TOWER

TOWER EXCHANGE

Olympix Remediation Report

Source-code remediation, production deployment and post-deployment validation in response to the Olympix contract findings.

PREPARED	November 5, 2026
NETWORK	Arc mainnet
PRIMARY CONTRACT	TowerSwapExecutorV2

Contents

1. Executive summary 3

2. Remediation architecture 4

3. Finding-by-finding disposition 6

4. Permit2 policy and compatibility 7

5. Recurring-order containment 7

6. Removed and retained source 7

7. Deployment and operational checklist 8

8. Verification evidence 8

9. Auditor review requests 9

10. Source references 9

Prepared: November 5, 2026
Scope: Source-code remediation, production deployment, and post-deployment validation performed in the Tower Exchange repository in response to the Olympix contract findings.
Status terminology:

- **Deployed / active:** remediation is deployed on Arc mainnet, source verified, configured in the application, and confirmed by on-chain read checks.
- **Live tested:** a deployed path has successfully executed on Arc mainnet through `TowerSwapExecutorV2`.
- **Decommissioned in source:** the obsolete source and deployment paths have been removed from this repository. Deployed bytecode cannot be removed by a repository change.
- **Disabled:** all product entry points fail closed; no new use should be possible through the application.
- **Retained / out of active scope:** code is preserved intentionally, but is not part of the active product/deployment scope and should be reassessed before reuse.

1. Executive summary

Tower Exchange implemented and deployed a new, separately deployable `TowerSwapExecutorV2` rather than modifying or proxy-upgrading the legacy executor. V2 adds a mandatory on-chain deadline, two-step ownership transfer, disabled ownership renunciation, and hardened adapter integration.

`TowerSwapExecutorV2` and the Aero, DZap, KyberSwap, and Uniswap V2 adapters are deployed, source verified, allowlisted, and configured in the application through their V2 environment addresses. Two live Arc mainnet swaps have successfully called the V2 executor. The legacy V1 contracts remain separate on-chain deployments and have not been altered by this remediation.

The standalone `Tower-AMM/` contract workspace has been removed. Per product direction, the pool UI, its API, and its supporting application code are retained; removal of the AMM workspace is not a statement that those UI files are deleted or that deployed contracts cease to exist.

Recurring orders are disabled across the product while a replacement design is prepared for a future audit. The legacy `RecurringOrderExecutor.sol` source remains with an explicit inactive notice to preserve audit history, but application routes and the execution worker fail closed.

Current Arc mainnet deployment state

The following state was confirmed through read-only Arc JSON-RPC calls on November 5, 2026. All listed deployment records report source verification as `verified`.

Component	Arc mainnet address	Current state
`TowerSwapExecutorV2`	`0x29c39683Bc6Ce1aCE7D9a8daEDA0E9F314eBD2F3`	Deployed, source verified, unpaused, and active at 30 bps platform fee.
`AeroAdapterV2`	`0x107D90dB1FEb3A6ad421d6957C5447A6D30f2455`	Contract code present; allowlisted as V2 route target and approval spender.
`DZapAdapterV2`	`0x57eCc1B93f4e6d02A130f2B79DD6e5af5Adee7dD`	Contract code present; allowlisted as V2 route target and approval spender.

Component	Arc mainnet address	Current state
`KyberSwapAdapterV2`	`0xD635bb50030466c239677c56e6b12e97FFDa5c3D`	Contract code present; allowlisted as V2 route target and approval spender.
`UniswapAdapterV2`	`0xD66fD081B4c5CEB658a9a6508d16c170F862EEAE`	Contract code present; allowlisted as V2 route target and approval spender.

The current V2 owner is the designated rollout EOA `0xe71dD45E7d21409b04b609D0E6C67FFff592d43d`. The configured treasury is `0xb3966683724303400B6fECDa1963825d994B546a`. Ownership transfer to a multisig remains an explicit post-smoke-test operational action.

Live V2 execution evidence

Both supplied transactions succeeded on Arc mainnet (`receipt.status = 0x1`), targeted `TowerSwapExecutorV2` , and used the V2 `executeSwap` selector (`0x3c7bf403`).

Transaction	Result	Evidence
`0x3f4e…06d6`	Successful V2 execution	Receipt succeeded; executor target; 15 emitted logs.
`0xdbf4…136d`	Successful V2 execution	Receipt succeeded; executor target; 17 emitted logs.

2. Remediation architecture

2.1 Separate V2 executor

New contract: `contracts/contracts/TowerSwapExecutorV2.sol`

V2 is a separate deployment with a new ABI for `executeSwap` . It is not a proxy upgrade and has no ability to alter V1 state. Its execution parameters add:

```
uint256 deadline;
```

The V2 executor:

1. rejects a swap when `deadline < block.timestamp` before receiving user funds;
2. keeps route targets and approval spenders independently allowlisted;
3. calculates and transfers the platform fee only from the received input amount;
4. clears the exact ERC-20 approval after the route call;
5. transfers only the swap's newly received output to the recipient; and
6. refunds only the caller's newly unspent input balance.

It uses `Ownable2Step` . An EOA may be the initial owner at deployment, per Tower's stated rollout plan. A later governance transfer is deliberately two-step:

```
EOA owner calls transferOwnership(multisig)
multisig calls acceptOwnership()
```

`renounceOwnership()` is disabled, preventing accidental loss of pause, recovery, and configuration authority.

2.2 Hardened aggregator adapter base and named venue adapters

New contracts: `contracts/contracts/adapters/HardenedAggregatorAdapterV2.sol`, `DZapAdapterV2.sol`, `KyberSwapAdapterV2.sol`, and `UniswapAdapterV2.sol`

`HardenedAggregatorAdapterV2` is an abstract reusable V2 implementation. Tower deploys the named DZap, KyberSwap, and Uniswap V2 contracts rather than a generic adapter instance. Each named contract is configured at construction with its trusted router target(s) and the relevant Permit2 address.

The adapter is not a general-purpose arbitrary-call proxy. It:

- accepts `routeCalldata` only for its configured router target(s);
- never permits Permit2 itself to be the callable `routeTarget`;
- gives the trusted primary router only the exact ERC-20 amount required for that swap;
- uses Permit2 only as a temporary approval layer where the underlying trusted router requires it;
- clears both ERC-20 and Permit2 allowances after a successful call; and
- refunds only the input-token balance increase associated with its caller's own trade.

The delta-based refund is important: it prevents a partial-fill refund from sweeping token balances that were already present on the adapter.

2.3 Aero V2 adapter

New contract: `contracts/contracts/adapters/AeroAdapterV2.sol`

The Aero V2 adapter preserves the existing exact-input swap interfaces while replacing broad residual-balance refunds with a per-call input balance delta. It also adopts two-step ownership and disabled ownership renunciation.

2.4 Application migration wiring

New helper: `lib/towerSwapExecutorV2.ts`

The application selects V2 only when `NEXT_PUBLIC_TOWER_SWAP_EXECUTOR_V2_ADDRESS` is explicitly configured. It then encodes the V2 execution tuple, including the deadline. When that variable is absent, the app continues to encode the legacy V1 tuple and use existing V1 addresses.

The following venue builders recognize V2-specific adapter addresses while preserving their V1 fallbacks:

- Aero
- DZap
- KyberSwap
- Uniswap

The V2 environment addresses are now configured for Arc mainnet. The app therefore builds V2 executor transactions for the configured mainnet venue paths. The retained V1 fallback is only used if the V2 configuration is removed; it is not a proxy upgrade or a mutation of V1 contracts.

3. Finding-by-finding disposition

Olympix finding area	Remediation	Status	Remaining action / limitation
Executor lacks an on-chain transaction deadline	V2 adds `deadline` to `ExecuteSwapParams` and rejects expired execution before token transfer.	Deployed / active; live tested	Continue to verify quote/build deadlines in routine monitoring. V1 remains a separate legacy deployment.
One-step ownership / risk of orphaned administration	V2 executor and V2 adapters use `Ownable2Step`; `renounceOwnership()` reverts.	Deployed / active	Complete the planned two-step transfer to the multisig after the rollout smoke-test window. Existing V1 ownership requires a separate owner action.
Arbitrary Permit2 target execution and persistent approvals in aggregator adapters	Hardened V2 adapter permits calls only to configured router target(s), not Permit2. It uses exact temporary allowances and clears them after the swap.	Deployed / active	Routes whose aggregator response targets Permit2 directly must remain disabled on V2. Obtain a router/diamond-targeted route or add a specifically reviewed integration.
Partial-fill / stranded-balance sweep risk in aggregator adapters	V2 adapter refunds only `balanceAfter - balanceBefore` for the current input token and sends only newly received output.	Deployed / active	V1 adapters and any deployed V1 balances require an owner-led migration/recovery plan; source changes cannot change deployed V1 behavior.
Aero partial-fill residual refund risk	`AeroAdapterV2` snapshots the pre-swap input balance and refunds only the call's residual amount.	Deployed / active	Continue route-specific smoke testing and monitoring of partial-fill/refund behavior.
XyloNet adapter transfer/output-validation issues	LI.FI/XyloNet adapter source, deployment scripts, quote/build paths, route selection, and UI setup are removed.	Decommissioned in source	If legacy deployed instances exist, remove them from allowlists and pause/retire them with the authorized owner.
Legacy TowerRouter approval, fee, native-value, stale-ledger, and split-route issues	Legacy TowerRouter source, supporting `SwapMath`, and registration/deployment paths are removed.	Decommissioned in source	Deployed legacy instances must be paused or retired through their owner; repository removal does not remove blockchain bytecode.
UnitFlow adapter partial-fill issue	Legacy UnitFlow adapter source and deployment script are removed. Direct UnitFlow integration remains in the application.	Decommissioned in source	Confirm no legacy UnitFlow adapter remains allowlisted on active executors before V2 activation.
Recurring order overwrite / relayer fixed-price-floor concerns	Recurring-order UI, order API, authorization API, execution API, app cron, and Supabase worker are hard-disabled. The source contract is annotated as inactive.	Disabled	A future recurrence design must define immutable order identifiers, protected update semantics, and a reviewed fixed-price/minimum-output policy before re-enablement.
TowerDex recipient/caller behavior	Pool UI/support code is retained by product decision, while the standalone AMM workspace is removed. No behavioral change was made to this retained path.	Retained / out of active scope	Reassess and audit this path before any new pool or AMM deployment is activated.

4. Permit2 policy and compatibility

What V2 rejects

V2 rejects an aggregator response that requests a direct low-level call to the Permit2 contract. A direct Permit2 target combined with opaque calldata can encode approvals or transfers outside the intended swap scope; this is the behavior addressed by the remediation.

What V2 still permits

V2 does not ban the Permit2 protocol. The hardened adapter may use Permit2 internally to authorize its configured primary router for the exact input amount needed by the current swap. This authorization is cleared after successful execution.

Effect on swaps

Swaps remain compatible when the aggregator provides calldata directed to its trusted router or diamond contract. For example, DZap, KyberSwap, and Uniswap routes can be supported by their corresponding named hardened V2 adapter.

If a provider returns `Permit2` as the outer transaction target, V2 rejects that route by design. This is not a user-facing Permit2 approval failure; it is a route-selection restriction. Such a route must be replaced by a provider-supported router-targeted route or reviewed before being enabled.

The V2 environment addresses are configured for Arc mainnet and successful live swaps have reached `TowerSwapExecutorV2`. V1 remains deployed separately and must be retired through an explicit owner-led plan; it is not changed or upgraded by the V2 rollout.

5. Recurring-order containment

The following layers now fail closed with a `503` response or an unavailable product screen:

- `/recurring-orders`
- `/api/user/recurring-orders`
- `/api/user/recurring-orders/[id]`
- `/api/user/recurring-orders/[id]/authorize`
- `/api/user/recurring-order-executions`
- `/api/cron/execute-recurring-orders`
- `supabase/functions/execute-recurring-orders`

Historical Supabase migrations and database rows are retained. They are not deleted because applied migration history and historic records should not be altered by a source-code decommissioning.

6. Removed and retained source

Removed

- `Tower-AMM/` standalone Hardhat workspace, including AMM contracts, scripts, tests, and deployment record.

- Legacy `TowerRouter.sol` and obsolete routing support.
- LI.FI/XyloNet and De1 adapter contracts, deployment scripts, quote/build integrations, and UI route setup.
- Legacy UnitFlow adapter and its deployment path.
- Obsolete TowerRouter registration/deployment paths.

Intentionally retained

- Pool UI, pool API, and supporting application libraries.
- `TowerDexAdapter` source and associated support, per product direction.
- Current direct third-party DEX integrations.
- `RecurringOrderExecutor.sol` as inactive, auditable historic source.
- Historic Supabase migration files and records.

7. Deployment and operational checklist

Item	Current disposition
Choose the initial owner and treasury	Complete. The rollout EOA is owner and the treasury is configured on-chain; both are recorded above.
Deploy `TowerSwapExecutorV2`	Complete. Source verified at `0x29c39683Bc6Ce1aCE7D9a8daEDA0E9F314eBD2F3`.
Deploy V2 adapters	Complete. Aero, DZap, KyberSwap, and Uniswap V2 adapters are deployed and source verified.
Confirm V2 allowlists	Complete. Every listed V2 adapter has code and is currently allowlisted as both route target and approval spender.
Configure V2 application addresses	Complete for the deployed Arc mainnet configuration.
Live smoke-test V2 execution	Started and successful. Two successful executor transactions are recorded above. Continue venue-, pair-, direction-, and amount-specific coverage before declaring the full route matrix complete.
Review aggregator target shape	Ongoing release control. V2 must continue to reject direct Permit2 outer targets.
Monitor the migration	Ongoing. Reconcile input, 30 bps fee, output, and any residual refund for each production test and early user transaction.
Retire V1 carefully	Not yet complete. Do not remove V1 allowlists or pause legacy contracts until the V2 rollout has sufficient coverage and an owner-approved retirement plan.
Transfer ownership to multisig	Not yet complete. The EOA should call `transferOwnership(multisig)` and the multisig must call `acceptOwnership()` after the designated smoke-test period.

8. Verification evidence

The following local verification was completed after the changes:

```
npm run compile --prefix contracts
```

Result: Solidity compilation completed successfully.

```
npm test --prefix contracts
```

Result: 28 passing tests, including the V2-focused tests below.

Test suite	Verified behavior
`TowerSwapExecutorV2.test.js`	valid non-expired swap settlement; expired swap rejection before fund movement; two-step ownership; renunciation disabled
`HardenedAggregatorAdapterV2.test.js`	DZap, KyberSwap, and Uniswap V2 adapter deployments; only current-call residual input is refunded; pre-existing adapter balance is not swept; Permit2 cannot be used as a route target

Application lint and TypeScript checks were also run after the implementation changes.

Deployment and live-execution evidence

- Deployment records for the V2 executor and all four V2 adapters record `verificationStatus: "verified"`.
- Read-only Arc mainnet verification confirmed the V2 executor is unpaused, uses a 30 bps platform fee, and has the expected treasury and rollout EOA owner.
- Read-only Arc mainnet verification confirmed contract code plus both allowlist entries (`routeTargets` and `approvalSpenders`) for Aero, DZap, KyberSwap, and Uniswap V2 adapters.
- The two transactions in the live-execution evidence table each have a successful receipt and call `TowerSwapExecutorV2` with the V2 `executeSwap` selector.

9. Auditor review requests

Tower requests that Olympix focus a follow-up review on:

1. V2 executor parameter validation, fee accounting, deadline semantics, and output/refund accounting.
2. The hardened adapter's router-target restrictions and Permit2 allowance lifecycle.
3. The interaction between each real aggregator's generated calldata and the V2 target policy.
4. Ownership transfer, pause, recovery, and operational separation of duties.
5. The planned retirement of V1 on-chain allowlists and deployed legacy contracts after the V2 monitoring period.
6. The future recurring-order design before it is re-enabled.

10. Source references

- `contracts/contracts/TowerSwapExecutorV2.sol`
- `contracts/contracts/adapters/HardenedAggregatorAdapterV2.sol`
- `contracts/contracts/adapters/AeroAdapterV2.sol`
- `contracts/contracts/adapters/DZapAdapterV2.sol`
- `contracts/contracts/adapters/KyberSwapAdapterV2.sol`
- `contracts/contracts/adapters/UniswapAdapterV2.sol`
- `lib/towerSwapExecutorV2.ts`
- `contracts/scripts/check-v2-swap-configuration.cjs`

- `contracts/deployments/tower-swap-executor-v2-arc-mainnet-deployment.json`
- `contracts/deployments/aero-adapter-v2-arc-mainnet.json`
- `contracts/deployments/dzap-adapter-v2-arc-mainnet-deployment.json`
- `contracts/deployments/kyberswap-adapter-v2-arc-mainnet-deployment.json`
- `contracts/deployments/uniswap-adapter-v2-arc-mainnet-deployment.json`
- `app/api/cron/execute-recurring-orders/route.ts`
- `supabase/functions/execute-recurring-orders/index.ts`
- `contracts/contracts/RecurringOrderExecutor.sol`
- `.env.local.example`