PRE-PRODUCTION SECURITY REVIEW · ROUND 2 · RE-TEST COMPLETE

Security review: Kestrel Driver API v2 and Dispatch web

We tested the driver API, the dispatch web app and the driver app before the Duisburg rollout. Nine findings, one of them high. The high finding (a driver could post proof of delivery for someone else's stop) is fixed and re-tested. Two items are still open; neither blocks the rollout.

SAMPLE DOCUMENT · KESTREL FREIGHT IS A FICTIONAL CLIENT

Window 22 Sep – 2 Oct 2026 · re-test 9 Oct
Team 2 testers (Techsy) · 1 reviewer (Kestrel IT)
Targets api-driver.kestrelfreight.eu · dispatch.
Approach Grey box, 3 driver accounts, 2 depots
Build api 2.4.0-rc3 · web 1.19 · app 2.4 (241)
Distribution Kestrel IT, Techsy; not public

0 critical · **1** high · **3** medium · **5** low · **6** fixed · **2** in progress · **1** accepted

241 /286 ASVS L2 controls applicable · **238** pass

1,412 packages scanned · **1** known CVE

Ship, with two follow-ups.

The driver API is fit for the Duisburg rollout. The one high finding is closed and could not be reproduced on 9 Oct. KST-SEC-04 (viewer role can export shipper contacts) must close before the CRM module opens to the sales team on 20 Oct; KST-SEC-08 (unencrypted photo cache on Android) is scheduled for app 2.4.1. Nothing we found allowed access without a valid Kestrel account.

Findings

9 TOTAL · ORDERED BY SEVERITY

ID	SEVERITY	FINDING	STATUS	CLOSED
KST-SEC-02	HIGH	Any authenticated driver could post proof of delivery for a stop not assigned to them (object-level authorisation missing). Driver API · POST /v2/stops/{id}/pod	Fixed	9 Oct
KST-SEC-01	MEDIUM	Driver refresh tokens lived 90 days and were not rotated on use; a copied token stayed valid after the driver logged out. Driver API · auth	Fixed	1 Oct
KST-SEC-03	MEDIUM	No rate limit on the SMS one-time-code endpoint; 600 requests in a minute were accepted (cost and code-guessing risk). Driver API · POST /v2/auth/otp	Fixed	30 Sep
KST-SEC-04	MEDIUM	CSV export of shipper contacts ignores the account scope of the "viewer" role; a viewer at Venlo could export Duisburg accounts. Dispatch web · CRM export	In progress	due 17 Oct
KST-SEC-05	LOW	No Content-Security-Policy header on the dispatch web app; inline scripts allowed. Dispatch web · headers	Fixed	26 Sep
KST-SEC-06	LOW	Error responses included Postgres constraint names and table names. Driver API · error handler	Fixed	26 Sep
KST-SEC-07	LOW	fast-xml-parser 4.3.x (CVE-2024-41818, regex DoS) used by the CMR import; bumped to 4.5.x. Dependencies · dispatch web	Fixed	24 Sep
KST-SEC-08	LOW	Proof-of-delivery photos waiting for sync are cached unencrypted on Android external storage. Driver app · Android	In progress	app 2.4.1
KST-SEC-09	LOW	Public Mapbox token carries styles:read beyond the minimum; URL-restricted to kestrelfreight.eu, rotated quarterly. Dispatch web · third party	Accepted	risk owner: Kestrel IT

SCOPE

- **Driver API v2**: Node 22 / Fastify, Postgres 16 with row-level security, 41 endpoints.
- **Dispatch web**: Next.js 16, SSO via Entra ID, roles dispatcher / planner / viewer / admin.
- **Driver app** 2.4: Flutter, iOS 16+ and Android 10+, offline queue.
- **CRM module**: shipper accounts, contacts, rate cards (read paths only this round).

METHOD

- **OWASP ASVS 4.0.3, Level 2** checklist against code and config; 241 controls applicable.
- **Dependency scan**: pnpm audit, OSV-Scanner and Trivy on the three container images.
- **Pen-test of the driver API**: 4 days grey box with three driver accounts across both depots; Burp Suite, custom scripts, authorisation matrix of 41 × 4 roles.
- **Mobile static review**: MobSF on both store builds, storage and transport checks.

SEVERITY SCALE

Critical data of all shippers, or no auth needed
High cross-driver or cross-account access
Medium abuse needs an account; limited data
Low hardening, hygiene, defence in depth

KST-SEC-02 · Proof of delivery accepted for stops not assigned to the driver

HIGH | CWE-639 | ASVS 4.2.1 | Fixed · re-tested 9 Oct

EVIDENCE

Driver account A (Venlo) posted a signature to stop 88214, assigned to driver B (Duisburg). The API checked the token but not stop ownership. The stop moved to "Delivered" on the dispatch board with A's signature attached.

```
# driver A's token, driver B's stop
POST /v2/stops/88214/pod HTTP/1.1
Authorization: Bearer eyJhbGciOi…(driver A)
Content-Type: application/json

{"signedBy":"S. de Vries","pallets":12,"photoIds":["ph_7e1"]}

HTTP/1.1 201 Created
{"stopId":88214,"status":"delivered","podId":"pod_41a9"}
```

Impact. A driver, or anyone holding a driver token, could mark any of the roughly 1,100 daily stops delivered and attach a false signature. Invoicing runs off delivered status, so this reaches billing.

FIX

Ownership check in the handler and a matching row-level security policy, so the database refuses the write even if a future handler forgets to check.

```
// stops/pod.ts
const stop = await db.stop.findFirst({
  where: { id, assignedDriverId: req.driver.id,
           status: { in: ["en_route","arrived"] } }
});
if (!stop) return reply.code(404).send();

-- migration 0412_pod_rls.sql
CREATE POLICY pod_insert_own_stop ON proof_of_delivery
  FOR INSERT WITH CHECK (
    stop_id IN (SELECT id FROM stops
      WHERE assigned_driver_id = current_driver_id()));
```

Re-test. Same request now returns 404 (not 403, so stop IDs are not enumerable). 41 endpoints re-run through the authorisation matrix: `164 / 164 pass`. Audit log shows 0 cross-driver PODs in production history since 1 Jan 2026.

What's left to watch

OWNERS AND DATES AGREED 9 OCT

KST-SEC-04 before CRM opens to sales

Scope the export query by account visibility, same as the list view. Add a test that a Venlo viewer gets 0 Duisburg rows.

OWNER TECHSY · DUE 17 OCT

KST-SEC-08 in app 2.4.1

Move the sync queue to app-private storage with the platform keystore; wipe on sign-out. Verify with MobSF before the store build.

OWNER TECHSY · DUE 31 OCT

Token rotation in the field

Watch the refresh-token rotation (KST-SEC-01) for a week of real shifts; drivers with poor signal must not get logged out.

OWNER KESTREL IT · REVIEW 20 OCT

Next round

CRM write paths and the AI dispatch assistant's tool access (rate card, Dispatch API) once those ship. Repeat dependency scan monthly in CI.

PLANNED · DEC 2026