# LayerZero Labs Security Audit

*LZEndpointDollar*

Released February 6, 2026

**Performed By**

| | |
|---|---|
| Carter Snay | csnay@iol.unh.edu |
| James Kahn | jkahn@iol.unh.edu |
| Oliver Willis | owillis@iol.unh.edu |

University of New Hampshire
Interoperability Labs

+1-603-862-0090 | www.iol.unh.edu

# Table of Contents

# 1 Legal Notice

The Interoperability Labs Blockchain team makes every effort to identify as many vulnerabilities in the code as possible within the given time period but assumes no responsibility for the findings presented in this document. A security audit by the team does not constitute an endorsement of the underlying business or product. The audit was time-boxed, and the review focused solely on the security aspects of the Solidity implementation of the contracts.

# 2 Executive Summary

The UNH Interoperability Labs conducted a security assessment for LZEndpointDollar from January 21, 2026 to Feburary 6, 2026. During this assessment, The UNH Interoperability Labs reviewed the LayerZero Labs LZEndpointDollar code for security vulnerabilities, design issues and general weaknesses.

During the assessment, 0 findings were identified by the team.

## 2.1 About LayerZero and LZEndpointDollar

LayerZero is an omnichain interoperability protocol designed to facilitate seamless messaging of arbitrary data between blockchains. It achieves this by leveraging a combination of on-chain endpoints, a decentralized network of verifiers, and executors to securely transmit messages across chains. The protocol enables cross-chain applications to maintain atomicity and composability across multiple networks.

Tempo has no native token, choosing instead to pay for gas and priority fees using TIP-20 stablecoins. LZEndpoints require a singular native token or alternative token for handling fees. LayerZero Labs created `LZEndpointDollar`, a ERC20 token basket contract to wrap whitelisted tokens on the Tempo blockchain. The purpose of the `LZEndpointDollar` contract is to act as the standard token for the LZEndpoint deployed on Tempo.

Core permissioned features of the `LZEndpointDollar` contract include upgradeability, burnability, emergency withdrawal and whitelisting of underlying wrapped ERC20 tokens. `LZEndpointDollar` supports freezing the underlying tokens in the contract by removing the corresponding tokens from the whitelist. The `LZEndpointDollar` tokens are minted when whitelisted tokens are wrapped, and conversely the tokens are burned when unwrapped. Direct burning of `LZEndpointDollar` tokens can only be performed by the owner of the contract.

### 2.1.1 Review Timeline

- **January 21, 2026**: Initial Audit Scope Review
- **January 23, 2026**: Audit draft report delivered
- **January 28, 2026**: Second audit draft report delivered
- **Feburary 6, 2026**: Final Audit report delivered

### 2.1.2 Scope

| | | | |
|---|---|---|---|
| **Project Name** | LZEndpointDollar | | |
| **URL** | `https://layerzero.network/` | | |
| **Language** | Solidity | | |
| **Scope** | Repo | `https://github.com/LayerZero-Labs/EndpointToken` | |
| | Hash | ~~e08e5d9405ee205610dc9eb69b2ff2e9323fe7a3~~ | January 20, 2026 |
| | | b701948190200aada99f33565a7042ea70db306c | January 27, 2026 |

**Files in Scope**

```
src/
 ├─interfaces/
 │   └─ILZEndpointDollar.sol
 └─LZEndpointDollar.sol
```

# 3 Vulnerabilities

During the audit, no vulnerabilities were found in the provided `LZEndpointDollar` scope.

| Severity | Count |
|---|---|
| critical | 0 |
| high | 0 |
| medium | 0 |
| low | 0 |
| info | 0 |
| gas | 0 |

# Appendix A: Our Methodology

The Interoperability Labs audit team follows a comprehensive methodology in ensuring the security and reliability of smart contracts and Web3 protocols. While the specific testing procedures performed vary between the project and protocol, the tooling and manual review process remains the same to ensure thorough analysis has been completed on all items within the defined scope of the audit. Throughout the security review, the audit team maintains communication with the development team, providing feedback on identified vulnerabilities and optimizations. The following sections provide an overview of our systematic audit process and methodology.

## Risk Classification

Impact

Likelihood

| | Informational | Low | Medium | High | Critical |
|---|---|---|---|---|---|
| Very Unlikely | Info | Low | Low | Medium | Critical |
| Unlikely | Info | Low | Low | Medium | Critical |
| Possible | Info | Low | Medium | High | Critical |
| Likely | Info | Low | Medium | High | Critical |
| Very Likely | Low | Medium | High | Critical | Critical |

The PricewaterhouseCoopers-style matrix is used to provide a comprehensive risk assessment.

## Review Phases

### Phase I: Initial Scoping

- Independent review of project documentation to understand the business logic of the project.
- Identification of critical components and key areas of focus and possible areas of exploitation.
- Ensure that the project's documentation is accurate, complete, understandable, and there is alignment between the code and the documentation.
- Discussion with the development team to clarify objectives, expectations, and known issues.

### Phase II: Codebase Review

- **Static Analysis**: Automated tools to scan for common vulnerabilities with Slither and Aderyn.
- **Manual Review**: In-depth inspection of the code by the audit team to identify issues, including unsafe coding practices from known previous exploits.
- **Function State Machine Diagramming**: Generate a flow diagram illustrating the intended transaction paths, as well as unintended and potentially exploitable paths.

## Phase III: Local Testing

**Methods:**

- **Unit Testing**: Validate individual functions for correctness.
- **Integration Testing**: Ensure that different components interact as expected.

**Techniques Used in This Audit:**

- **Unit Testing**
- **Manual Review**
- **Function State Machine Diagramming**

## Proof of Vulnerability

**Objective:** Prove how a found exploit can be executed.

**Activities:**

- Perform controlled attacks on a local fork of the protocol to show how an exploit can be executed.
- Test edge cases and unexpected scenarios discovered in the diagramming phase.

By following a structured and comprehensive methodology, we aim to provide actionable insights to strengthen the security and reliability of the protocol. This ensures security, resilience, and long-term success for the protocol.

# Appendix B: The Interoperability Labs

The University of New Hampshire Interoperability Labs (UNH-IOL) is the foremost independent testing facility for data networking companies worldwide.

We accelerate the launch of innovative products by providing standards and compliance testing to ensure that devices meet industry standards. Whether it's traditional Ethernet or advanced technologies like 5G, blockchain, and autonomous vehicles, our services provide comprehensive testing for device interoperability, conformance, and certification.

Our state-of-the-art laboratory and 36 years of extensive experience make it a strategic resource for industry startups and Fortune 500 companies needing collaboration, innovation, and standards development to help them shape the future of networking.

Join us and become a part of a community driving the next generation of networking technology. Together, we can shape the future of networking.

https://www.iol.unh.edu/membership

University of New Hampshire Interoperability Laboratory

21 Madbury Rd., Ste 100 Durham, NH 03824-4716

+1-603-862-0090 | www.iol.unh.edu

Contact our Blockchain Team: `blockchain@iol.unh.edu`