Codebase Health & Security Audit Report

Date: 2026-02-11
Ref: GitHub Issue #5

Executive Summary

This report details three critical findings identified during the recent codebase scan of 'My-hq'. These issues affect application stability, user experience, and API security.

1. Memory Leak Risk (Frontend)

SEVERITY: MEDIUM

Observation: The real-time log subscriptions in `app/page.js` append new events/messages to the state array indefinitely.

Impact: If the dashboard is left open for extended periods (hours/days), the browser memory usage will grow until the tab crashes or becomes unresponsive.

Recommendation: Implement a "sliding window" buffer to keep only the last 50-100 items.

```
setEvents(prev => [...prev, payload.new].slice(-50));
```

2. Audio Autoplay Blocking (UX)

SEVERITY: LOW

Observation: The application attempts to play sound effects (beeps) immediately upon state changes. Modern browsers (Chrome/Safari) block `AudioContext` until the user explicitly interacts with the page (click/tap).

Impact: Sound effects may fail silently or generate console warnings until the user clicks somewhere on the dashboard.

Recommendation: Add an "Enable Audio" button or visual indicator to explicitly capture the user gesture before attempting playback.

3. Unsecured API Endpoints (Backend)

SEVERITY: CRITICAL

Observation: The API routes `app/api/dispatch/route.js` and `app/api/gateway-bridge/route.js` are publicly exposed and do not verify any authentication headers or signatures.

Impact: Any actor with the URL can:

- Dispatch arbitrary commands to agents.
- Inject fake events into the dashboard.
- Corrupt the application state.

Recommendation: Implement API Key verification (e.g., `x-admin-key` header) or a shared secret validation immediately.