Pheonix5981 Security

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

LaunchDarkly RESOLVED — $0

Platform: Bugcrowd
Program dates: Research 2026-06-15 to 2026-06-24; program complete
Coverage: Full REST API surface (242 endpoints) mapped; approval-workflow and webhook subsystems tested

SCOPE TESTED

LaunchDarkly's feature-flag management REST API (app.launchdarkly.com/api/v2), specifically its production-change approval-workflow (SOC2 change-management control).

METHODOLOGY APPLIED

- H11 business-logic checklist — systematically tested every write path (JSON patch, semantic patch, flag-copy) against a documented approval requirement
- G1 duplicate/known-issue verification before treating a confirmed bypass as submittable

OUTCOME

> A High-severity approval-workflow bypass was confirmed live with a full reproduction matrix: three separate API write paths (standard JSON patch, semantic patch, and flag-copy) all successfully modified a production feature flag despite an active approval requirement configured to block exactly that change, while only the formal “apply approved change” endpoint correctly enforced the control. This meant any API user with write access could silently bypass a SOC2 change-management control. The finding was closed as a duplicate (Known Issue — already tracked internally by the vendor). Three related hypotheses (approval bypass via early-apply, admin-announcement injection, webhook SSRF) were tested and ruled out as properly protected. Total: $0 (known issue), program complete.