Pheonix5981 Security

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

Rapyd RESOLVED — $0

Platform: Bugcrowd
Program dates: Research 2026-06-18 to 2026-06-24; program complete
Coverage: Comprehensive — SAML/SSO flow, 203 mapped API endpoints, full IDOR sweep across two independent test organizations

SCOPE TESTED

Rapyd's merchant dashboard (dashboard.rapyd.net), production and sandbox payment APIs (api.rapyd.net, sandboxapi.rapyd.net), and SAML-based SSO authentication.

METHODOLOGY APPLIED

- H12 authentication/session checklist — SAML assertion signing analysis (Response-level vs. Assertion-level signing)
- H11 web/API checklist — systematic IDOR sweep across ewallets, customers, and transfer endpoints using two independently-created merchant organizations
- G11 privilege-delta verification — confirmed whether a discovered SAML bypass granted genuinely new capability beyond the attacker's existing role
- G12 concrete-harm gate — applied to a broken-endpoint observation before considering it a security finding

OUTCOME

> A SAML NameID-injection authentication bypass was fully demonstrated (cross-account login without password, confirmed via a live proof-of-concept) but ruled a duplicate: the escalation path only worked within an admin's own organization, which the platform correctly noted was not a genuine privilege escalation since org admins can already access their own members' accounts by design. A cross-merchant data-exposure issue on a list endpoint (returning other merchants' invoice line items) was also ruled a duplicate. A third report (a consistently erroring endpoint) was ruled not a security issue — a broken feature rather than an exploitable vulnerability. A full IDOR sweep across fund-transfer and wallet endpoints using two separate test organizations found all vectors properly scoped. Total: $0, all three reports resolved as duplicate/not-applicable.