PENETRATION TEST · ENGAGEMENT REPORT

Web, API & Cloud Security Assessment

CLIENT	Vellum Health, Inc.
ENGAGEMENT ID	OW-2026-Q2-07
WINDOW	12 May – 02 Jun 2026
SCOPE	Web · API · AWS production estate
AUTHOR	OmegaWulf, Pack 02
REPORT VERSION	1.0 — Final

PAGE 02 · EXECUTIVE SUMMARY

Three ways in. One trivial.

What we found, what it means, and what to close first.

Across three weeks of testing against Vellum's web application, public API, and AWS production estate, OmegaWulf identified seven findings of note. Two are Critical — a subdomain primed for takeover by an anonymous attacker, and a JWT verifier that accepts forged tokens at the front door. Both are reachable from the internet. Both can be closed this week.

Three High-severity findings concern data exposure: cross-tenant access to patient records, an S3 bucket of database snapshots open to the public, and an IAM role permitting trivial pipeline-to-account privilege escalation. Two Medium findings round out the engagement.

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	3	2	0	0
FINDINGS	FINDINGS	FINDINGS	FINDINGS	FINDINGS

TOP RISK · CRITICAL

JWT signature bypass

Forged token grants administrator impersonation against the public API. Reproducible with three lines of Python.

F-OW-2026-0058 · CVSS 9.8

DISCOVERED BY OMEGAWULF SCOUT

Three AWS findings, one pass.

Our AWS reconnaissance agent surfaced the S3, IAM, and RDS findings below in the first eight minutes of cloud testing.

See page 08 for tooling detail

PAGE 03 · SCOPE & METHODOLOGY

Tested like a pack.

Four phases. Six operators. No spray-and-pray scanner output.

IN SCOPE

- Web application · app.vellum.health (authenticated and unauthenticated paths)
- Public API · api.vellum.health (REST + GraphQL)
- AWS estate · account 750199275*** (prod), us-east-1 + us-west-2
- Identity · Okta tenant, federated SSO into AWS and the platform

OUT OF SCOPE

- Internal corporate network and endpoint estate
- Third-party SaaS integrations (Stripe, Twilio, SendGrid)
- Physical access and social-engineering vectors
- Production data deletion or destructive proofs of exploit

METHODOLOGY

01

Recon

Map the attack surface. Enumerate exposed assets, identify technologies, and build a model of the system before touching anything sensitive. Includes a continuous SCOUT pass over the AWS estate.

02

Exploitation

Test for vulnerabilities the way a real attacker would — chained, prioritised by impact, and verified manually. Findings without reproduction steps don't make the report.

03

Post-exploitation

Validate impact. Demonstrate what an attacker could actually do with each foothold — lateral movement, privilege escalation, data access — within the limits of the engagement letter.

04

Reporting

Findings delivered with reproduction steps, severity rationale, and concrete remediation guidance — written for engineers, not auditors. Debrief call scheduled within five business days of delivery.

PAGE 04 · RISK OVERVIEW

Findings at a glance.

One row per finding. Sort by what hurts most.

ID	SEVERITY	FINDING	CVSS
F-OW-2026-0042	CRITICAL	Subdomain takeover on marketing tenant	9.1
F-OW-2026-0051	HIGH	IDOR exposes cross-tenant patient records	8.2
F-OW-2026-0058	CRITICAL	JWT signature verification bypass via algorith...	9.8
F-OW-2026-0063	HIGH	GraphQL introspection enabled in production	7.5
F-OW-2026-0071	HIGH	S3 bucket exposes nightly database snapshot...	8.6
F-OW-2026-0078	HIGH	iam:PassRole on wildcard resource permits pri...	8.4
F-OW-2026-0091	MEDIUM	RDS automated snapshot shared with unknow...	6.5

DISCOVERY ATTRIBUTION

- 3 findings surfaced by OmegaWulf SCOUT during recon (continuous AWS scan)
- 4 findings reproduced by hand during exploitation and post-exploitation phases

PAGE 05 · FINDING DETAIL · WEB APPLICATION

Web application

What we tested on app.vellum.health.

CRITICAL F-OW-2026-0042

Subdomain takeover on marketing tenant

AFFECTED ASSET

go.vellum.health · CNAME -> vellum-marketing.fastly-cms.net

FINDING

The marketing tenant CNAME points at a Fastly CMS hostname no longer claimed by Vellum. An anonymous attacker can register the target name and serve arbitrary content under go.vellum.health, including credential-harvesting pages indistinguishable from the real brand. Reproduced from open-source tooling in four minutes during the engagement window.

REMEDIATION

- Remove the dangling CNAME record in Route 53 (zone Z3K42...). Hot-fix, <=15 min.
- Add a CI step that fails when a CNAME resolves to an unclaimed third-party host.
- Audit the remaining 218 records in the marketing zone against the same check.
- Brief the marketing tenant owner so future CMS migrations include a DNS cleanup step.

EXTERNAL UNAUTHENTICATED CVSS 9.1 CWE-350

PAGE 06 · FINDING DETAIL · API

API

What we tested on api.vellum.health.

CRITICAL F-OW-2026-0058

JWT signature verification bypass via algorithm confusion

AFFECTED ASSET

api.vellum.health · Authorization: Bearer <jwt>

FINDING

The auth middleware accepts JWTs signed with the HS256 algorithm using the server's public RSA key as the HMAC secret. Forged tokens succeed against /api/v1/auth/me, granting impersonation of any user including platform administrators. No detective control fires. CloudTrail and the application WAF treat the forged calls as legitimate.

REMEDIATION

- Pin the JWT verifier to a single algorithm (RS256) and reject alg=none.
- Rotate signing keys; treat all sessions issued during the engagement as suspect.
- Add WAF rule to log JWTs with alg headers other than RS256 for triage.

EXTERNAL UNAUTHENTICATED CVSS 9.8 CWE-347

PAGE 07 · FINDING DETAIL · CLOUD / AWS

Cloud / AWS

What OmegaWulf SCOUT and our cloud operators tested.

HIGH F-OW-2026-0071

S3 bucket exposes nightly database snapshot to the public

AFFECTED ASSET

s3://vellum-analytics-backup-prod · ACL: public-read

FINDING

A bucket used by the analytics team for nightly Postgres exports is configured public-read at the bucket ACL level. Files include encrypted PHI extracts and a JSON manifest listing every object key. Public-Access-Block is off at the account level. Object-level ACLs inherit the bucket setting. Discovered in the first eight minutes of cloud testing by OmegaWulf SCOUT.

REMEDIATION

- Enable Block Public Access at the account level; revoke bucket ACLs.
- Move snapshots to a VPC-scoped bucket and serve via signed URLs.
- Rotate database encryption keys; assume the snapshots were read by a third party.

EXTERNAL PHI CVSS 8.6 CWE-732 SCOUT · CONTINUOUS SCAN

PAGE 08 · TOOLING SPOTLIGHT · OMEGAWULF SCOUT

Three AWS findings, found before coffee.

OmegaWulf SCOUT is our proprietary AWS reconnaissance agent. It runs continuously against your estate from the first hour of the engagement, surfacing the misconfigurations that human operators would otherwise have to find by reading IAM JSON for a week. SCOUT produced three of the seven findings in this report — including two High-severity issues.

WHAT SCOUT CHECKS

Identity & access

- Wildcard PassRole / iam:* / kms:* policies
- Cross-account role trust, including unbounded externalIds
- Inactive credentials with prod-tier privileges
- Federated identity provider drift
- Conditions missing aws:SourceVpc / SourceIp

Data exposure

- S3 buckets with public ACLs or open bucket policies
- RDS / DocumentDB snapshots shared cross-account
- Public EBS snapshots and public AMIs
- Unencrypted data stores in prod-tier accounts
- SES, SQS, SNS policies allowing Principal="*"

Perimeter & exposure

- Security groups with 0.0.0.0/0 on non-public ports
- Public-facing Lambda Function URLs without auth
- API Gateway and ALB without WAF
- ECR images with critical CVEs in production
- Route 53 records pointing to unclaimed third-parties

ON THIS ENGAGEMENT

8 min	3 / 7	612	0
to first finding	findings surfaced	checks running	false positives

PAGE 09 · REMEDIATION ROADMAP

Close in this order.

Sequence chosen for impact-per-hour, not ticket count.

THIS WEEK

F-OW-2026-0042	Remove dangling go.vellum.health CNAME	CRITICAL
F-OW-2026-0058	Pin JWT verifier to RS256; rotate signing keys	CRITICAL
F-OW-2026-0071	Enable Block Public Access on the prod account	HIGH

THIS SPRINT

F-OW-2026-0051	Tenant-scope the patient lookup at the data layer	HIGH
F-OW-2026-0078	Scope CIDeployer iam:PassRole to specific roles	HIGH
F-OW-2026-0063	Disable GraphQL introspection in prod; add depth limit	HIGH

THIS QUARTER

F-OW-2026-0091	Revoke RDS snapshot share; investigate via CloudTrail	MEDIUM
PROACTIVE	Add SCP denying PassRole to roles tagged tier-0	INFO
PROACTIVE	Add Config rule for cross-account RDS / EBS shares	INFO

PAGE 10 · ENGAGEMENT METADATA

Receipts.

Engagement parameters, tooling, and chain-of-custody.

ENGAGEMENT		PACK	
ID	OW-2026-Q2-07	LEAD	M. Andersen · Pack 02
CLIENT	Vellum Health, Inc.	OPERATORS	6 · web, API, cloud
WINDOW	12 May – 02 Jun 2026	AUTOMATION	OmegaWulf SCOUT (AWS)
ENG. LETTER	MSA-2026-Q2-07-amend-1	CONTACT	engagements@omegawulf.com
DEBRIEF	09 Jun 2026, 10:00 PT	PGP	0xA019 3E72 8C1B 4FD5
RETENTION	Destroyed 31 Aug 2026	REPORT V.	1.0 — Final

TOOLING & TECHNIQUES

RECON	subfinder, amass, OmegaWulf SCOUT, Route 53 audit, Burp Suite
EXPLOITATION	Burp Suite Pro, custom Python harness, jwt_tool, sqlmap, ffuf
CLOUD	OmegaWulf SCOUT, cloudsplaining, prowler, aws-iam-actions
CHAIN-OF-CUSTODY	All artefacts retained in encrypted operator vault until 31 Aug 2026

NEXT

Closed findings should be re-tested before the engagement window closes. OmegaWulf SCOUT remains attached to the AWS estate for 30 days post-engagement at no additional charge — alerts route to your Slack workspace.