AIAC AgentToken OFT

Security Assessment

Prepared by: **RigSec**

August 12, 2025

Contents

1 Introduction 2

1.1 About RigSec . . . 2

1.2 About AIAC . . . 2

2 Executive Overview 3

2.1 Scope . . . 3

2.2 Risk Classification . . . 3

2.3 Finding Summary . . . 3

3 Findings 4

3.1 (RS-01) Bridge whitelist blocks on-chain bots from balancing the token prices on different chains . 4

1 Introduction

ai.ac engaged RigSec to conduct a comprehensive security assessment of their smart contracts from July 28, 2025 to July 31, 2025. The purpose of this audit was to ensure the security and reliability of the smart contracts implemented by ai.ac.

1.1 About RigSec

RigSec is a blockchain regulatory technology company with a strong presence across Singapore, Hong Kong, Taiwan, and Japan. We are dedicated to providing regulatory-compliant digital asset wallet solutions and security consulting services.

With a focus on ensuring the integrity and resilience of blockchain technologies, we work closely with clients to identify and mitigate potential vulnerabilities within their systems. Our team of experts combines extensive knowledge of blockchain technology with a proactive approach to security, enabling us to provide comprehensive assessments and recommendations.

Through our meticulous audits of smart contracts and implementation of regulatory-compliant wallet solutions, RigSec helps clients protect their valuable digital assets and maintain the trust of their stakeholders.

1.2 About AIAC

ai.ac enables every Business Intelligent Agents to autonomously finance, operate, evolve, and collaborate with humans and other agents, driving a new era of economic interaction.

Connect on X - https://x.com/me_aiac

Follow MIA on X - https://x.com/mwa_ia

2 Executive Overview

The team of 3 consultants from RigSec meticulously examined the smart contracts provided by AIAC team. This process involved a thorough analysis of the codebase, including static and dynamic testing. The consultants employed both automated and manual processes to test the security of the codebase.

2.1 Scope

The security assessment was scoped to the following project repository:

https://github.com/aiac-platform/aiac-smart-contracts

Commit hash: 773ac191e01c7e4937c11e43b0f5cf1afe8755bc

Files in scope:

- contracts/layerzero/AgentTokenOFT.sol
- contracts/layerzero/AgentTokenAdapter.sol

2.2 Risk Classification

RigSec uses a risk classification matrix to determine the risk of a found issue. The matrix is based on the likelihood of the issue occurring and the impact of the issue. The risk classification is based on the following matrix:

Table 1: Risk Classification

Risk	Impact - High	Impact - Medium	Impact - Low
Likelihood - High	Critical	High	Medium
Likelihood - Medium	High	Medium	Low
Likelihood - Low	Medium	Low	Informational

2.3 Finding Summary

Table 2: Summary of Findings

Critical	High	Medium	Low	Informational
0	0	0	0	1

3 Findings

3.1 (RS-01) Bridge whitelist blocks on-chain bots from balancing the token prices on different chains

Severity: Informational
Status: Acknowledged

Description

A whitelist is employed when bridging tokens. If enabled, only whitelisted addresses can bridge tokens and on-chain bots will not be able to help balance the prices between different chains, resulting in potential price differences for the same token across different chains.

Listing 1: contracts/layerzero/AgentTokenAdapter.sol

```
function _debit(
    address _from,
    uint256 _amountLD,
    uint256 _minAmountLD,
    uint32 _dstEid
) internal override returns (uint256 amountSentLD, uint256 amountReceivedLD) {
    // Whitelist check
    if (whitelistEnabled) {
        require(whitelist[_from], "AgentTokenAdapter: sender not whitelisted");
    }

    // Call parent implementation
    return super._debit(_from, _amountLD, _minAmountLD, _dstEid);
}
```

Recommendation

Disable the whitelist if you want to allow on-chain bots to balance the prices of tokens across different chains.