SECURITY ASSESSMENT

Provided by Accretion Labs Pte Ltd. for Light Protocol

June 19, 2025

A25LIG2

Accretion

Light Protocol

AUDITORS

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

CLIENT

Light Protocol (https://lightprotocol.com/) builds a ZK compression layer on top of the Solana blockchain. They engaged Accretion Labs to audit an update which updates the system program to pinocchio, and adds multiple other CU optimizations to the programs. These updates also include read only account instructions, changes to hashing internals, and multiple small changes for minor optimizations.

ENGAGEMENT SCOPE

Programs: System, Compression, Registry

Link: https://github.com/Lightprotocol/light-protocol

Commit: 2a6ff8c6c1052c836133cadce9794c4f94a7a2dd

ProgramID:

SySTEM1eSU2p4BGQfQpimFEWWSC1XDFeun3Nqzz3rT7,

compr6CUsB5m2jS4Y3831ztGSTnDpnKJTKS95d64XVq,

Lighton6oQpVkeewmo2mcPTQQp7kYHr4fWpAgJyEmDX

ENGAGEMENT TIMELINE

22 Apr	Project Kickoff	Initial planning and scope definition
22 Apr	Assessment Begins	Security review and testing phase
04 Jun	Review Fixes	Security recommendations are given and implemented
19 Jun	Project Completion	Report delivery and on-chain confirmation

ASSESSMENT

The Light Protocol upgrade demonstrated excellent code quality with strong engineering and thorough testing. We weren't able to find any security issues in the codebase and the team was very responsive to our feedback. The changes made to the system program and other programs were well thought out and implemented, resulting in a more efficient protocol.

SEVERITY DISTRIBUTION
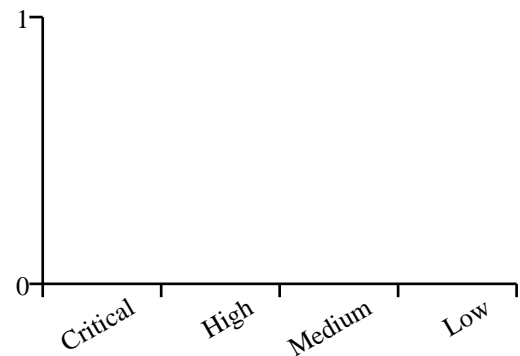
AUDITED CODE

Program 1

ProgramID: SySTEM1eSU2p4BGQfQpimFEWWSC1XDFeun3Nqzz3rT7

Repository: https://github.com/Lightprotocol/light-protocol

Commit: 053c4a0bb9699007c7a1fc0c37fe4642752aef79

Program 2

ProgramID: compr6CUsB5m2jS4Y3831ztGSTnDpnKJTKS95d64XVq

Repository: https://github.com/Lightprotocol/light-protocol

Commit: 053c4a0bb9699007c7a1fc0c37fe4642752aef79

Program 3

ProgramID: Lighton6oQpVkeewmo2mcPTQQp7kYHr4fWpAgJyEmDX

Repository: https://github.com/Lightprotocol/light-protocol

Commit: 053c4a0bb9699007c7a1fc0c37fe4642752aef79

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.