Audit Report - f734bee1-c3f5-4441-b508-8930c6940442

Vulnerabilities

HIGH - Line 134

Issue: Reentrancy vulnerability in fulfillRandomWords function

Recommendation: Use a reentrancy lock or the Checks-Effects-Interactions pattern to prevent reentrancy attacks

MEDIUM - Line 83

Issue: Use of tx.origin is not present, but the contract relies on msg.sender which can be manipulated in certain cases

Recommendation: Consider using a more secure method of authentication if needed, or ensure that the contract's functionality is not affected by this

LOW - Line 164

Issue: Use of call() without gas stipend

Recommendation: Consider using a gas stipend or a more modern transfer method like OpenZeppelin's Address.sendValue()

LOW - Line 53

Issue: Missing input validation for constructor parameters

Recommendation: Add input validation for constructor parameters to prevent incorrect configuration

Gas Optimizations

Estimated Gas Usage: 25,00,000 gas

Line 93: Use a more gas-efficient way to check if an array is empty

Estimated Savings: 100 gas

Line 134: Minimize the number of storage writes in the fulfillRandomWords function

Estimated Savings: 5,000 gas

Line 164: Use a more gas-efficient way to transfer Ether

Estimated Savings: 2,000 gas

Line 83: Pack multiple storage variables into a single slot

Estimated Savings: 1,000 gas