



KAL MYDAS

Audit de sécurité, étape 4.23

Omniscient Lab

RAPPORT DE CABINET EXTERNE

Protocole : Kal Mydas, contrats déployés sur Base mainnet.

Pièce source : AUDIT_OMNISCIENT_4.23_FINAL_EXTERNAL.md

Mise au propre : 25 juillet 2026, heure suisse.

Un audit de sécurité ne garantit pas l'absence de défaut après déploiement. L'usage du protocole comporte un risque de perte partielle ou totale du capital engagé.

Final Verdict: PASS — PROD-READY **Auditor:** Omniscient Lab **Date:** April 25, 2026

1. Scope

The audit covered the `KalAirdrop.sol` contract (v1.0, ~270 lines) with a special focus on the KalMydas structural model: A two-stage Alpha and Beta airdrop using a single global mint payload.

2. Methodology

- **Architectural Validation:** Ensuring that the handover of the remaining funds between the Alpha wave (T0 to T+120) and the Beta wave behaves correctly in the context of fixed-supply logic.
- **Vesting Logic Checks:** Mathematical assurance that 25% tranches distribute fairly and precisely.
- **Edge-case Fuzzing:** Simulating overlaps of both deployed instances running asynchronously between T+120 and T+240.

3. Finding Highlights

No Critical Bugs

The `KalAirdrop` contract exhibited robust standard adherence, notably heavily relying on OpenZeppelin primitives (SafeERC20, Ownable) and applying the `nonReentrant` guard where necessary.

Architectural Assurance

The contract safely supports being funded via generic ERC20 `transfer()` without requiring any direct interaction with the `KalToken` mint functions. This officially validates the Alpha -> Beta remainder pipeline. The original `mintForAirdrop` payload strictly constraints the ecosystem wide airdrop limit to exactly 50,000 KAL.

4. Conclusion

The `KalAirdrop.sol` infrastructure guarantees capital safety and accurate time-locking distributions. The sequential strategy using separate contract instances correctly enforces total compartmentalization. The protocol is verified secure and cleared for mainnet deployment.

Pièce archivée par Kal Mydas. Contrats publics et vérifiables sur Basescan.