



# Smart Contract Security Audit Report



# Table Of Contents

<b>1 Executive Summary</b>	_____
<b>2 Audit Methodology</b>	_____
<b>3 Project Overview</b>	_____
3.1 Project Introduction	_____
3.2 Vulnerability Information	_____
<b>4 Code Overview</b>	_____
4.1 Contracts Description	_____
4.2 Visibility Description	_____
4.3 Vulnerability Summary	_____
<b>5 Audit Result</b>	_____
<b>6 Statement</b>	_____

# 1 Executive Summary

On 2024.07.08, the SlowMist security team received the StakeStone team's security audit application for StakeStone - SymbioticDepositWBETHStrategy, developed the audit plan according to the agreement of both parties and the characteristics of the project, and finally issued the security audit report.

The SlowMist security team adopts the strategy of "white box lead, black, grey box assists" to conduct a complete security test on the project in the way closest to the real attack.

The test method information:

Test method	Description
Black box testing	Conduct security tests from an attacker's perspective externally.
Grey box testing	Conduct security testing on code modules through the scripting tool, observing the internal running status, mining weaknesses.
White box testing	Based on the open source code, non-open source code, to detect whether there are vulnerabilities in programs such as nodes, SDK, etc.

The vulnerability severity level information:

Level	Description
Critical	Critical severity vulnerabilities will have a significant impact on the security of the DeFi project, and it is strongly recommended to fix the critical vulnerabilities.
High	High severity vulnerabilities will affect the normal operation of the DeFi project. It is strongly recommended to fix high-risk vulnerabilities.
Medium	Medium severity vulnerability will affect the operation of the DeFi project. It is recommended to fix medium-risk vulnerabilities.
Low	Low severity vulnerabilities may affect the operation of the DeFi project in certain scenarios. It is suggested that the project team should evaluate and consider whether these vulnerabilities need to be fixed.
Weakness	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.
Suggestion	There are better practices for coding or architecture.

## 2 Audit Methodology

The security audit process of SlowMist security team for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using automated analysis tools.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that was considered during the audit of the smart contract:

Serial Number	Audit Class	Audit Subclass
1	Overflow Audit	-
2	Reentrancy Attack Audit	-
3	Replay Attack Audit	-
4	Flashloan Attack Audit	-
5	Race Conditions Audit	Reordering Attack Audit
6	Permission Vulnerability Audit	Access Control Audit
		Excessive Authority Audit
7	Security Design Audit	External Module Safe Use Audit
		Compiler Version Security Audit
		Hard-coded Address Security Audit
		Fallback Function Safe Use Audit
		Show Coding Security Audit
		Function Return Value Security Audit
		External Call Function Security Audit

Serial Number	Audit Class	Audit Subclass
7	Security Design Audit	Block data Dependence Security Audit
		tx.origin Authentication Security Audit
8	Denial of Service Audit	-
9	Gas Optimization Audit	-
10	Design Logic Audit	-
11	Variable Coverage Vulnerability Audit	-
12	"False Top-up" Vulnerability Audit	-
13	Scoping and Declarations Audit	-
14	Malicious Event Log Audit	-
15	Arithmetic Accuracy Deviation Audit	-
16	Uninitialized Storage Pointer Audit	-

## 3 Project Overview

### 3.1 Project Introduction

This audit is mainly focused on a new staking strategies: SymbioticDepositWBETHStrategy. The owner role can wrap ETH in the contract into WBETH and deposit the WBETH in the contract into the third-party protocol, and then redeem the deposit certificate in the contract into WBETH.

### 3.2 Vulnerability Information

The following is the status of the vulnerabilities found in this audit:

NO	Title	Category	Level	Status
N1	Ignoring the Return Value	Others	Information	Acknowledged

## 4 Code Overview

### 4.1 Contracts Description

#### Audit Version:

<https://github.com/stakestone/stone-vault-v1>

commit: a1735b715f64b462a7f352325bfb7d89b3e71c0d

Audit scope:

- /contracts/strategies/SymbioticDepositWBETHStrategy.sol

The main network address of the contract is as follows:

**The code was not deployed to the mainnet.**

### 4.2 Visibility Description

The SlowMist Security team analyzed the visibility of major contracts during the audit, the result as follows:

SymbioticDepositWBETHStrategy			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Can Modify State	StrategyV2
deposit	Public	Payable	onlyController notAtSameBlock
withdraw	Public	Can Modify State	onlyController
instantWithdraw	Public	Can Modify State	onlyController
clear	Public	Can Modify State	onlyController
_withdraw	Internal	Can Modify State	-

SymbioticDepositWBETHStrategy			
getAllValue	Public	Can Modify State	-
getInvestedValue	Public	Can Modify State	-
getWBETHValue	Public	-	-
wrapToWBETH	External	Can Modify State	onlyOwner
depositIntoSymbiotic	External	Can Modify State	onlyOwner
withdrawFromSymbiotic	External	Can Modify State	onlyOwner
requestToEther	External	Can Modify State	onlyOwner
claimPendingAssets	External	Can Modify State	onlyOwner
checkPendingAssets	Public	-	-
<Receive Ether>	External	Payable	-

## 4.3 Vulnerability Summary

### [N1] [Information] Ignoring the Return Value

#### Category: Others

#### Content

In the SymbioticDepositWBETHStrategy contract, the owner can extract the claimable ETH by calling the claimPendingAssets function. This function will call the claimWithdraw function of the UnwrapTokenV1ETH contract to claim the corresponding ETH by passing in a specific index.

The claimWithdraw function returns a value (\_ethAmount) after each call to represent the number of ETH claimed.

Code Location:

contracts/strategies/SymbioticDepositWBETHStrategy.sol#L176

```
function claimPendingAssets(uint256 _index) external onlyOwner {
    IUnwrapTokenV1ETH(unwrapTokenV1ETHAddr).claimWithdraw(_index);
}
```

```
}
```

**Solution**

N/A

**Status**

Acknowledged; Project team response: The wbETH contract implementation only stores a value of ETH to be claimed. After triggering the claimWithdraw function, it only transfers the same amount of ETH back to the SymbioticDepositWBETHStrategy contract, and there is no other logic that will cause the value of this return to be inconsistent with the value previously recorded

## 5 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002407080001	SlowMist Security Team	2024.07.08 - 2024.07.08	Passed

Summary conclusion: The SlowMist security team uses a manual and SlowMist team's analysis tool to audit the project, during the audit work we found 1 information. All findings were acknowledged . The code was not deployed to the mainnet.



## 6 Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility based on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.



**Official Website**  
[www.slowmist.com](http://www.slowmist.com)



**E-mail**  
[team@slowmist.com](mailto:team@slowmist.com)



**Twitter**  
[@SlowMist\\_Team](https://twitter.com/SlowMist_Team)



**Github**  
<https://github.com/slowmist>