SAAS PLATFORM / API HIGH

Every Customer Record Reachable by Changing One Number

BOLA / IDOR | SOC 2 audit passed three months prior

01 Engagement Overview

A multi-tenant SaaS platform engaged DivIHN for an API-focused penetration test three months after completing a SOC 2 Type II examination. The organization viewed the successful examination as evidence that its access control model was sound.

- **Scope:** REST API endpoints, authentication and session handling, object-level access control across tenant boundaries
- **Approach:** Authenticated testing using a standard customer account, with a focus on authorization logic gaps rather than authentication bypasses.
- **Baseline: SOC 2 Type II examination completed three months prior, with no anomalies flagged in access logs.**

02 Technical Discovery

While testing a standard record-retrieval endpoint, DivIHN found that the API authenticated each request but failed to verify whether the requesting account owned the requested record. This exposed a textbook broken object-level authorization vulnerability.

- Mechanism: Incrementing the numeric record ID in the request URL returned another customer's complete record without checking the session against the record owner.
- Scope: The same weakness affected every endpoint that used the ID scheme, allowing any authenticated customer to enumerate records belonging to other customers.
- Why it was missed: The SOC 2 examination assessed whether relevant controls operated as intended during the examination period, but it did not test every endpoint for object-level authorization. Each request was authenticated and technically valid, resulting in a normal-looking HTTP 200 response in the logs.

03 Risk & Business Impact

The finding received a HIGH severity rating rather than Critical because exploitation required a valid customer account. However, the vulnerability created a complete failure of tenant-level data isolation.

- Any single paying customer could access records belonging to other customers, creating a broad multi-tenant data exposure risk.
- Standards exposure: BOLA/IDOR represents a major API security risk and is addressed within the OWASP API Security Top 10. The finding also raised concerns around the effectiveness of access controls supporting the organization's SOC 2 commitments.
- A finding of this nature only three months after the SOC 2 examination could raise questions about the depth and coverage of security testing beyond control documentation and operating effectiveness.

04 Remediation & Outcome

DivIHN worked with the client's engineering team to strengthen object-level authorization and improve visibility into suspicious cross-tenant access.

- Added ownership verification to every object-level API call, validating the authenticated session against the record's tenant ID.
- Replaced sequential numeric record IDs with non-guessable UUIDs to make trivial enumeration more difficult.
- Instituted automated BOLA/IDOR testing within CI/CD pipelines before each release.
- Added record-level anomaly detection to identify and flag potential cross-tenant access in application logs.