Platform Hardening Audit

Multipass summary — August 2026

Version 1.17.0

June 2026

What this document is

In August 2026, Smooth Brains ran a structured multipass platform hardening audit across the live application: portfolio and settings, deposit and withdrawal flows, signup and wallet connect, ambassador and Fee Auto Pay, notifications (Telegram / email / in-app), chat/RAG, content surfaces, the admin site, and a careful reliability review of the execution path.

The mandate was explicit: fix real product, security, and reliability issues; treat the execution system as key intellectual property - go slow; document any change that would alter strategy, sizing, entries, exits, or gate semantics and hold those for founder approval. This public summary contains findings classes and remediation status - no exploit paths, no secrets, and no proprietary strategy parameters.

Scope and method

– Pass A - product and security harden. Auth gaps, deep-link correctness, portfolio equity display races, ambassador referral counts, Fee Auto Pay user-facing copy, chat link allowlists, private cache headers, settings Help surface, signup FAQ path.

– Pass B - admin money-path auth and alert hygiene. Manual deposit and profile-approve routes require admin role (not secret alone). Fill-drift monitoring no longer double-pings two channels for the same slippage observation.

– Pass C - adversarial verify. Independent review of Pass A/B for incomplete wiring; closed a fee-notification deep-link gap so one-tap Approve lands on the correct invoice.

Evidence standard: code review, targeted automated tests, and an internal ledger of held items. Strategy thresholds and gate fail-open/fail-closed semantics were inventoried and left unchanged unless separately approved.

Headline results

– High-severity product/security items closed in this wave include: unauthenticated Telegram link generation that could redirect a user's notification channel; Settings deep-links that ignored Ambassador / Notifications targets; portfolio overlay that could briefly paint a funded account as $0; chat that stripped legitimate Ambassador and model-portfolio links; ambassador referral counts stuck at zero; Fee Auto Pay copy that read like silent collection.

– Admin money paths hardened: forging manual deposits or approving profiles now requires an admin wallet role in addition to credentials.

– Monitoring hygiene: thin-sample and dual-channel fill-drift noise (already partially fixed earlier in August) was further reduced so Strategy Health owns fill-slippage alerts without a second parallel ping for execution-only drift.

– Fee Auto Pay truth unchanged and reinforced: Enable enrolls once; each owed fee still requires a user-signed one-tap Approve. Agents cannot move funds. No silent debit path was enabled for the fleet.

What was deliberately not changed

The following remain documented holds for separate founder review - they sit on or next to the capital path:

– Retargeting of Trading addresses on legacy link-wallet paths (ownership binding).

- Optional keeper collection modes that are not the product default (must stay allowlisted / off for the fleet).
- Coarse admin-status discovery used to bootstrap the admin UI before a signed admin session exists (super-admin detail already session-gated).
- Intent status edge cases after rare venue-fill / database write failures, and TWAP fill-deferred status wording - reliability work that needs a dedicated, explained change set.
- Strategy-facing items: permission fail-open on stale upstream permissions, feature-flag storage-miss defaults, and pre-submit drift / slippage thresholds. Measurement and alerts only; no automatic risk resize.

Relation to earlier audits

This pack complements the July 2026 pre-launch hardening audit (execution engine, stop stack, signal integrity) and the AI-assisted security audit series. It does not replace venue-level or third-party penetration testing.

Disclaimer

Point-in-time review (August 2026). Not a guarantee against future defects. Not financial advice.