PuppyRaffle Smart Contract Audit Report

Protocol Summary

PuppyRaffle is an NFT raffle protocol where users enter by paying an entrance fee. After a fixed duration, a winner is selected, receives the ETH prize, and an NFT puppy is minted. Users may refund their entry before the raffle concludes. The protocol owner controls fee configuration.

Disclaimer

This audit was conducted on a time-boxed basis and focuses solely on the security of the smart contracts. No guarantee is provided that all vulnerabilities have been identified. This report is not an endorsement of the protocol.

Executive Summary

The audit identified multiple security and design issues, including weak randomness, MEV-related refund griefing, and denial-of-service risks caused by unbounded loops.

High Severity Findings

H-01: Weak and predictable randomness in selectWinner() can be manipulated by attackers or MEV actors.

Medium Severity Findings

M-01: Players can front-run selectWinner() with refunds after learning outcomes.
M-02: Duplicate checks in enterRaffle() can lead to denial of service as the players array grows.

Low Severity Findings

L-01: Refunded players may result in zero-address winners, causing loss of funds or NFTs.

Recommendations

Use verifiable randomness (e.g., Chainlink VRF), lock raffle state at end time, replace loops with mappings, and add defensive checks for admin actions.