

RITA AI Smart Contract Auditor

Unknown

0xfb5b838b6cfeedc2873ab27866079ac55363d37e

Detailed Security Audit

Critical Functions Check

Issue Description	Checking Status
Compiler errors	Passed
Race conditions and Reentrancy, Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
Timestamp dependence	Low Risk
Integer Overflow and Underflow	Low Risk
Dos with Revert	Low Risk
Dos with block gas limit	Passed
Methods execution permissions	Low Risk
Economy model of the contract	Passed
The impact of the exchange rate on the logic	Passed
Private user data leaks	Passed
Malicious Event log	Low Risk
Scoping and Declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Design Logic	Passed
Cross-function race conditions	Passed
Safe Open Zeppelin contracts implementation and usage	Passed
Fallback function security	Passed
Unsafe delegatecall usage	Passed
Unrestricted public functions	Passed
Potential infinite loops	Low Risk
High gas consumption operations	Passed
Unsafe send/transfer usage	Low Risk

Risky Functions Details

Function: timestamp

Potential timestamp dependence detected, risking manipulation of block timestamps for malicious behavior

Function: permissions

Potential insecure method execution permissions detected, risking unauthorized access

Function: loops

Potential infinite loops detected, risking contract freezing or high gas costs

Function: send/transfer

Potential unsafe send/transfer usage detected, risking reentrancy or fund loss



This audit was conducted and prepared by RITA AI