MultiStablesVault Smart Contract Audit Report

This report summarizes the findings from a comprehensive audit of the MultiStablesVault smart contract,

Vulnerability Summary:

The analysis reveals no high-severity vulnerabilities. The contract leverages SafeMath for all arithmetic o

Vulnerability Details:

1. Potential Stack Overflow Vulnerability:

- **Severity**: Low
- **Description**: Slither detected a potential stack overflow vulnerability within the `withdrawFor` function
- **Impact**: This could lead to a Denial-of-Service (DoS) attack if the contract is forced to execute a large
- **Mitigation**: Refactor the `withdrawFor` function to simplify the call structure, minimizing the number o

2. Potential Information Disclosure through `getPricePerFullShare` and `get_virtual_price` Functions:

- **Severity**: Low
- **Description**: LLaMA identified potential information disclosure through these functions, which calcula
- **Impact**: An attacker could potentially gain insights into the vault's underlying assets and strategies ba
- **Mitigation**: Implement appropriate masking or rounding mechanisms to minimize the sensitivity of the

3. Potential Vulnerability in `input2Want` Mapping:

- **Severity**: Not Applicable
- **Description**: LLaMA initially flagged this mapping as vulnerable to manipulation due to its lack of inpu
- **Impact**: N/A
- **Mitigation**: N/A

4. Potential Denial-of-Service (DoS) Attack through Infinite Loops:

- **Severity**: Not Applicable
- **Description**: LLaMA initially suggested a DoS vulnerability through the `harvestAllStrategies` function
- **Impact**: N/A
- **Mitigation**: N/A

Recommendations:

- **Address Stack Overflow Vulnerability**: Refactor the `withdrawFor` function to optimize the call structu
- **Enhance Information Disclosure Mitigation**: Consider masking or rounding for sensitive data calculat
- **Perform a Thorough Security Review:** Conduct a comprehensive security review of the contract to id

Disclaimer:

This report provides a summary of the audit findings and should not be considered a comprehensive secu