AGORA

Post-Quantum Security Audit Pack

Program: /home/king_d/solana/testing/marinade

Scan date: 2026-05-24T04:38:41.796862491+00:00

Tool: Pinpoint SPECTRE 1.2.2

Executive Summary

Total findings: 52

Cryptographic components inventoried (CBOM 1.6): 26

Findings by rule: CA-001=0, CA-002=17, CA-003=0, CA-004=0

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

Findings

CA-002

programs/marinade-finance/src/instructions/admin/change_authority.rs:16 | sev=Medium | S
programs/marinade-finance/src/instructions/admin/config_lp.rs:24 | sev=Medium | Single-s
programs/marinade-finance/src/instructions/admin/config_marinade.rs:34 | sev=Medium | Si
programs/marinade-finance/src/instructions/admin/config_validator_system.rs:13 | sev=Med
programs/marinade-finance/src/instructions/admin/emergency_pause.rs:17 | sev=Medium | Si
programs/marinade-finance/src/instructions/admin/realloc_stake_list.rs:16 | sev=Medium |
programs/marinade-finance/src/instructions/admin/realloc_validator_list.rs:16 | sev=Medi
programs/marinade-finance/src/instructions/delayed_unstake/order_unstake.rs:27 | sev=Med
programs/marinade-finance/src/instructions/liq_pool/liquid_unstake.rs:49 | sev=Medium |
programs/marinade-finance/src/instructions/liq_pool/remove_liquidity.rs:27 | sev=Medium
programs/marinade-finance/src/instructions/management/add_validator.rs:13 | sev=Medium |
programs/marinade-finance/src/instructions/management/emergency_unstake.rs:22 | sev=Medi
programs/marinade-finance/src/instructions/management/partial_unstake.rs:28 | sev=Medium
programs/marinade-finance/src/instructions/management/remove_validator.rs:22 | sev=Mediu
programs/marinade-finance/src/instructions/management/set_validator_score.rs:18 | sev=Me
programs/marinade-finance/src/instructions/user/deposit_stake_account.rs:35 | sev=Medium
programs/marinade-finance/src/instructions/user/withdraw_stake_account.rs:46 | sev=Mediu

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	17
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).