Pheonix5981 Security — Security Research Summary

Contact: willworachat@gmail.com | Report date: 2026-07-02

Target	BitGo
Platform	Cantina
Engagement dates	2026-06-04 to 2026-06-11
Reports submitted	1 (F1); F2/F3 not submitted
Outcome	DUPLICATE

Scope Tested

eth-multisig-v4 and eth-multisig-v2 smart contract repositories (multi-chain multisig wallet infrastructure).

Methodology Applied

H3 signature-replay/signature-scheme checklist (cross-chain domain separator check), H8 boundary conditions (CREATE2 zero-address handling), SWC-117 signature malleability review.

Coverage

Full review of both in-scope repositories.

Outcome / Findings Summary

F1 (Critical, cross-chain signature replay in WalletSimple.sol due to missing chainid in signed hash) judged DUPLICATE by Cantina. F2 (signature malleability, High) and F3 (silent CREATE2 failure, Medium) assessed as high duplicate-risk / low severity and not submitted. $0.