AGORA

Post-Quantum Security Audit Pack

Program: /home/king_d/solana/testing/klend

Scan date: 2026-05-24T04:39:51.757238772+00:00

Tool: Pinpoint SPECTRE 1.2.2

CONFIDENTIAL. For authorised recipients only.

Executive Summary

Total findings: 35

Cryptographic components inventoried (CBOM 1.6): 33

Findings by rule: CA-001=0, CA-002=33, CA-003=0, CA-004=0

CA-005: not applicable. PDAs are quantum-safe by construction.

Findings

CA-002

programs/klend/src/handlers/handler_abort_obligation_ownership_transfer.rs:33 | sev=Medi
programs/klend/src/handlers/handler_accept_obligation_ownership_transfer.rs:43 | sev=Med
programs/klend/src/handlers/handler_approve_obligation_ownership_transfer.rs:38 | sev=Me
programs/klend/src/handlers/handler_borrow_obligation_liquidity.rs:173 | sev=Medium | Si
programs/klend/src/handlers/handler_cancel_withdraw_ticket.rs:110 | sev=Medium | Single-
programs/klend/src/handlers/handler_deposit_obligation_collateral.rs:111 | sev=Medium |
programs/klend/src/handlers/handler_deposit_reserve_liquidity.rs:102 | sev=Medium | Sing
programs/klend/src/handlers/handler_deposit_reserve_liquidity_and_obligation_collateral.
programs/klend/src/handlers/handler_enqueue_to_withdraw.rs:177 | sev=Medium | Single-sig
programs/klend/src/handlers/handler_flash_borrow_reserve_liquidity.rs:65 | sev=Medium |
programs/klend/src/handlers/handler_flash_repay_reserve_liquidity.rs:106 | sev=Medium |
programs/klend/src/handlers/handler_init_farms_for_reserve.rs:33 | sev=Medium | Single-s
programs/klend/src/handlers/handler_init_lending_market.rs:23 | sev=Medium | Single-sign
programs/klend/src/handlers/handler_init_obligation.rs:42 | sev=Medium | Single-signer a
programs/klend/src/handlers/handler_init_user_metadata.rs:34 | sev=Medium | Single-signe
programs/klend/src/handlers/handler_initiate_obligation_ownership_transfer.rs:44 | sev=M
programs/klend/src/handlers/handler_mark_obligation_for_deleveraging.rs:26 | sev=Medium
programs/klend/src/handlers/handler_redeem_reserve_collateral.rs:98 | sev=Medium | Singl
programs/klend/src/handlers/handler_repay_obligation_liquidity.rs:116 | sev=Medium | Sin
programs/klend/src/handlers/handler_request_elevation_group.rs:71 | sev=Medium | Single-
programs/klend/src/handlers/handler_set_borrow_order.rs:50 | sev=Medium | Single-signer
programs/klend/src/handlers/handler_set_obligation_order.rs:14 | sev=Medium | Single-sig
programs/klend/src/handlers/handler_socialize_loss.rs:89 | sev=Medium | Single-signer au
programs/klend/src/handlers/handler_update_global_config.rs:30 | sev=Medium | Single-sig
programs/klend/src/handlers/handler_update_global_config_admin.rs:14 | sev=Medium | Sing
programs/klend/src/handlers/handler_update_lending_market_owner.rs:20 | sev=Medium | Sin
programs/klend/src/handlers/handler_update_obligation_config.rs:39 | sev=Medium | Single
programs/klend/src/handlers/handler_withdraw_obligation_collateral.rs:103 | sev=Medium |
programs/klend/src/handlers/handler_withdraw_obligation_collateral_and_redeem_reserve_co
programs/klend/src/state/nested_accounts.rs:24 | sev=Medium | Single-signer authority `o
programs/klend/src/state/nested_accounts.rs:34 | sev=Medium | Single-signer authority `o
programs/klend/src/state/nested_accounts.rs:54 | sev=Medium | Single-signer authority `o
programs/klend/src/state/nested_accounts.rs:82 | sev=Medium | Single-signer authority `o

NIST IR 8547 Traceability Matrix

Maps each audit-pack section to a NIST IR 8547 post-quantum transition phase.

Phase	Rule(s)	Finding Count
Inventory	CA-001	0
Risk Prioritisation	CA-002, CA-003, CA-004	33
Hybrid Deployment	(no rules at this release)	n/a
Full Migration	(no rules at this release)	n/a

Hybrid Deployment and Full Migration are documented for framework completeness.
No CA rule fires for those phases at this release. Coverage expands in Tier 2.

Methodology

Pre-pass: Anchor expand subprocess invoked before tree-sitter walks source.

Expanded output is cached per program hash to avoid redundant re-expansion.

OtterSec downstream framing: CA-003 cross-program assumption findings surface migration cascade complexity following OtterSec's CPI-trust analysis framework.

CA-005 dropped: PDAs are quantum-safe by construction. Off-curve points derived via SHA-256 have no Ed25519 private key, so the Grover speedup falls beyond the attack horizon. Confirmed with Jump Crypto and Helius.

CA-004 is inventory and exposure only. It does not prescribe a hybrid Falcon co-signer. Protocol-layer migration (address format, ZK proof of Ed25519 seed) is owned by Anza and Firedancer, not by individual program developers.

Rule pack: pinpoint-rules-pq v0.1.0. CBOM format: CycloneDX 1.6.

PDF renderer: printpdf (pure Rust, no system library dependency).