JELLEO | AUTONOMOUS SOLANA AUDIT

AUDIT REPORT · CYCLE 20260428-213920

Hunt cycle · default.

AUDITOR	Kirill Sakharuk · kirill@jelleo.com
CUSTOMER	default
WINDOW	cycle 20260428-213920
CYCLE	20260428-213920
ENGINE SHA	a946e5508f
WRAPPER SHA	5fcf0fc2eb
GENERATED	2026-05-08T22:32:49+00:00

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

CONFIRMED · DISCLOSED · FIXED · VERIFIED

16 REJECTED (FALSE POSITIVE)

SIGNED · ED25519

MCowBQYDK2VwAyEAvCFSLBecPuNClei48PWjHuelHlBX9uYZo4wELbQ7b+k=

verify with `audit-pipeline sign verify <file> <file>.sig --pubkey jelleo.ed25519.pub`
public key at
https://jelleo.com/keys/jelleo.ed25519.pub

PLATFORM · V0.1

JELLEO · The underwriting layer for Solana DeFi.

Methodology	jelleo.com/methodology.html
Disclosure	jelleo.com/security.html
Source	github.com/Copenhagen0x/audit-pipeline-cli

Apache-2.0 · contact security@jelleo.com

default · hunt cycle

`20260428-213920` · started 2026-04-28T22:24:24+00:00 · engine `a946e5508f` · wrapper `5fcf0fc2eb`

01 — CYCLE SUMMARY

CRITICAL	HIGH	MEDIUM	CONFIRMED
4	5	6	0

TOTAL VERDICTS: 16

Critical 4 · High 5 · Medium 6 · Low 1 · Info 0

02 — FINDINGS

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
CRITICAL	`L4-keeper-authorization-surface`	Every public/permissionless instruction that reaches use_insurance_buffer requires either an admin signer OR cannot drai	FALSE / HIGH	REJECTED	—
CRITICAL	`V2-vault-balance-equation`	For every market state transition, the change in vault balance equals the sum of (cash deposited into orderbook + claima	UNKNOWN / HIGH	REJECTED	—
CRITICAL	`CI1-deposit-then-withdraw-zero`	Deposit X immediately followed by withdraw X (with no intervening activity) leaves vault + account-state byte-identical	FALSE / HIGH	REJECTED	—
CRITICAL	`IX6-account-owner-check`	Every account read by the program verifies the account's `owner` field matches the expected program_id, preventing fake-	FALSE / MED	REJECTED	—
HIGH	`L1-liquidation-discount-bounded`	Liquidation bonus paid to a liquidator cannot exceed the configured LIQUIDATION_INCENTIVE_PCT of seized collateral, even	UNKNOWN / LOW	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
HIGH	`O3-position-authority-binding`	An account's `position_q` and `claimable_pnl` can only be mutated when the account's bound authority signs (or via permi	FALSE / HIGH	REJECTED	—
HIGH	`P9-pnl-arithmetic-bounds`	The lazy mark-to-market computation pnl_delta = abs_basis * (K_now - K_snap) / (a_basis * POS_SCALE) cannot overflow i12	UNKNOWN / HIGH	REJECTED	—
HIGH	`S7-epoch-staleness-gate`	Risk gates that depend on per-epoch state (e.g., funding-window mark) reject when the captured epoch is stale relative t	UNKNOWN / HIGH	REJECTED	—
HIGH	`IX5-no-arbitrary-cpi`	The program does not invoke arbitrary CPI based on user-supplied program_id values; all CPIs are to fixed, hardcoded tar	UNKNOWN / HIGH	REJECTED	—
MEDIUM	`P10-funding-index-monotonic-modulo-direction`	Cumulative funding index changes monotonically within a continuous funding-rate sign window; flips only on rate-sign cha	FALSE / HIGH	REJECTED	—
MEDIUM	`V9-rebate-accumulation-bounded`	Maker-rebate accumulation across all accounts is bounded by the configured rebate-rate × cumulative volume; never exceed	FALSE / HIGH	REJECTED	—
MEDIUM	`A8-multisig-threshold`	If a multisig is used, threshold is enforced atomically and cannot be partially bypassed by replaying signatures.	FALSE / HIGH	REJECTED	—
MEDIUM	`CI10-resolution-final`	Once a market is resolved and all matured claims are paid, the market account can be safely closed with no residual debt	FALSE / HIGH	REJECTED	—
MEDIUM	`IX3-rent-exemption-check`	Every account allocated by the program is rent-exempt, with sysvar rent verified at allocation time.	UNKNOWN / MED	REJECTED	—
MEDIUM	`IX4-clock-sysvar-required`	Every instruction that consumes a timestamp uses the Solana clock sysvar (not a user-supplied value).	UNKNOWN / HIGH	REJECTED	—
LOW	`R3-finality-gate`	Settlement-class operations only consider state from finalized slots, never from confirmed-but-unfinalized state.	FALSE / HIGH	REJECTED	—

A — SEVERITY RUBRIC

TIER	DEFINITION
CRITICAL	Direct loss of user funds or full protocol takeover with no meaningful preconditions. Reachable from a permissionless instruction by any signer. Must be patched immediately.
HIGH	Significant loss of user funds or protocol invariant violation under realistic preconditions (specific market state, signer with limited but obtainable role). Patch should ship in next release.
MEDIUM	Hardening issue, partial loss possible, or invariant violation requiring privileged signer or improbable state. Worth fixing in normal cadence.
LOW	Minor issue with no plausible path to fund loss. Code-quality or defense-in-depth concern.
INFO	Informational. No security impact. Documentation or style suggestion.

B — METHODOLOGY

This cycle was produced by Jelleo's continuous, hypothesis-driven Solana audit loop. Every finding originates as a falsifiable invariant claim from a per-protocol hypothesis library, dispatched to multi-agent recon (Layer 1), promoted on contested verdicts via adversarial debate (Layer 1.5), and confirmed empirically via a `cargo test` proof-of-concept (Layer 2) before transitioning to `confirmed`. Confirmed findings auto-fire structural sibling derivation and cross-protocol propagation hooks, then move through a restricted lifecycle (`new → triaged → confirmed → disclosed → fixed → verified`). Every cycle is signed Ed25519 against the platform key — see the cover-page receipt.

Full spec: docs/methodology/ (eleven sections, §01–§10) · Live reference: jelleo.com/methodology.html · Inaugural disclosure: aeyakovenko/percolator-prog#39 (F7, 2026-04)