

RITA AI Smart Contract Auditor

Unknown

0xba2ae424d960c26247dd6c32edc70b295c744c43

Detailed Security Audit

Critical Functions Check

Issue Description	Checking Status
Compiler errors	Passed
Race conditions and Reentrancy, Cross-function race conditions	High Risk
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
Timestamp dependence	Passed
Integer Overflow and Underflow	Passed
Dos with Revert	Low Risk
Dos with block gas limit	Low Risk
Methods execution permissions	Passed
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	Low Risk
Cross-function race conditions	Passed
Safe Open Zeppelin contracts implementation and usage	Passed
Fallback function security	Low Risk
Unsafe delegatecall usage	Low Risk
Unrestricted public functions	Low Risk
Potential infinite loops	Low Risk
High gas consumption operations	Low Risk
Unsafe send/transfer usage	Low Risk

Risky Functions Details

Function: reentrancy

Critical reentrancy vulnerability detected, risking multiple function calls during a single transaction

Function: delegatecall

Potential unsafe use of delegatecall detected, risking unauthorized code execution

Function: public

Potential unrestricted public functions detected, risking unauthorized access to contract functionality

Function: loops

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

Function: gas

Potential high gas consumption operations detected, risking transaction failures or DoS attacks

Function: send/transfer

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

This audit was conducted and prepared by RITA AI

Verify this report at: https://raw.githubusercontent.com/RETOKENofficial/RITA/main/audit_0xba2ae424d960c26247dd6c32e