

Abundera Security Assessment Summary

Assessing Partner: BreachLock, Inc.

Engagement Window: October 7 to 14, 2026

Methodology: Multi-role authenticated, gray-box, invasive API penetration test

Scope: Core API (abundera.ai/v1)

Result: Zero Critical, High, or Medium severity findings. Two findings below that threshold (one Low, one Informational), both tracing to a single root cause.

Summary

BreachLock conducted an invasive, authenticated penetration test of Abundera's core API over a seven-day window, testing across multiple account roles (owner, admin, and member tiers) to probe for authorization bypass, cross-tenant data access, and business-logic abuse, in addition to standard API security testing.

The assessment returned zero findings at the Critical, High, or Medium severity levels. Two lower-severity findings were reported: a Low-severity finding (CVSS 3.7) and an Informational finding (CVSS 0), both referencing the same underlying condition, legacy CBC-mode TLS 1.2 cipher suites still negotiable at our edge, alongside the modern AEAD suites already in use.

Independent verification of testing volume

BreachLock's declared testing infrastructure generated 41,901 requests against our API during the engagement. Our own edge security telemetry, independent of the testing firm's own reporting, recorded 11,137 of those requests blocked automatically at the network edge (26.6%), with the remaining 30,764 reaching the application layer directly. This is our own measurement, confirming the volume and reach of the assessment.

The two findings, and why they're not an application defect

Both findings are instances of a well-documented class of TLS vulnerability (CVE-2013-0169 and CVE-2016-2107, both over a decade old) that scanners flag whenever a server's TLS 1.2 configuration still offers CBC-mode cipher suites, regardless of whether a specific exploit is practical against that server.

We traced the condition to its source: our hosting infrastructure provider does not currently support restricting which cipher suites are offered on our hosting tier. We confirmed this directly, our attempt to restrict the cipher list succeeded at the API level but had no effect on the live connection, and reported the gap to the provider.

This is a platform-level limitation of our infrastructure provider, not a defect in Abundera's application code. TLS 1.3 connections, the modern default for most clients, are unaffected. Given the severity, we are accepting this as a documented residual risk while we pursue a resolution with the provider, rather than holding up other work.

What this confirms

Zero Critical, High, or Medium findings across an invasive, multi-role authenticated test, probing authorization boundaries, tenant isolation, and business logic directly, is a strong result for a first external assessment. Combined with our continuous internal testing program (1,053 automated attack simulations across 50 categories) and weekly external DAST scanning, this reflects a sustained security posture rather than a one-time result.

References

- CVE-2013-0169 (Lucky13)
- CVE-2016-2107 (LuckyMinus20)

- Full BreachLock reports and remediation correspondence available to banking partners, auditors, and enterprise customers on request at security@abundera.ai