SLOWMIST

Smart Contract Security Audit Report

The SlowMist Security Team received the team's application for smart contract security audit of the ParticleOFT on 2025.03.21. The following are the details and results of this smart contract security audit:

Token Name :

ParticleOFT

The contract address :

https://github.com/Particle-Network/oft-token/

commit: 8280d20ce5bfcf1e747f32d1c8863a2ab979032c

The audit items and results :

(Other unknown security vulnerabilities are not included in the audit responsibility scope)

NO.	Audit Items	Result
1	Replay Vulnerability	Passed
2	Denial of Service Vulnerability	Passed
3	Race Conditions Vulnerability	Passed
4	Authority Control Vulnerability Audit	Passed
5	Integer Overflow and Underflow Vulnerability	Passed
6	Gas Optimization Audit	Passed
7	Design Logic Audit	Passed
8	Uninitialized Storage Pointers Vulnerability	Passed
9	Arithmetic Accuracy Deviation Vulnerability	Passed
10	"False top-up" Vulnerability	Passed
11	Malicious Event Log Audit	Passed
12	Scoping and Declarations Audit	Passed
13	Safety Design Audit	Passed

NO.	Audit Items	Result
14	Non-privacy/Non-dark Coin Audit	Passed

Audit Result : Passed

Audit Number : 0X002503250001

Audit Date : 2025.03.21 - 2025.03.25

Audit Team : SlowMist Security Team

Summary conclusion : This is an OFT contract that does not contain the token vault section and the dark coin functions. The total amount of contract tokens remains unchangeable. The contract does not have the Overflow and the Race Conditions issue.

The source code:

```
// SPDX-License-Identifier: UNLICENSED
//SlowMist// The contract does not have the Overflow and the Race Conditions issue
pragma solidity ^0.8.28;

import { Ownable } from "@openzeppelin/contracts/access/Ownable.sol";
import { OFT } from "@layerzerolabs/lz-evm-oapp-v2/contracts/oft/OFT.sol";
import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Permit.sol";

contract ParticleOFT is OFT, ERC20Permit {
    uint256 public immutable MAX_SUPPLY = 1_000_000_000 * 10 ** 18; // 1 billion
total tokens

    constructor(
        uint256 _mainChainId,
        string memory _name,
        string memory _symbol,
        address _lzEndpoint,
        address _delegate,
        address _treasury
    ) OFT(_name, _symbol, _lzEndpoint, _delegate) Ownable(_delegate)
ERC20Permit(_name) {
        if (block.chainid == _mainChainId) {
            _mint(_treasury, MAX_SUPPLY);
        }
    }
}
```

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.

SLOWMIST

Official Website

www.slowmist.com

✉

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist