Trail of Bits: what a resolved finding can mean

The Kiln Lagoon vault report separates project coverage and fix review, but its resolution narratives require more care than a status total.

DSA research, prepared with AI assistance

Published September 5, 2026 | Version 1.0

Public-source research; independent expert review pending

This document reviews cited public evidence. It is not a code audit, a certification, or an endorsement by an appointed expert panel.

Measurements in this report

Version hashes listed in project targets	3
Detailed findings and fix-review entries	2
Resolution narratives based on intended behavior	1
Resolution narratives referencing a code change	1

Read online: https://defisec.info/reports/trail-of-bits-evidence-review-2026

Evidence coverage against the seven criteria

All scores are withheld. These are source-evidence observations, not independent technical assessments.

Technical finding quality | Not scored

Published finding narratives available. Exploits have not been reproduced by DSA.

Depth and threat model | Not scored

Scope and method material available. Test adequacy and omitted threats need expert review.

Scope and version traceability | Not scored

Version or deployed-address anchors are recorded. Independent repository/build validation is pending.

Demonstrated specialization | Not scored

Sampled projects identify relevant technologies. Assigned-team fit remains unverified.

Fix verification | Not scored

Resolution narratives inspected. Accepted risk is kept separate from a verified code fix.

Internal quality control and response | Not scored

No independent internal QA workpapers inspected.

Transparency and conflicts | Not scored

Public identity sources are available. Reviewer and commercial conflict declarations have not been collected.

Sample and method

From the official reports index, we selected the PDF with the most recent month encoded in the visible 2026 report filenames: the May 2026 Kiln Lagoon vault review. The document is dated May 11, 2026 and covers version 0.6.0. This deterministic filename selection is an access sample, not a claim that no newer private or differently indexed report exists.

Original evidence inventory

We manually checked the project-targets and fix-review sections after extracting the PDF text. The targets section contains three version hashes associated with the main vault and additional change sets. It names Solidity and EVM. The coverage section explains which paths were examined, including fee arithmetic, storage and upgrade behavior and the sanctions-list integration.

The PDF includes two detailed findings and two fix-review entries. Both entries are labeled resolved. That label alone would produce a misleading impression if interpreted as two code defects fixed and retested.

Resolution is broader than a code change

One finding concerns user operations failing when a sanctions-list dependency reverts. The fix-review narrative records that the client regarded this behavior as intended, because it preserves the sanctions restriction. The other finding concerns calculating an entry fee in the wrong unit and references a corrective pull request.

Our classification is therefore one resolution based on intended behavior and one resolution linked to a code change, within a two-finding sample. This is an interpretation of the published narratives, not an independent judgment that either decision is correct for another deployment. It illustrates why reviewers must read accepted-risk and design-intent explanations rather than count green status labels.

What a buyer can learn

The report makes the review's scope and follow-up visible and gives a potential buyer concrete material for a technical interview. Ask an assigned reviewer to explain how they distinguish asset units from share units and how external-policy dependencies enter the threat model. Then ask how changes after the assessed version affect the engagement.

For a committee assessment, request two more recent relevant project reports, reproducibility material for a material finding and the final revision associated with each fix. A single published vault review is insufficient to score the entire provider and the original engagement's effort should not be treated as an estimate for a different codebase.

Expanded five-project packet

We also inspected target and outcome sections for Ripple XRP Ledger confidential transfers, Gensyn ERC-20, Franklin Templeton BenjiSwap and Shape Tokenlock. Together with Kiln, these are five distinct projects. All identify versioned targets. Four include a dedicated fix-review section. The Gensyn report has no such section and describes a short assessment without a reported finding; its absence is not automatically a process failure. Its filename contains April 2026, but the document itself is dated September 26, 2025. The packet preserves both dates instead of treating a filename as the engagement date.

Limits and next verification step

This is a bounded review of public evidence. We did not rerun exploits, inspect private workpapers, interview the assigned audit team or verify current booking availability. The observations describe the cited artifacts and cannot establish the provider's overall defect-detection rate. A procurement decision still needs a scoped proposal, relevant recent work and independent technical review.

Sources and reproducibility

All source checks were made on September 5, 2026. Content hashes identify the retrieved artifacts. Data definitions and the source manifest are available from the report page and the link below.

1. Kiln Lagoon Vault v0.6.0 security assessment

Official source: raw.githubusercontent.com

SHA-256: ce300c02223b89be2686a74e2b4eca67ab993dc12f744575f1927c12ba34e38b

2. Official report index

Official source: www.trailofbits.com

SHA-256: ac5ed62a6753c30bfcf2f90fb80c3de964ecb2e015e259e3f6f960ee4a11ef60

3. 2026 04 ripple labs xrp ledger confidential transfer securityreview.pdf

Official source: raw.githubusercontent.com

SHA-256: ea38f093f477225884f91707ec44a1f74bcc72ef80e795f44cb6d58b4856c70f

4. 2026 04 gensyn erc 20 token securityreview.pdf

Official source: raw.githubusercontent.com

SHA-256: b8affdca20bd8afccb1140587dec2c5c03f95a8a901a9fd8b5d238b5de3666a7

5. 2026 04 franklintempleton benjiswapdifferentialreview securityreview.pdf

Official source: raw.githubusercontent.com

SHA-256: 00b4d390152963b829bfb40f1ed03a1d9333396a70bd7c0da8d8f6b3036f54f0

6. 2026 03 shape tokenlock securityreview.pdf

Official source: raw.githubusercontent.com

SHA-256: 89c7103c80b3ac351ccca7f432a02a4551943d13bccc8d4d1779d0aead55223b

Data and methodology

https://defisec.info/downloads/research/evidence-measurements-2026-09-05.json

Selection rules, HTTP results, source hashes, and original counts are recorded in the accompanying data. The research used AI assistance. No independent technical committee review is claimed.

https://defisec.info/methodology