

Audit Report - 17380e1d-b35e-4fd0-8f44-3cc9bce551c0

HIGH - Line 156

Issue: Reentrancy vulnerability due to external call before state update

Recommendation: Use the Checks-Effects-Interactions pattern. Move the external call to after state updates.

MEDIUM - Line 91

Issue: Lack of input validation for constructor parameters

Recommendation: Validate constructor parameters to prevent unexpected behavior or potential vulnerabilities.

LOW - Line 138

Issue: Missing zero address check for recentWinner

Recommendation: Check if recentWinner is the zero address before transferring funds to prevent potential loss.

LOW - Line 116

Issue: Unused requestId parameter in fulfillRandomWords

Recommendation: Remove unused parameters to improve code readability and maintainability.

LOW - Line 61

Issue: Potential denial of service due to unbounded array s_players

Recommendation: Consider implementing a mechanism to limit the number of players or use a more gas-efficient data structure.