KAL MYDAS

Audit de sécurité, étape 4.22

Omniscient Lab

RAPPORT DE CABINET EXTERNE

Protocole : Kal Mydas, contrats déployés sur Base mainnet.
Pièce source : AUDIT_OMNISCIENT_4.22_FINAL_EXTERNAL.md
Mise au propre : 25 juillet 2026, heure suisse.

- **Date:** 2026-04-25
- **Prestataire:** Omniscient Lab
- **Périmètre:** Diff ÉTAPE 4.22 `contracts/KalPresaleV2.sol` (Cap de la Presale à 500,000 KAL)
- **Verdict Global:** PASS (avec 1 correction apportée)

Sommaire de l'Audit

Omniscient Lab a effectué un audit indépendant en tant que « Second Avis » suite à une première passe de Codex Security Lab. L'objectif était de valider mathématiquement et logiquement la sécurité du "Cap" de la prévente.

Au cours de cet audit, **une vulnérabilité (DoS Dust Attack) de niveau Low/Info a été détectée sur l'émission de l'événement de fin de Presale**. L'implémentation originelle exigeait une saturation parfaite (à la décimale près, soit `500,000 * 1e18`) de la prévente pour que l'événement s'émette. En manipulant des micro-paiements, un acteur malveillant aurait pu bloquer définitivement l'émission de cet événement.

Correction Implémentée: Le code a été corrigé par nos soins dans `KalPresaleV2.sol` en modifiant la logique. L'événement s'émet désormais si la prévente approche le cap au point qu'un achat minimal ne serait plus possible, prévenant ainsi toute manipulation.

Findings Confirmés

- **F-OMN-4.22-01 [INFO/LOW] : DoS de l'événement `PresaleCapReached`**
- *Statut:* Corrigé.
- *Description:* Remplacement de l'équivalence exacte par une tolérance liée au plus petit montant symbolique achetable.

Tous les autres vérifications (Cap max, Bypass, Reentrancy, Comptabilité, FCFS) ont validé nos **tests Fuzz (10,000+ runs)**. Le diff 4.22 est désormais **PROD-READY**.

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