Pheonix5981 Security

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

Morpho Midnight RESOLVED — $0

Platform: Cantina (competition)
Program dates: Research 2026-06-01 to 2026-06-05; competition closed 2026-06-13; judging complete 2026-06-22
Coverage: Exhaustive — 5 full review sessions, ~1,900 lines of core protocol source, all liquidation/reentrancy/callback paths

SCOPE TESTED

Morpho's Midnight protocol — a fixed-rate, fixed-term, intent-based peer-to-peer lending system on Ethereum (morpho-org/midnight), including its core settlement engine and peripheral bundling contracts.

METHODOLOGY APPLIED

- P5 invariant-first analysis — defined and continuously re-verified core solvency/accounting invariants across 5 independent review passes
- H6 reentrancy checklist including callback-ordering and staticcall-based gate/ratifier verification
- H8 boundary-condition checklist — identified division-by-zero and underflow conditions at specific price-tick boundaries
- P7 delta-aware review focused on the peripheral bundling contracts explicitly excluded from the protocol's own formal verification (Certora) scope

OUTCOME

> Four Medium-severity denial-of-service findings were submitted, all rooted in price-tick boundary conditions where a maker's permissionlessly-created offer at a specific tick value causes a division-by-zero or arithmetic-underflow panic outside the protocol's try/catch error handling, permanently reverting any bundled transaction that includes the offer. All four were judged duplicates of earlier-submitted findings covering the same root causes. An extensive multi-session Critical-severity hunt covering liquidation math, callback re-entrancy, and cross-function invariants found no exploitable Critical or High-severity issues — the protocol's formal verification coverage proved comprehensive. Total: $0 (all duplicate), program formally exhausted after 5 sessions.