AGORA

Post-Quantum Security Audit Pack

Program: /home/king_d/solana/testing/drift

Scan date: 2026-05-24T04:40:29.077438487+00:00

Tool: Pinpoint SPECTRE 1.2.2

Executive Summary

Total findings: 143

Cryptographic components inventoried (CBOM 1.6): 161

Findings by rule: CA-001=0, CA-002=136, CA-003=0, CA-004=0

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

Findings

CA-002

programs/drift/src/instructions/admin.rs:5251 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5315 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5325 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5393 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5407 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5419 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5458 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5472 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5483 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5493 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5516 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5536 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5558 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5572 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5584 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5598 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5609 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5628 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5645 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5671 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5705 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5729 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5734 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5747 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5754 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5767 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5781 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5789 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5804 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5828 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5839 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5850 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5870 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5887 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5911 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5930 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5984 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:5998 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:6010 | sev=Medium | Single-signer authority `ad
programs/drift/src/instructions/admin.rs:6020 | sev=Medium | Single-signer authority `ad

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	136
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).