Pheonix5981 Security

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

Circle BBP RESOLVED — $0

Platform: HackerOne
Program dates: Research 2026-05-18 to 2026-06-23; program complete
Coverage: 12 findings investigated across 3 repositories (Malachite consensus engine, Stellar CCTP, Arc Remote Signer)

SCOPE TESTED

Circle's open-source cross-chain infrastructure: the Malachite BFT consensus engine, the Stellar Cross-Chain Transfer Protocol (CCTP) implementation, and the Arc Remote Signer validator-signing service.

METHODOLOGY APPLIED

- P4 prior-audit awareness — recognized these are heavily-audited, actively-monitored repositories requiring elevated duplicate-risk assessment
- H8 boundary-condition checklist across consensus round/height arithmetic and type-conversion edge cases
- G9 attacker-controllability check — correctly identified that an overflow finding required a trusted off-chain attester to trigger, sharply limiting its real-world exploitability
- H6/H3 reentrancy and replay checklists applied to the signing and message-parsing layers

OUTCOME

> Seven findings were formally submitted across the three repositories, spanning integer-overflow/wraparound conditions in consensus round-tracking, panic-on-conversion bugs in model-based-testing call sites, a nonce-replay window in cross-chain message handling, and a stateless-signing gap in the remote validator signer. All seven were resolved: six as duplicates of existing internal reports and one (a type-truncation finding in message parsing) as Informative after confirming the affected field is set by a trusted off-chain attester rather than being user-controlled, sharply limiting real-world exploitability. Five additional candidate findings were investigated and deliberately not submitted due to high assessed duplicate risk in this heavily-audited codebase. Total: $0, all resolved dead.