JELLEO | AUTONOMOUS SOLANA AUDIT

AUDIT REPORT · CYCLE 20260428-225139

Hunt cycle · default.

AUDITOR	Kirill Sakharuk · kirill@jelleo.com
CUSTOMER	default
WINDOW	cycle 20260428-225139
CYCLE	20260428-225139
ENGINE SHA	a946e5508f
WRAPPER SHA	d163960700
GENERATED	2026-05-08T22:32:54+00:00

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

CONFIRMED · DISCLOSED · FIXED · VERIFIED

3 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

20260428-225139 · started 2026-04-28T22:51:39+00:00 · engine a946e5508f · wrapper d163960700

01 — CYCLE SUMMARY

CRITICAL	HIGH	MEDIUM	CONFIRMED
2	1	0	0

TOTAL VERDICTS
3

Critical 2 High 1 Medium 0 Low 0 Info 0

02 — FINDINGS

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
CRITICAL	SH3-k-walk-via-oracle-rejected	A sequence of two `WithdrawCollateral(decoy, amount=1)` calls at 10-slot increments, where each carries a Pyth observati	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	SH4-k-walk-via-funding-rejected	A multi-day warp under static Pyth oracle but non-zero funding rate (driven by `mark_ewma` divergence from attacker-cont	FALSE / HIGH	REJECTED	—
HIGH	SH7-mark-ewma-update-rate-cap	The wrapper's `mark_ewma_e6` update at `src/percolator.rs:6746-6776` clamps per-slot mark divergence to ≤ 49 bps/slot un	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.

TIER	DEFINITION
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)