



# SECURITY ASSESSMENT

Provided by Accretion Labs Pte Ltd. for Light Protocol  
January 21, 2025  
A24LIG1



Light Protocol

## AUDITORS

Role	Name
Lead	Robert Reith (robert@accretion.xyz)

## CLIENT

**Light Protocol** (<https://lightprotocol.com>) engaged Accretion to conduct a security assessment of two pull requests that extend the functionality of the Light ZK compression protocol. The first PR adds a new wrapper instruction to the token compression program. The second PR adds Token22 support to the same program.

## ENGAGEMENT SCOPE

### New Wrapper Compression Instruction

**Link:** <https://github.com/Lightprotocol/light-protocol/pull/1361>

**Commit:** 6be1bda2cb538db69f34efdd0feca40997194b5f

**ProgramID:** cTokenmWW8bLPjZEBaUgYy3zKxQZW6VKi7bqNFEVv3m

### Added Token22 Support

**Link:** <https://github.com/Lightprotocol/light-protocol/pull/1344>

**Commit:** cdbfbd8cc518e76714c0eaff224dee7c229d8ca3

**ProgramID:** cTokenmWW8bLPjZEBaUgYy3zKxQZW6VKi7bqNFEVv3m

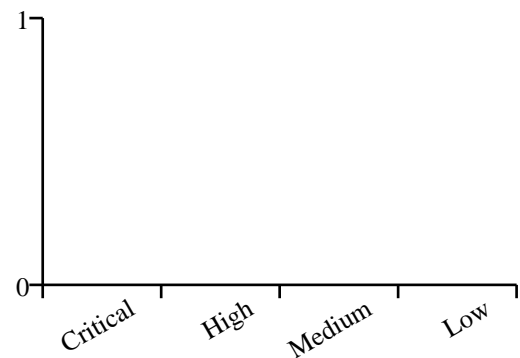
## ENGAGEMENT TIMELINE



## ASSESSMENT

The security assessment of Light Protocol's two pull requests revealed a well-structured update with robust security measures in place. The PRs, which were relatively small in size, **did not yield any new security vulnerabilities**. Overall, the Light Protocol team demonstrated strong adherence to best practices in protocol development. A few minor recommendations were identified and promptly addressed during the review period.

## SEVERITY DISTRIBUTION



## VERIFIED ON-CHAIN CODE

### Program 1

**ProgramID:** cTokenmWW8bLPjZEBaUgYy3zKxQZW6VKi7bqNFEVv3m

**Repository:** <https://github.com/Lightprotocol/light-protocol>

**Build Hash:** d7c58e2f97e8d192f8480de1bc23f9f6e19ca0d969369a46e8ad565fa4df1d81

**Commit:** 0a42c44b0f6aaf7c9f793c970455c188f5f7f103

## APPENDIX

### Vulnerability Classification

We rate our issues according to the following scale. Informational issues are reported informally to the developers and are not included in this report.

Severity	Description
<b>Critical</b>	Vulnerabilities that can be easily exploited and result in loss of user funds, or directly violate the protocol's integrity. Immediate action is required.
<b>High</b>	Vulnerabilities that can lead to loss of user funds under non-trivial preconditions, loss of fees, or permanent denial of service that requires a program upgrade. These issues require attention and should be resolved in the short term.
<b>Medium</b>	Vulnerabilities that may be more difficult to exploit but could still lead to some compromise of the system's functionality. For example, partial denial of service attacks, or such attacks that do not require a program upgrade to resolve, but may require manual intervention. These issues should be addressed as part of the normal development cycle.
<b>Low</b>	Vulnerabilities that have a minimal impact on the system's operations and can be fixed over time. These issues may include inconsistencies in state, or require such high capital investments that they are not exploitable profitably.
<b>Informational</b>	Findings that do not pose an immediate risk but could affect the system's efficiency, maintainability, or best practices.

### Audit Methodology

Accretion is a boutique security auditor specializing in Solana's ecosystem. We employ a customized approach for each client, strategically allocating our resources to maximize code review effectiveness. Our auditors dedicate substantial time to developing a comprehensive understanding of each program under review, examining design decisions, expected and edge-case behaviors, invariants, optimizations, and data structures, while meticulously verifying mathematical correctness—all within the context of the developers' intentions.

Our audit scope extends beyond on-chain components to include associated infrastructure, such as user interfaces and supporting systems. Every audit encompasses both a holistic protocol design review and detailed line-by-line code analysis.

During our assessment, we focus on identifying:

- Solana-specific vulnerabilities
- Access control issues
- Arithmetic errors and precision loss
- Race conditions and MEV opportunities
- Logic errors and edge cases
- Performance optimization opportunities
- Invariant violations
- Account confusion vulnerabilities
- Authority check omissions
- Token22 implementation risks and SPL-related pitfalls
- Deviations from best practices

Our approach transcends conventional vulnerability classifications. We continuously conduct ecosystem-wide security research to identify and mitigate emerging threat vectors, ensuring our audits remain at the forefront of Solana security practices.