Phoenix5981 Security

Security Research Summary · Contact: willworachat@gmail.com · Report date: 2026-09-06 (supersedes the 2026-07-02 interim summary)

Redbelly Network

RESOLVED — 2 of 3 findings accepted as valid, bounty paid (1,000 USDC)

Platform	Hashlock (Redbelly Network bug bounty program)
Program dates	Research 2026-06-01 to 2026-06-23; submissions 2026-06-08 and 2026-06-23; all three tickets closed by 2026-07-30
Coverage	Broad L1 + dApp coverage — core smart contracts cleared, custom RPC namespace cleared, identity/KYC subsystem (Averer) fully mapped
Reports submitted	3 (1 High + 1 High + 1 Medium as reported)
Outcome	All three confirmed as genuine vulnerabilities by the vendor's triager. Two (an authentication weakness and an unauthenticated configuration-exposure issue) accepted as **Complete – Valid** and paid a combined **1,000 USDC**. The third (a phishing-dependent PII exposure) was confirmed valid but ruled non-bounty-eligible because it requires a social-engineering prerequisite.

SCOPE TESTED

Redbelly Network L1 blockchain infrastructure (DBFT consensus, EVM compatibility layer, custom RPC namespace) and its Averer identity/KYC dApp ecosystem, including associated web services and the identity-provider registry contracts.

METHODOLOGY APPLIED

- H15 blockchain-infrastructure checklist — custom RPC namespace probing, consensus-layer review, EVM compatibility edge cases
- H11 / H12 web and authentication checklists — postMessage origin validation, API authentication and session-establishment flow analysis
- P10 systematic reconnaissance — JavaScript bundle mining across the dApp surface surfaced the authentication weaknesses
- H4 access-control privilege-chain validation — each weakness was chained end-to-end and demonstrated with a live, minimal proof-of-concept before submission

OUTCOME / FINDINGS SUMMARY

Three findings were identified in the identity/KYC subsystem: a broken origin check in a postMessage handler enabling PII exposure via a phishing page, an unauthenticated configuration endpoint exposing a backend service key, and an authentication weakness allowing a session to be established with reduced verification. All three were reported with working proofs-of-concept. The vendor accepted the authentication weakness and the configuration-exposure issue as valid and paid a combined 1,000 USDC; the remediation stated by the vendor was removal of the exposed key and hardening of the authentication path. The phishing-dependent finding was acknowledged as accurate but closed without reward under the program's social-engineering exclusion. Core smart contracts and consensus-layer surfaces were reviewed and found properly access-controlled.

Exploit-level detail (endpoints, keys, request sequences) remains withheld from this public summary as a matter of responsible-disclosure practice.
