Smart Contract Audit Report: TaxableERC20

This report summarizes the findings of a comprehensive audit of the TaxableERC20 smart contract, conc

1. Owner Privilege Misuse

- **Severity**: High
- **Description**: The `onlyOwner` modifier grants the contract owner extensive control over tax settings,
- **Impact**: If the owner's account is compromised, an attacker could manipulate these parameters, pote
- **Mitigation**: Implement a multi-signature wallet or a timelock mechanism for owner operations to prev

2. Unchecked Underflow

- **Severity**: Medium
- **Description**: The contract uses the `unchecked` keyword in several functions, bypassing Solidity's bu
- **Impact**: This can lead to unexpected underflows, allowing an attacker to manipulate balances or pote
- **Mitigation**: Remove the `unchecked` keyword and implement manual underflow checks using `requir

3. Insecure Service Payer

- **Severity**: Medium
- **Description**: The `ServicePayer` constructor uses the `msg.value` to send Ether to a receiver addres
- **Impact**: An attacker could potentially manipulate the receiver address during deployment, diverting th
- **Mitigation**: Validate the receiver address before sending Ether. Consider using a trusted address or a

4. Missing Access Control in `_mint`

- **Severity**: Medium
- **Description**: The `_mint` function within the ERC20 contract lacks proper access control mechanism
- **Impact**: This could allow any address to mint an unlimited supply of tokens, potentially devaluing the
- **Mitigation**: Implement access control in the `_mint` function, restricting it to authorized addresses.

5. High Tax Rate Risks

- **Severity**: Low
- **Description**: The contract's tax mechanism, while functional, doesn't have a built-in mechanism to pr
- **Impact**: Setting a high tax rate might discourage users from interacting with the token due to high tra
- **Mitigation**: Implement a maximum tax rate limit to prevent excessively high tax burdens.

Overall Recommendations

This audit identified several vulnerabilities in the TaxableERC20 contract, requiring immediate attention. T

This report is for informational purposes only and does not constitute financial or legal advice. Always con