Smart Contract Audit Report: YFVStake

This report summarizes the findings of a comprehensive audit conducted on the YFVStake smart contrac

Note: This report only reflects vulnerabilities identified in the code provided. Any changes to the contra

1. Compiler Version Mismatch

- **Severity**: High
- **Description**: The contract uses `pragma solidity ^0.5.5;`, which is incompatible with the current comp
- **Impact**: The contract will fail to compile with the current version of Solidity, making it unusable.
- **Mitigation**: Update the `pragma` statement to match the compiler version used.

2. Unsupported Instruction (extcodehash)

- **Severity**: Low
- **Description**: The contract uses the `extcodehash` instruction in assembly, which is not supported by
- **Impact**: The instruction may fail to execute properly, potentially causing unexpected behavior.
- **Mitigation**: Remove the `extcodehash` instruction or use a compatible instruction for this VM versior

3. Potential for Referral Abuse

- **Severity**: Medium
- **Description**: The `setReferrer` function does not check if the new referrer is already associated with
- **Impact**: A malicious actor could potentially earn multiple commissions by repeatedly setting themsel
- **Mitigation**: Implement a check to ensure that a user cannot be set as a referrer for multiple accounts

4. Potential for Unintended Reward Rate Changes

- **Severity**: Medium
- **Description**: The `updateReward` function does not check if the new reward rate is valid. This could
- **Impact**: An attacker could potentially set an invalid reward rate, leading to incorrect reward calculati
- **Mitigation**: Add a check to validate the new reward rate before updating it.

Overall Assessment:

This smart contract exhibits a moderate level of security risk. The critical compiler version mismatch and

Recommendation:

- **Priority 1:** Update the `pragma` statement and remove the `extcodehash` instruction to ensure comp
- **Priority 2:** Implement checks to prevent referral abuse and validate the new reward rate in the `upda

It's crucial to conduct further analysis and have the contract audited by a professional security firm to ens