Unauthenticated Source Priorities Manipulation

Moderate **tkurki** published **GHSA-gfmv-vh34-h2x5** yesterday

Package

signalk-server (npm)

Affected versions	Patched versions
All versions prior to a fix	v2.24.0-beta.1

Description

Summary

The SignalK Server exposes an unauthenticated HTTP endpoint that allows remote attackers to modify navigation data source priorities. This endpoint, accessible via `PUT /signalk/v1/api/sourcePriorities`, does not enforce authentication or authorization checks and directly assigns user-controlled input to the server configuration.
As a result, attackers can influence which GPS, AIS, or other sensor data sources are trusted by the system. The changes are immediately applied and persisted to disk, allowing the manipulation to survive server restarts.

Affected Component

- **File**: `src/serverroutes.ts`
- **Endpoint**: `PUT /signalk/v1/api/sourcePriorities` (also accessible at `/skServer/sourcePriorities`)
- **Lines**: 1064-1076
- **Function**: Source priorities configuration handler

Vulnerable Code

```
// src/serverroutes.ts - Lines 1064-1076
app.put(
```

```
    `${SERVERROUTESPREFIX}/sourcePriorities`,
    (req: Request, res: Response) => {
      app.config.settings.sourcePriorities = req.body
      app.activateSourcePriorities()
      writeSettingsFile(app, app.config.settings, (err: any) => {
        if (err) {
          res
            .status(500)
            .send('Unable to save to sourcePrefences in settings file')
        } else {
          res.json({ result: 'ok' })
        }
      })
    }
  )
```

Vulnerability Characteristics

Missing Authentication: The endpoint has zero authentication middleware, allowing unauthenticated access from any network-adjacent attacker.
Direct Configuration Assignment: User-supplied request body is directly assigned to app.config.settings.sourcePriorities without validation or sanitization.
Persistent Storage: Malicious configuration is written to disk via writeSettingsFile(), ensuring changes survive server restarts.
Live Configuration Update: Changes take effect immediately via activateSourcePriorities(), affecting live navigation data processing.
No Input Validation: No JSON schema validation, type checking, or field allowlisting is performed on the request body.

Impact

- **Navigation Data Manipulation**: Attackers can modify source priorities to change which existing, active source's data is being used

Severity

Moderate

CVE ID

CVE-2026-33951

Weaknesses

▶ CWE-284
▶ CWE-306

Credits

VashuVats Reporter