

Bilko — Entra OAuth hardening audit (2026-07, MC #105975)

Bilko — Entra OAuth hardening audit (2026-07)

MC: #105975 · **Auditor:** Parisa Tabriz (Securion) · **Peer-verify:** 6/7 PASS (nezavisni verifier) · **Verdict:** **FINDINGS** (2 low, 0 high/critical)

Povod: živa kampanja OAuth Client ID spoofinga (validacija ukradenih Entra kredencijala lažnim client ID-evima), TLDR/Proofpoint/THN 2026-07. Napomena o izvoru: MS blog o ShinyHunters (2026-07-13) je Salesforce-specifičan — audit rađen po OWASP OAuth 2.0 BCP okviru, ne po tom članku.

Rezultat

- **10 OK / 2 FINDING / 6 NEEDS-LIVE-TENANT** (Bilko krak) + QODY = N/A (nema Entra; JWT HS256+argon2id+TOTP; grep dokaz 0 referenci).
- **Jaka srž (potvrđena i John probe-om i peer-verifyjem):** backend server-side pinuje audience+issuer (`EntraExternalIdService.kt:129-130`), JWKS domain-pin na `*.ciamlogin.com/login.microsoftonline.com` (startup + per-call, fail-closed `IllegalStateException`); CSP connect-src IdP = tačno ta 2 hosta; `/dashboard 307` → `/login` za neautentifikovane.

Nalazi

1. **(LOW-MED, korigovan peer-verifyjem)** `/auth/entra/session` exchange IMA per-IP rate-limit (`rateLimit(RateLimitName("auth"))`), ~5/min, MC #103075 D4 komentar u `Routing.kt` — stvarni ostatak gapa: **nema per-identity/per-oid throttle** za returning usere; distribuirani replay preko više IP-ova zaobilazi per-IP limit. Preporuka: per-oid throttle ili Front Door pravilo.
2. **(LOW)** `CORS.kt:15` fail-open fallback na hardkodiranu default origin listu kad `CORS_ORIGINS` nije postavljen (uz `allowCredentials=true`), nekonzistentno s fail-closed patternom

EntraExternalIdService-a. Preporuka: baciti exception na missing config (isti pattern).

NEEDS-LIVE-TENANT follow-up (samo portal/Graph — 6 stavki)

Entra App Registration redirect URI allowlist · Conditional Access policy stanje · passkey/WebAuthn tenant default · stvarni CORS_ORIGINS po ACA reviziji · ingress rate limiting (Front Door/ACA) · sign-in/consent audit logovi. (az ad/Graph blokiran iz agentskih sesija — ovo je imenovani CEO/portal korak.)

Evidence

`~/system/evidence/105975/` — parisa-entra-audit-2026-07-18.md (23 statusirane stavke), peer-verify-transcript-2026-07-18.md (7 atomskih tvrdnji, sirovi outputi), gotcha-task-105975.md, verdict-105975.json (sha256 kontrakt). Vezano: #104547 QODY httpOnly JWT zatvoren istim danom (Proveo 10/10 UAT + Parisa re-grep).

Revision #2

Created 2026-07-18 10:51:40 UTC by John

Updated 2026-08-10 07:37:43 UTC by John