Bilko — MC #105163 multi-tenant E2E verdikt (2026-07-10): test-harness identity bug, ne RLS leak

MC #105163 — Multi-Tenant E2E Verdikt (2026-07-10)

Zaklju?ak

FALSE-POSITIVE test signal, ne stvarna RLS/tenant-isolation ranjivost.

E2E multi-tenant-isolation failures su uzrokovani bug-om u test harness-u (`loginViaApiInject` ignoriše `_user` parametar), ne backend tenant leak-om. Bilko RLS i org-scoped WHERE klauzule RADE ISPRAVNO.

Root Cause — Test Identity Bug

`apps/e2e/tests/multi-tenant-isolation.spec.ts` poziva `loginViaApiInject(page, _user)` gdje je `_user` parametar (leading underscore = namjerno nekorišten) **ignorisan**. Funkcija uvijek poziva `getCiamSessionTokens()` koja vraća token za **jedan hardkodiran CIAM identitet** (`E2E_TEST_EMAIL`, default `bilko-e2e-test@bilkociam.onmicrosoft.com`).

Posljedica:

- "demo@bilko.rs" i "ci@bilko.rs" u ovom testu su **ista organizacija**
- Test koji provjerava "ci@bilko.rs vidi demo org fakture" — normalno PASS jer gleda SVOJE fakture

- Test koji provjerava "cross-tenant POST /invoices/send ne vraća 404" — normalno FAIL jer šalje SVOJU fakturu

Fajl `auth-ciam.ts:34-40` već dokumentuje ovo: "Both DEMO_USER and CI_USER map to the same CIAM test session."

Dvostruka Verifikacija

1. Parisa Tabriz (Securion) — Kod Analiza

- Helper ignoriše `_user` param
- Jedan CIAM email za sve test korisničke uloge
- Application kod je **org-scoped**: `InvoiceService` ima WHERE `organizationId` + `orgTransaction` postavlja `SET LOCAL app.current_org_id`
- RLS policies su aktivne i ispravne

2. John — Grep Nezavisna Provjera

```
# multi-tenant-isolation.spec.ts:54 — param = _user (ignoriran)
# getCiamSessionTokens koristi E2E_EMAIL hardkodiran (auth-ciam.ts:48)
# Komentar :39 to priznaje
```

3. John — Log Provjera Build 356

Živi log build 356: **NULA** `[demo-auth] 429` događaja.

Parisin "429count=30" bio grep artefakt (test-ime "register: 429 mocked"). MC #105128 demo fix RADI.

RLS Sentinel Potvrda

Contacts RLS sentinel: 404 PASS 3/3

RLS policy na `contacts` tabeli BLOKIRA cross-tenant pristup kako treba. Multi-tenant test failures nisu pokazatelj RLS problema.

Backend Org-Scoping — Funkcionalan

InvoiceService.kt

`getInvoice()` (line 361) radi unutar `orgTransaction(organizationId)` i filtrira:

```
Invoices.selectAll().where {
  (Invoices.id eq invUuid) and
  (Invoices.organizationId eq orgUuid)
}
```

Bacuje `NotFoundException` na bilo koji org mismatch, što route hvata i mapira u 404.

OrgScopeSessionVariable.kt

`orgTransaction()` dodatno postavlja Postgres session-scope varijablu za RLS defense-in-depth:

```
SET LOCAL app.current_org_id = '<org-uuid>';
```

Ovaj kod je stabilan od 2026-07-06 (commit e6180f25), predates build 356, i prisutan je na trenutnom HEAD.

Sekundarni Gap (niži severity, NE prijavljeni signal)

`POST /invoices/{id}/send` **NE poziva** `call.requireOrgOwnership(...)` kao što `/pdf`, `/status`, `PUT /{id}`, i `DELETE /{id}` rade.

Funkcionalno još uvijek vraća 404 ispravno (via `getInvoice` WHERE-clause), ali:

- Nema `SECURITY_VIOLATION` audit-log unos za cross-tenant `/send` probe (audit-log parnost gap)
- Nema **live HTTP integration test** (`testApplication` + pravi client + pravi DB) koji dokazuje ovo na wire nivou za `/send`

Follow-up Taskovi

MC #105165 — Test Identity Fix

Pravi drugi CIAM identitet za `ci@bilko.rs`:

- Whitelist `E2E_TEST_EMAIL2` + seed `entra_external_identities`
- ILI backend RLS integracijski test (dva `org_id`, assert row visibility)

MC #105166 — Hardening

Dodati `requireOrgOwnership` na `POST /invoices/{id}/send`:

- Jedini write route bez eksplicitnog guard-a
- Oslanja se na `getInvoice` org-scope — nije aktivni vuln
- Defense-in-depth konzistentnost + audit-log parnost

MC #104962 — DEMO_READ_ONLY

Instant-demo write-protection 5 failures — zaseban uzrok, nije 429 (log potvrdio). `DEMO_READ_ONLY` gate u `TrialGatePlugin.kt` izgleda ispravan (Parisa Read). Treba zaseban pogled, nije hitno.

Fajlovi Pro?itani (Tool-Verified)

- `apps/e2e/tests/multi-tenant-isolation.spec.ts`
- `apps/e2e/tests/helpers/auth-ciam.ts`
- `apps/api/src/main/kotlin/no/alai/bilko/routes/InvoiceRoutes.kt`
- `apps/api/src/main/kotlin/no/alai/bilko/services/InvoiceService.kt`
- `apps/api/src/main/kotlin/no/alai/bilko/features/TrialGatePlugin.kt`
- `apps/api/src/test/kotlin/no/alai/bilko/routes/CrossTenantIsolationTest.kt`
- `apps/api/src/test/kotlin/no/alai/bilko/routes/OrgScopeIsolationTest.kt`
- Git log na `InvoiceService.kt` / `InvoiceRoutes.kt` (commit e6180f25, HEAD 46a3082a)

Reference

- **Source Evidence:**
  - `/Users/makinja/system/evidence/105163/verdict.md`

    - `/Users/makinja/system/evidence/105163/read-only-investigation.md`
    - `/Users/makinja/system/evidence/104960/build356-comparison.md`
- **Related Tasks:**
    - MC #105163 (ovo), MC #105165 (test fix), MC #105166 (hardening), MC #104962 (DEMO_READ_ONLY)
- **Build Comparison:** 341→349→356 (71→33→29 failures, 39.6m→12.8m)

Datum: 2026-07-10
Analiza: Parisa Tabriz (Securion) + John (nezavisna verifikacija)
Confidence: High — bazirana na direktnom čitanju koda, ne pretpostavkama

---

Revision #2
Created 2026-07-10 14:06:21 UTC by John
Updated 2026-08-10 07:37:35 UTC by John