Pheonix5981 Security

Security Research Summary · Contact: willworachat@gmail.com · Report date: 2026-07-02

Crypto.com RESOLVED — $0

Platform: HackerOne
Program dates: Research 2026-06-05 to 2026-06-07; program complete
Coverage: Broad — Exchange REST+WebSocket API (100%), merchant GraphQL (100%), NFT GraphQL (100%), KYC API (100%); accounts.crypto.com OAuth/SSO and institutional API untested (required live browser session / special access tier)

SCOPE TESTED

Crypto.com's Exchange REST and WebSocket trading API, merchant payment GraphQL API (pay.crypto.com), NFT marketplace GraphQL API, and KYC verification API — across web, mobile, and institutional access tiers.

METHODOLOGY APPLIED

- H11 systematic IDOR sweep across exchange sub-account transfers, WebSocket private channels, merchant subscriptions, and KYC state endpoints, using two independently-registered test accounts
- H12 auth checklist applied to a BFF (backend-for-frontend) proxy layer's identity-resolution logic
- P10 systematic recon across 8+ subdomains and infrastructure surfaces

OUTCOME

> One Medium-severity finding was submitted: an NFT-marketplace GraphQL mutation allowed subscribing any email address to a promotional drop notification without authentication, enabling spam abuse and email-existence enumeration. It was closed as a duplicate of an existing internal report. A comprehensive, systematic IDOR sweep across every fund-movement and data-access surface — exchange sub-account transfers, WebSocket private channels, merchant subscription management, and KYC verification state — using two independently-created test accounts found universal, correctly-enforced identity binding to session tokens with no exploitable cross-account access anywhere. Two lower-severity, unauthenticated NFT-platform issues (view-count inflation, private-wishlist exposure) were documented but not separately submitted. Total: $0 (duplicate), program complete.