JELLEO | AUTONOMOUS SOLANA AUDIT

AUDIT REPORT · CYCLE 20260507-003500-5059332

Hunt cycle · percolator-bounty3-regression.

AUDITOR	Kirill Sakharuk · kirill@jelleo.com
CUSTOMER	percolator-bounty3-regression
WINDOW	cycle 20260507-003500-5059332
CYCLE	20260507-003500-5059332
ENGINE SHA	5059332
WRAPPER SHA	04b854e571
GENERATED	2026-05-08T22:33:14+00:00

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

CONFIRMED · DISCLOSED · FIXED · VERIFIED

5 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

percolator-bounty3-regression · hunt cycle

`20260507-003500-5059332` · started 2026-05-07T00:35:00+00:00 · engine `5059332` · wrapper `04b854e571`

01 — CYCLE SUMMARY

CRITICAL	HIGH	MEDIUM	CONFIRMED
2	3	0	0

TOTAL VERDICTS: 5

Critical 2 · High 3 · Medium 0 · Low 0 · Info 0

02 — FINDINGS

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
CRITICAL	`B57-sweep-gap-k-drift-insurance-drain`	Sweep-Gap K-Drift attack (per disclosed issue #57). KeeperCrank Phase 2 takes 64 cranks to cycle through 4096 slots. Unt	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	`B61-tradenocpi-cascade-bypass`	TradeNoCpi cascade bypass (per disclosed issue #61). Two permissionless TradeNoCpi(C, D, +/-1) calls where C/D are attac	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`B55-cursor-wrap-consumption-budget-atomic-reset`	Cursor-wrap consumption-budget atomic reset (per disclosed issue #55, follow-up to #54). At keeper_crank_not_atomic line	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`B63-keeper-crank-reward-redirect-attacker`	KeeperCrank reward redirect (per disclosed issue #63). A keeper caller whose account materialized in the same slot as th	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`B76-catchup-accrue-partial-rollback-monotonicity`	CatchupAccrue partial-mode rollback monotonicity (per disclosed issue #76). In the partial-catchup branch of Instruction	UNKNOWN / UNKNOWN	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)