Trail of Bits
228 Park Ave S #80688
New York, NY 10003

Jim Miller
Engineering Director
james.miller@trailofbits.com
www.trailofbits.com

March 25, 2025

Scroll

Scroll engaged Trail of Bits to review the security of the changes introduced during phase 2 of the Euclid upgrade. These changes add enforced transactions and enforced batches, as well as restructuring block information from calldata to blobs, with associated changes to the zero-knowledge chunk and batch circuits.

A team of three consultants conducted the review from March 6 to March 21, 2025, for a total of four engineer-weeks of effort. Our testing efforts focused on assessing the soundness and correctness of the changes made to the chunk and batch circuits, the soundness of the enforced liveness mechanism, and whether the rollup contract correctly handles version 7 batches. With full access to source code and documentation, we performed static and dynamic testing of the codebase, using automated and manual processes.

Our audit uncovered one low-severity issue and four informational issues.

We did not uncover any soundness or completeness issues in the changes made to the chunk, batch, and bundle circuits. However, we identified one potentially impactful but difficult-to-exploit supply-chain issue in the use of GitHub actions in the `zkvm-prover` repository.

We did not uncover any issues in the smart contract logic that would adversely affect the confidentiality, integrity, or availability of the system. The updates have sufficient data validation, access controls, and testing to ensure liveness and support the processing of v7 batches.

Sincerely,
Jim Miller