

FRESH REVIEW / OCTOBER 15, 2026

Onward Presale Technical Security Review

Published website v60 | Solana mainnet | Evidence captured October 15, 2026

Conclusion

The reviewed controls passed the executed tests, and the live delivery binary matches the supplied artifact. One medium-severity capacity issue was reproduced. Launch readiness remains conditional: the separate launch-staking program is intentionally deferred and not deployed. This report does not assign an unconditional security pass.

Review outcome	Current result
Critical / high vulnerabilities	None confirmed within this review; this is not proof that none exist.
Medium findings	1 - checkout can admit more buyers than final allocation processing supports.
Validation	240 existing tests + 2 new audit tests passed; production build passed.
Production dependencies	0 known advisories returned by npm audit --omit=dev.
Launch-staking status	Deferred; deployment and fixed stake allocations remain prerequisites.

What this review covers

Fresh inspection of current website source, payment acceptance and recovery, token custody, delivery claims, staking and weekly reward logic. Read-only checks of live public APIs and finalized Solana accounts supplement local program execution and adversarial tests.

Evidence boundaries

Prior report conclusions were excluded. Findings below were established from the captured v60 source, current live reads and newly executed tests. Historical reports were retained as records. No production code, website content, balances or ownership settings were changed.

This is an AI-assisted technical review. It is not an independent third-party certification, a guarantee against loss, or verification of project identity or business claims.

01 / DEPLOYMENT & CUSTODY

What is live now

Finalized account snapshot: October 15, 2026 at 18:43:47 UTC, slot 457341743. Reserve balances were captured at slot 457341992. These are point-in-time observations.

Asset / control	Verified state
ONWARD mint	4,000,000,000 tokens; 9 decimals; standard SPL Token program; mint authority and freeze authority absent.
Presale + bonus vault	2,600,000,000 ONWARD; campaign PDA controls the token account; no delegate or close authority. Campaign state is not initialized; claims are not open.
Team vault	200,000,000 ONWARD; program-controlled custody; launch and unlock timestamps are zero; not withdrawn.
Remaining reserves	800,000,000 liquidity + 200,000,000 development + 200,000,000 listings. These accounts remain treasury-controlled, not time-locked.
Delivery program	Executable; upgrade authority absent; complete 103,104-byte deployed ELF matches the local artifact with no trailing bytes.
Launch-staking program	Expected address has no account; source feature flag is false; live endpoint returns phase=deferred.
Weekly reward distributor	Pinned immutable program deployment check passed. Beta timestamp is zero and no reward periods are listed.

Public identifiers

Mint: 3D7bV5Kog4AQcdk62GyyvqPZoUMnLqP2JKe9MCB7JTGd

Treasury: 6j8zqbxD bKaGP9tJR1ZTfsAeax6d46jKiL4DFixmB3Li

Delivery program: DCiadKRWCT7oYGDBsdjkMe3LaCSi6D5dfw4MjGJyphh1

Presale vault: AxWE1RrXUhLur1mG7XTScHZeennyceyLYc4D2NgPPTQ4

Expected launch-staking program: FZ7TUPNfnHxvtAa9ZzujYqaKCxpGR4AVsEoHJE8kMJCK

Delivery ELF SHA-256: 1316e7c1ed8100c5f8c6a02aca10d17e59676bf332b4198d253bb92808cfb252

Funding a vault does not by itself prove buyer allocations, refund rights, liquidity provisioning, or successful launch. Those dependencies are discussed on page 4.

02 / CONFIRMED FINDING

M-01: Admission exceeds finalization capacity

Severity	Status	Affected surface
Medium	Open; reproduced locally	Checkout admission and final buyer snapshot

Condition and impact

The final prefund snapshot rejects more than 16,383 distinct buyers, but quote generation and atomic purchase reservation do not enforce that same count. The sale can accept paid allocations that the current finalization code cannot process. At the threshold, the normal workflow cannot fix the buyer root and claims remain closed until processing is expanded. This is an availability/scalability defect, not a demonstrated token theft.

Reproduction

A local SQLite ledger containing 16,383 synthetic confirmed \$1 USDC purchases finalized successfully. A new wallet then received a production v3 quote, signed the payment transaction, passed `reservePurchase` and received an authenticated acceptance receipt. After marking that simulated ledger purchase confirmed and closing the sale, `finalPrefundSnapshot` refused with the 16,383-wallet capacity error.

The final confirmation in this capacity test was a synthetic database state; RPC availability and simulation were mocked. No 16,384-buyer live condition or mainnet attack is claimed. The live sale had only one recorded stake and \$1.110850 recorded contributions in the captured API response.

Evidence

server/presale.mjs: `quote()`, `RESERVE_SQL` and `reservePurchase()`; server/prefund.mjs: `finalPrefundSnapshot()`, especially the explicit wallet-count and 100,000-purchase bounds. Reproduction: `audit-evidence/fresh-audit.test.mjs`, first test; output is embedded with this PDF.

Recommended correction

Either support a larger or safely partitioned final allocation process, or enforce the supported distinct-buyer capacity atomically before accepting new payments. Include pending reservations in that limit and allow existing buyers only where purchase-count capacity also remains. Do not truncate paid buyers or simply remove proof/packet safety limits.

Retest the exact boundary, concurrent last-slot reservations, refunds, buyer and staking proofs, wallet packet size, and reward processing. The separate 100,000-purchase ceiling should also be reconciled with admission; its exhaustion was identified in source but not separately load-tested.

03 / LAUNCH CONDITIONS & TRUST

Requirements that remain

L-01: Launch staking is a deferred dependency

This is an intentional operational prerequisite, not a newly alleged exploit. The live delivery API lists no campaigns or escrow positions and reports the prefund vault as prefunded with `launchAt=0`. It reports one recorded stake. The additional launch-staking address is absent on mainnet, and deployment/launch-start routes are disabled by `LAUNCH_STAKING_ENABLED=false`.

The public details page discloses that deployment and fixed allocations must be completed before launch. Existing server guards reject legacy finalization while active stake enrollments exist. The new staking code passed local tests for atomic launch funding, committed amounts/tiers, launch-relative unlocks, late claims, replay protection and maximum-size proofs. These local results do not constitute a live deployment check.

Before trading launch: resume the saved deployment, verify its deployed bytes and immutability, reconcile payments, close checkout, seal buyer/staking roots, fund selected stakes at the recorded launch, and verify both vault balances and clock agreement. Re-review any changed code or configuration.

T-01: Owner confirmations remain consequential

SOL and USDC payments go directly to the treasury rather than a refundable payment escrow. Buyer entitlements depend on the accepted purchase ledger and owner-confirmed allocation root. The delivery program does not independently reconstruct all payments. An incorrect or dishonest root can omit buyers despite full token funding; buyers need the matching proofs to claim. Trading launch is owner-attested, and the team clock measures that recorded event rather than independently detecting market trading.

Use a reconciled, downloadable allocation manifest and independent verification before committing immutable roots. Protect owner access and the treasury signing key. The liquidity, development and listings reserves are still treasury-controlled; their balances are not proof of future use.

T-02: Weekly distributions are funded operationally

The reward code calculates 50% of an owner-supplied gross-fee amount. It does not independently prove total launchpad revenue or automatically collect and split every fee. Rewards depend on actual revenue, accurate reporting and weekly funding. State those dependencies clearly; multipliers are weights, not a guaranteed yield.

O-01: Unmatched incoming payments need review

The public payment-review API listed four unmatched incoming transfers, including an uploader refund. A transfer alone is not an accepted token purchase. Classify each from its verified transaction history; do not treat every incoming transfer as sales or automatically grant tokens. None had a quote-linked purchase ID in the captured response, so they do not trigger the quote-dispute finalization gate.

04 / TESTING & HANDOFF

Validation and limitations

Check	Result / practical meaning
Existing suite	240 passed, 0 failed, 0 skipped. Includes payment acceptance/recovery, sale cap, signing, claims, program custody, staking and reward tests.
Fresh capacity test	Confirmed admission/finalization mismatch at buyer 16,384.
Fresh signed-claim test	Inflated amount, substituted destination and duplicate claim failed; valid buyer-signed claim succeeded in LiteSVM.
Build / dependencies	Production build succeeded. npm production advisory query returned zero known advisories at review time.
Live custody / binary	Mainnet genesis checked; finalized mint/vault state decoded; exact deployed delivery ELF bytes compared. Reward-program immutability check passed.

Limits of this review

No mainnet transaction was signed or broadcast. Local owner setup signatures were substituted where the production treasury key was unavailable; buyer signatures in the new claim test were real ephemeral keypair signatures with verification enabled. The new capacity test used a synthetic paid ledger and mocked RPC, not actual contributions.

Rust/Agave/SBF build tools were unavailable, so source-to-binary reproducibility was not independently established. Binary equality proves correspondence to the supplied ELF, not that a fresh compiler run of the reviewed Rust source produces it. A reproducible build remains recommended before an external certification.

No exhaustive formal verification, comprehensive fuzzing, device-wallet UI session, browser penetration test, private production database export, full sale-history reconciliation, infrastructure access review, or business/KYC verification was performed. Public API reads were retried after initial 403 responses; successful snapshots are included. No live reward period or launched stake existed to validate end-to-end on mainnet.

Engineering handoff

Address M-01 before approaching the capacity boundary. Complete L-01 before trading launch. Reconcile unmatched transfers and preserve accepted receipts. Verify the allocation manifest before root commitment and keep the owner-control disclosures visible. Changes after this snapshot require a fresh review of affected components.

Reviewed website: <https://onward.us.org>

Published version: v60 (deployment confirmed succeeded)

Source commit: 58265a299d249e539c64539275040470826d264a

Embedded evidence ZIP: new tests, logs, public snapshots and source hashes. In the cited checkout, extract it and run `node --test audit-evidence/fresh-audit.test.mjs`. Existing suite: `npm run test:token`. No credentials or private keys are included.