classification

Each finding is classified by two independent ratings: `Impact` and `Confidence`.

Impact

Measuring the potential consequences of the issue on the system.

- **Critical** - Code that activates the issue directly enables theft of significant assets with minimal preconditions.
- **High** - Code that activates the issue will lead to undefined or catastrophic consequences for the system.
- **Medium** - Code that activates the issue will result in consequences of serious substance.
- **Low** - Code that activates the issue will have outcomes on the system that are either recoverable or don’t jeopardize its regular functioning.
- **Warning** - The issue represents a potential security concern in the code structure or logic that could become problematic with code modifications.
- **Info** - The issue relates to code quality practices that may affect security. Examples include insufficient logging for critical operations or inconsistent error handling patterns.

Confidence

Indicating the probability that the identified issue is a valid security concern.

- **High** - The analysis has identified a pattern that strongly indicates the presence of the issue.
- **Medium** - Evidence suggests the issue exists, but manual verification is recommended.
- **Low** - Potential indicators of the issue have been detected, but there is a significant possibility of false positives.

Executive Summary

Revision 1.0

The audit reported no security issues across any severity or confidence level, indicating a clean result and a strong overall security posture.

Findings

Summary by Impact

Critical	High	Medium	Low	Warning	Info	Total
0	0	0	0	0	0	0

”Static analysis or stay rekt”

https://wakehacker.ai