

Audit Report - 564f5329-4c33-407c-b7b8-7a44901b295d

MEDIUM - Line 133

Issue: Potential reentrancy vulnerability

Recommendation: Use a reentrancy lock to prevent reentrancy attacks

HIGH - Line 134

Issue: Unsecured use of ``call`` for transferring Ether

Recommendation: Use a secure method like OpenZeppelin's ``Address.sendValue`` or implement a pull-over-push pattern for withdrawals

LOW - Line 82

Issue: Unused variable ``checkData``

Recommendation: Remove or utilize the ``checkData`` variable to improve code readability and maintainability

LOW - Line 109

Issue: Unused variable ``performData``

Recommendation: Remove or utilize the ``performData`` variable to improve code readability and maintainability

MEDIUM - Line 123

Issue: Potential denial of service due to unvalidated ``randomWords`` length

Recommendation: Validate the length of ``randomWords`` before accessing its elements to prevent potential denial of service

LOW - Line 75

Issue: Missing input validation for ``subscriptionId``, ``gasLane``, ``interval``, ``entranceFee``, ``callbackGasLimit``, and ``vrfCoordinatorV2`` in the constructor

Recommendation: Add input validation for these constructor parameters to prevent potential misconfigurations or attacks