VestingWallet Contract Audit Report

What does the contract do?

The VestingWallet contract is designed to gradually release funds (both Ether and ERC20 tokens) to a de

Vulnerabilities:

1. **Vulnerability Name:** **Unchecked ERC20 Transfer**
   - **Severity**: Medium
   - **Description**: The `release(address token)` function calls `IERC20(token).transfer(beneficiary(), rel
   - **Impact**: Users could lose funds if the ERC20 token transfer fails.
   - **Mitigation**: Always check the return value of `IERC20.transfer` and revert the transaction if it fails.

2. **Vulnerability Name:** **Potential Front-Running Attacks**
   - **Severity**: Medium
   - **Description**: The `release` and `release(address token)` functions are public, allowing anyone to t
   - **Impact**: Miners could potentially exploit the release functions for their own financial gain, possibly
   - **Mitigation**: Implement access controls to restrict who can call the `release` functions. This could b

3. **Vulnerability Name:** **Potential Loss of Funds Due to Contract Incompatibility**
   - **Severity**: Medium
   - **Description**: The contract assumes that all ERC20 tokens adhere to the standard interface. Howe
   - **Impact**: Funds sent to the contract could be lost if the token transfer fails due to incompatibility wit
   - **Mitigation**: Implement checks to ensure that the token contract follows the ERC20 standard before

4. **Vulnerability Name:** **Potentially Incorrect Vesting Schedule Calculation**
   - **Severity**: Medium
   - **Description**: The contract assumes a linear vesting schedule. This might not align with the intende
   - **Impact**: The beneficiary might receive more or less funds than intended if the actual vesting sched
   - **Mitigation**: Ensure the vesting schedule is correctly implemented to match the intended behavior.

5. **Vulnerability Name:** **Lack of Withdrawal Mechanism for Mistakenly Sent Tokens**
   - **Severity**: Low
   - **Description**: The contract lacks a mechanism to withdraw tokens that were mistakenly sent to it. T
   - **Impact**: The contract could lose valuable funds if tokens are mistakenly sent to it, as there's no me
   - **Mitigation**: Implement a function to withdraw mistakenly sent tokens, potentially with an authorizat

6. **Vulnerability Name:** **Single Point of Failure in Beneficiary Address**
   - **Severity**: Medium
   - **Description**: The beneficiary address is set in the constructor and cannot be changed. If the privat
   - **Impact**: Loss of access to the beneficiary address could result in irreversible loss of all funds in the
   - **Mitigation**: Implement a mechanism to change the beneficiary address in case of emergency or co

Conclusion:

The VestingWallet contract exhibits several vulnerabilities that could lead to financial losses for users. Th