Smart Contract
Security Audit Report

Table Of Contents

1 Executive Summary

On 2022.08.29, the SlowMist security team received the hashkey team's security audit application for DID Resolver, 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

Serial Number	Audit Class	Audit Subclass
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
		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

Audit Version

File name: contracts.zip

SHA256: 0cd43738e0108172a1a1afa9cdc9727f173e3e48d51a3e2a0ae70f45e35d33a6

Fixed Version

File name: resolver.zip

SHA256: ad80d66182427c57b3dd4c0dfb69b9cbac4ae92e2ab94bb5457bcebeab1f4991

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Missing event record	Others	Suggestion	Fixed

4 Code Overview

4.1 Contracts Description

Codebase:

https://auditspace.oss-cn-hangzhou.aliyuncs.com/zip/dbe82b2f-30f0-45a3-83f6-bae3431c4e8e.zip

ad80d66182427c57b3dd4c0dfb69b9cbac4ae92e2ab94bb5457bcebeab1f4991

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:

Resolver			
Function Name	Visibility	Mutability	Modifiers

Resolver			
initialize	Public	Can Modify State	initializer
setReverse	Public	Can Modify State	-
name	Public	-	-
setAddr	Public	Can Modify State	authorized
addr	Public	-	-
setContentHash	External	Can Modify State	authorized
contentHash	External	-	-
setPubkey	External	Can Modify State	authorized
pubkey	External	-	-
setText	External	Can Modify State	authorized
text	External	-	-

ResolverStorage			
Function Name	Visibility	Mutability	Modifiers

EternalStorageProxy			
Function Name	Visibility	Mutability	Modifiers
<Constructor>	Public	Payable	TransparentUpgradeableProxy

4.3 Vulnerability Summary

[N1] [Suggestion] Missing event record

Category: Others

Content

Modifying contract parameters is missing an event record.

Code location: resolver.sol #L46-48

```
    function setReverse(address _addr, bool isReverse) public {
        _isReverse[_addr] = isReverse;
    }
```

Solution

It is recommended to add corresponding event records.

Status

Fixed

5 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002208300001	SlowMist Security Team	2022.08.29 - 2022.08.30	Passed

Summary conclusion: The SlowMist security team uses a manual and SlowMist team's analysis tool for auditing the project, during the audit we have found 1 suggestion. And 1 suggestion has been fixed. 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

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist