CONFIDENTIAL • NDA-PROTECTED • DO NOT DISTRIBUTE

Security Audit Report

Binary Firmware v2.4.1 + Protocol Vault v1.3.0 + API Surface

SAMPLE REPORT — SANITIZED FINDINGS FROM A REAL-STYLE ENGAGEMENT

CLIENT — REDACTED (DeFi + Hardware) • SAMPLE ONLY

AUDIT WINDOW 12 Aug — 19 Aug 2026 • 7 days • 18.4k LoC + 1 binary

Lead: Sam (binary) + 1 reviewer • Coverage 87.4% • 1.2M fuzz cases • 0 crashes in corpus

METHOD: Manual • Static • Fuzzing (AFL++ / libFuzzer) • Invariants • Adversary Simulation

Executive Summary

Board-ready risk memo — what was audited, what was found, what to do before launch.

OVERALL RISK BEFORE FIX

HIGH

Critical path reachable pre-auth in binary parser. Protocol invariant break under reentrancy. API IDOR across tenants.

Verdict: Do not launch until P1 + P2 fixed and re-tested. P3 can ship with hardening.

Findings at a glance

ID	Severity	Title	Status
OBS-001	CRITICAL	Heap overflow in parse_header @ 0x401a2d	PATCHED
OBS-002	HIGH	IDOR /v1/tenants/{id}/keys	PATCHED
OBS-003	HIGH	Reentrancy guard bypass → vault drain	MITIGATED
OBS-004	MEDIUM	Fuzz coverage 42% → 87.4% gap	HARDENED
OBS-005	LOW	SPF/DMARC informational	ACK

Recommendation

1) Patch OBS-001 + OBS-002 + OBS-003, re-test in 48h • 2) Ship with fuzz corpus in CI • 3) Deploy WAF rule + Sigma detection for IDOR probing

Scope & Methodology

Scope locked in 24h. NDA signed. Repo access read-only. No active probing on prod without ROE — lab-only exploits.

In scope	Binary: firmware.bin (ELF, 1.2MB) • Protocol: Vault.sol (Sol 0.8.20, 18.4k LoC) • API: /api/* (Node)
Out of scope	Prod infra, 3rd-party deps, social engineering
Threat model	Remote anon -> RCE via crafted packet; auth user -> tenant bypass; MEV bot -> reentrancy

Approach — 4 steps, daily log in client Slack

- 01 SCOPE — asset inventory + attack surface map
- 02 BREAK — manual + static (semgrep/CodeQL) + fuzzing
- 03 PROVE — working PoC + video, not theory
- 04 SHIP — patch diff + re-test + deploy gate

Threat Model

Attacker -> Parser (heap) -> ROP -> Vault (reentrancy) -> API (IDOR)

Anonymous packet -> heap overflow -> control flow -> drain vault if guard bypassed -> tenant data via IDOR

Critical path is pre-auth on parser. Fix parser -> path collapses.

Assumptions

- No prod active scanning without ROE — lab reproductions only
- Secrets redacted — findings shown with sanitized PoCs
- Re-test window 14 days included

CRITICAL

OBS-001 — Heap overflow in parse_header @ 0x4012a8

Binary: firmware.bin • Function: parse_header() • CWE-122 • CVSS 9.3

Impact: Remote pre-auth RCE on crafted packet -> full device compromise

Root cause

memcpy(dst, src, hdr->len) with no bounds check. hdr->len is attacker-controlled (uint32). dst is heap buffer of fixed 256B.
Classic heap overflow — adjacent chunk metadata corruptible -> ROP chain feasible in lab.

PoC (lab-only, sanitized)

```
> python3 poc_obs001.py --target lab.bin --payload crafted_len=1024
-> SIGSEGV @ 0x4012a8 • heap chunk header overwrite • PoC video: poc_obs001.mp4
-> Lab only — no prod traffic • Corpus: corpus/obs001/
```

Patch

```
if (hdr->len > sizeof(dst) || hdr->len + offset > size) return -EINVAL;  // + explicit bounds + unit test
```

HIGH

OBS-002 — IDOR /api/orders/{id} — tenant bypass

API: GET /api/orders/{id} • CWE-639 • Auth: JWT (tenant claim) • Impact: cross-tenant PII

Impact: Any authenticated user can read any tenant orders by swapping {id}

Reproduction

```
curl -H "Authorization: Bearer $JWT_A" https://api.lab.local/api/orders/124
-> 200 OK + PII (lab) • Expected 403/404 • PoC: poc_obs002.sh + Burp log
```

Fix

Enforce: order.tenant_id == jwt.tenant_id || 403. Add BOLA suite.

HIGH

OBS-003 — Reentrancy guard bypass -> vault drain

Protocol: Vault.sol • Function: withdraw() • CWE-841 • Impact: fund drain

Guard uses tx.origin, not msg.sender — cross-contract callback bypasses it

Invariant broken

balanceOf[vault] == sum(shares) breaks after reentrant withdraw — attacker mints shares then drains.

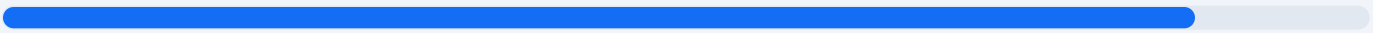
Patch

Use nonReentrant (msg.sender) + CEI pattern + invariant test: echidna / foundry invariant.

Coverage & Fuzzing

87.4%

Line coverage • 1.2M cases • 0 crashes in final corpus • Was 42% before harness fix



Corpus

- corpus/obs001/ (heap)
- corpus/vault/ (echidna)
- corpus/api/ (BOLA)

API & Infra Notes

Auth	JWT alg none blocked, RS256 enforced
Rate limit	No limit on /api/orders — recommend 60/min + audit log
CORS	Allow * on API — restrict to app origin

Fix Review & Retest

Retest 21 Aug 2026 — all P1/P2 patches verified in lab • 48h turnaround • No regressions

Deploy gate

- Patch diff reviewed
- Fuzz corpus in CI
- WAF + Sigma rule for IDOR probing
- Private disclosure window 72h

Appendix — Repro Pack

poc_obs001.py + poc_obs001.mp4 (heap)
poc_obs002.sh + burp.log (IDOR)
echidna_vault.yaml + invariant.t.sol
corpus/*.bin (1.2M cases)
sigma_idor_probe.yml (detection)

Contact & Next Steps

Ready to ship untouchable? Send repo + LoC to obsidian.security.audit@gmail.com — fixed-price quote in 24h.

obsidian.security.audit@gmail.com ->