Accretion

SECURITY ASSESSMENT

Provided by Accretion Labs Pte Ltd. for Light Protocol
January 22, 2025
A25LIG1

Light Protocol

AUDITORS

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

CLIENT

Light Protocol (https://lightprotocol.com/) engaged Accretion to conduct a security assessment of a pull request and multiple commits extending the Light ZK compression protocol. The new functionality adds the ability to have multiple token pool PDAs instead of just one per mint to reduce writelocks on the same accounts.

ENGAGEMENT SCOPE

New feature implementing multiple tokenPoolPda accounts per mint

Link: https://github.com/Lightprotocol/light-protocol/pull/1407
Commit: c385d63bd0ac2105f65e1b12b18a5a167682547f
ProgramID: cTokenmWW8bLPjZEBAUgYy3zKxQZW6VKi7bqNFEVv3m

Commits amending PR 1407

Link: https://github.com/Lightprotocol/light-protocol
Commit: 39262bad79d76d1c8e5685c2db420ac98898b186
b2f993c9789c974917182f87d2d5b1af93e0dc7d
abef3084e3c9e79429eeac6513824b1c8e7350a9
f648104d377bae9741ea1b8be6be2a5b4fe3b724
ProgramID: cTokenmWW8bLPjZEBAUgYy3zKxQZW6VKi7bqNFEVv3m

ENGAGEMENT TIMELINE

01 Jan — Project Kickoff
Initial planning and scope definition

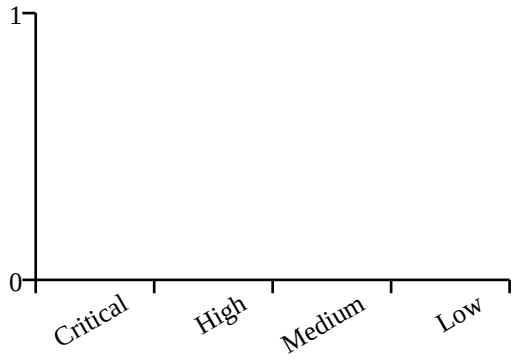
02 Jan — Assessment Begins
Security review and testing phase

03 Jan — Assessment Completion
Assessment completed

ASSESSMENT

The security assessment of Light Protocol's PR request and commits revealed a sound new feature that should improve the protocol's performance in the future. The relatively small update **did not yield any new security vulnerabilities**. The Light protocol team again demonstraded strong adherence to best practices in protocol development. A few minor recommendations were identified and shared with the Light protocol team during the assessment.

SEVERITY DISTRIBUTION



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
Critical	Vulnerabilities that can be easily exploited and result in loss of user funds, or directly violate the protocol's integrity. Immediate action is required.
High	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.
Medium	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.
Low	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.
Informational	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.