Pheonix5981 Security

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

Blockchain.com RESOLVED — $0

Platform: Bugcrowd
Program dates: Research and PoC 2026-05-27; triage outcome 2026-06-22
Coverage: Full API surface enumeration — WebSocket subscription layer, KYC/tier system, custodial transfer endpoints

SCOPE TESTED

Blockchain.com's WebSocket real-time API (ws.blockchain.info), main API gateway (api.blockchain.info/nabu-gateway), and KYC-tier/custodial-transfer subsystem.

METHODOLOGY APPLIED

- H11 systematic web/API checklist — IDOR testing across WebSocket subscription channels
- H4 full attack-chain construction — traced an initial IDOR finding through key-exchange cryptography to a complete, demonstrated account-takeover path
- H12 auth checklist applied to KYC-tier state transitions and geo-restriction enforcement

OUTCOME

> A Critical-severity account-takeover vulnerability was fully demonstrated end-to-end: the WebSocket real-time API allowed unauthenticated subscription to any user's private notification channel by GUID, which — chained through the desktop-to-mobile QR pairing handshake's key-exchange protocol — enabled full decryption of a victim's wallet credentials during pairing. The finding was confirmed as accurate by the vendor but closed as a known duplicate (already tracked internally). A secondary Medium-severity finding (a KYC-tier check bypass on a deposit-notification endpoint with no financial impact, since balances are independently verified on-chain) was also investigated. Total: $0 (duplicate), program complete.