INCIDENT — dev@alai.no mailbox + plaintext kredencijali (2026-07-30)

INCIDENT — dev@alai.no mailbox + plaintext kredencijali (2026-07-30)

Status: OTVOREN — DJELOMIČNO SANIRAN, KRITIČAN PASSWORD-REUSE. Migadu i Google `dev@alai.no` kredencijali rotirani su 2026-08-01; ostaju provider rotacije sedam naloga sa ponovljenom lozinkom, Gmail app-password i Git-history cleanup. Vlasnik: John (AI Director). **MC taskovi: #106589 (plaintext credentials), #106590 (dev IMAP outage), #106591 (Google alert 23.06), #106592 (OAuth verifikacija).**

Sve u ovom dokumentu je tool-verifikovano tokom sesije 2026-07-30 (17:00–23:10 CEST). Ništa nije iz sjećanja.

Izvršni sažetak

1. **dev@alai.no IMAP autentikacija pada od 20:17:40 CEST** — lozinka iz Vaultwardena koja je radila u 20:16:19 od tada je odbijena. Trezor nepromijenjen i sinhronizovan; CEO izričito NIJE mijenjao lozinku; pad traje ~3h (isključuje tipični rate-limit). **Radna hipoteza: lozinka/stanje naloga promijenjeno na Migadu strani — mogući kompromis naloga.**
2. **Google security alert od 23.06** na istom sandučiću: "*Someone just used your password to try to sign in — Google blocked them.*" Prijava s **tačnom lozinkom**, blokirana. **37 dana neobrađeno**, ništa rotirano. U kombinaciji s (1) — tretirati kao vjerovatan kompromis.
3. **Plaintext mail kredencijali van trezora**, tracked u gitu i push-ovani na GitHub remote (`alai-system`, privatan): `config/email-accounts.json` (bio world-readable ~3,7 mjeseca), `config/mail-credentials-dev.json`, plus **kompletan bw export s lozinkama** u

`evidence/105489/bw-lumiscare-search.json`. Kopije u 3 worktreea.

4. **Google OAuth verifikacija (snowit-seo-portal) mrtva 43 dana** — MC #103811 zatvoren kao done 17.06, a odgovor Googleu **nikad nije poslan** (dokazano živim IMAP pregledom svih Sent foldera).
5. Sistemski uzrok nevidljivosti: **inbox-watcher triage ne pomjera status** (poznat kvar, BookStack "Mail Pipeline E2E Debug MC #105892") — 528 poruka `new` / 0 `triaged` u 14 dana. Google alert je 37 dana ležao u redu koji niko ne prazni.

Timeline 2026-07-30 (CEST; svi unosi tool-verifikovani)

vrijeme	događaj	izvor
20:08:24	daemon: dev fetch OK	email-agent-launchd.log:25868
20:14:31	daemon: `Connected to dev (dev@alai.no)`	log:25907
20:16:19	John test: **IMAP OK + SMTP OK** (baseline)	mail-native test
20:17:40	John test: `1 NO Authentication failed`	mail-native test
20:19:42	dev pada; **alem/john/gmail OK u istoj sekundi**	mail-native test ×4
20:20–20:27	daemon: `IMAP error (dev): Command failed` ×3	log:25947,25957,25996
20:25:08	`bw sync` odrađen — bez efekta	bw status lastSync
20:28:30	i dalje pada (11 min pauze)	mail-native test
21:02–21:08	daemon: socket timeout / command failed	log:27075–27115
23:08:34	**i dalje pada — ~2h51min od početka**	mail-native test

Šta je dokazano / isklju?eno

- **Nije kvar alata**: ista komanda, ista sekunda — 3 druga naloga rade.
- **Nije zastarjeli lokalni trezor**: `bw sync` odrađen (lastSync 2026-07-30T18:25:08Z), bez promjene.
- **Nije John-only**: nezavisni daemon (email-agent) pada identično.

- **Nije CEO**: izričito potvrdio da lozinku nije mijenjao. (Prvobitni "test promjene lozinke" je bio false positive — lozinka nikad nije promijenjena, a pad se svejedno desio.)
- **Rate-limit (Migadu brute-force zaštita) oslabljen kao objašnjenje**: John jeste napravio 4 uzastopna logina u minuti prije pada (+ ~10 kroz dan), i runbook dokumentuje "wait 5 minutes" — ali pad traje ~3 sata.
- **Ostaje**: promjena lozinke/stanja naloga na Migadu strani, ne od CEO-a.

Sljede?i korak koji sve razlu?uje (CEO, ruke)

Migadu admin panel → dev@alai.no → datum zadnje promjene lozinke + log prijava/blokada.

- Lozinka nije dirana + vidi se blokada → uzrok je nalet logina, čeka se istek.
- Lozinka mijenjana danas → **potvrđen incident**, odmah: rotacija kroz Migadu admin, pregled forwarding/alias pravila, pregled ostalih naloga na istoj domeni.

NE raditi: dalje login pokušaje na dev@alai.no (produžavaju blokadu ako je rate-limit).

Google security alert 23.06 (MC #106591)

- email-inbox.db id=11864, `2026-06-23T08:23:25Z`, from `no-reply@accounts.google.com`, subject "Critical security alert", status `new`, bez MC taska do 30.07.
- Tijelo doslovno: "*Someone just used your password to try to sign in to your account. Google blocked them.*"
- Dodatni neobrađeni "Security alert" mailovi u dev sandučiću: id 9686/9692/9697/8939/8944/1263/1265 (april–juni).
- **Traženo**: Google account activity pregled, rotacija, 2FA, provjera da li je ista lozinka dijeljena s Migadu mailboxom.

Plaintext kredencijali (MC #106589)

fajl	stanje 30.07 prije fixa	poslije fixa
`~/system/config/email-accounts.json`	`-rw-r--r--` (world-readable), 457 B, od 08.04	`600` ✔

fajl	stanje 30.07 prije fixa	poslije fixa
`~/system/config/mail-credentials-dev.json`	`600`, 204 B, od 22.02	`600` ✔
`~/system/evidence/105489/bw-lumiscare-search.json`	`-rw-r--r--`, **puni bw export, login.password plaintext, 2 stavke**	`600` ✔
kopije u worktreeovima flowforge-105961, flowforge-105761, codecraft-106322	`-rw-r--r--`	sve `600` ✔

- **Git**: sva tri tracked (`git ls-files`), u historiji od initial commita + backup commiti 18.02/22.02/08.04, **prisutni na `refs/remotes/alai-system/main`** (github.com/johnatbasicas/alai-system, privatan — anonimni GET 404).
- **Nemaju potrošača**: nijedan .js/.sh/.plist u ~/system ih ne referencira (izvan worktreeova) — mrtvi ostaci od prije migracije na Vaultwarden. Kanonski izvor kredencijala JESTE Vaultwarden (`mail-native.js` čita isključivo BW; CEO potvrdio 30.07).
- **Sadržaj fajlova NIJE čitan** (permission gate) — polje lozinke utvrđeno pattern-matchom. Prije rotacije utvrditi koje naloge sadrže.
- **Urađeno 30.07**: chmod 600 svih 11 kopija; `.gitignore` dopunjen (`config/email-accounts.json`, `config/mail-credentials-dev.json`, `config/*credentials*`, `evidence/**/bw-*.json`) — verifikovano `git check-ignore --no-index`. Stari `.gitignore` je imao `config/mail-credentials.json` ali NE `-dev` varijantu — zato je promakla.
- **Čeka CEO**: `git rm --cached` + odluka o scrubu historije (fajlovi su na remote main; scrub = force-push), rotacija sadržaja.

OAuth verifikacija snowit-seo-portal (MC #106592)

- 17.06 Google traži reply s linkom na bolji demo video (projekat 337804838184).
- MC #103811 zatvoren `done` isti dan; u mail bazi `status=responded` + `draft_id=153` — **ali draft nikad nije poslan**.
- Dokaz: živi IMAP pregled Sent foldera 30.07 — dev Sent PRAZAN; alem Sent kompletan 16.02→21.07 bez ijednog maila Googleu (oko 17.06: 15.06 → skok na 23.06); info/john bez relevantnog.
- Isti obrazac kao memo `feedback_email_responded_status_not_proof_2026-06-03`: **`responded` u mail bazi znači "draft napisan", ne "poslano"**.
- Posljedica: app na "unverified" ekranu; sensitive/restricted scopes u testing modu (7-dnevni refresh tokeni).

Sistemske lekcije (za budu?e sesije)

1. **`status=new` u email-inbox.db ne znači "nepročitano"** — fetcher markira SEEN na serveru; `new` znači "neobrađeno kod nas". Živo `unread` na IMAP = 0, a u bazi 110 `new`.
2. **Triage daemon je i dalje mrtav** (poznat kvar iz MC #105892) — kritični alarmi leže u `new` redu mjesecima. Dok se ne popravi: sigurnosne alerte tražiti eksplicitno po pošiljaocu, ne oslanjati se na triage.
3. **MC `done` bez ishodnog dokaza je laž u trackeru** — #103811 zatvoren na osnovu drafta. Slanje maila dokazuje samo Sent folder (živi IMAP), ne mail-baza status.
4. **Negativna tvrdnja ("kredencijala nema van trezora") zahtijeva enumeraciju diska**, ne čitanje jednog alata. John je 30.07 tvrdio suprotno dok CEO nije insistirao — grep je našao 11 fajlova.
5. **`git check-ignore` bez `--no-index` preskače tracked fajlove** — lažni negativ pri verifikaciji .gitignore izmjena.
6. **IMAP probe disciplina**: ne bombardovati jedan nalog uzastopnim loginima; Migadu ima brute-force zaštitu, a `NO Authentication failed` ne razlikuje pogrešnu lozinku od blokade.

AŽURIRANJE 2026-07-31 — CEO tvrdnja potvr?ena, fix shipped (MC #106589)

CEO je insistirao: "*mail reader nije koristio BW*". **Tačno — za kanonski MCP put.**

Četvrta lokacija plaintext kredencijala (nijedan raniji sken je nije našao jer je van `~/system`): `~/.config/alai/email-accounts.json` (523 B, 29.06, prava 600) — sadrži dev@alai.no, alem, john, info. `email-mcp-launch.sh` (Securion B7, MC #104502) je predviđao macOS keychain kao primarni izvor, ali **keychain stavka `alai-email-accounts` nikad nije kreirana** — plaintext fallback je bio jedini stvarni put. Dakle: CLI (`mail-native.js`) i fetch daemon (`email-agent.js`) su koristili BW; **kanonski MCP bridge (`email-mcp-bridge-v2.js`) je koristio plaintext** + mrtve one.com hostove (pre-Migadu default).

Fix (shipped + živo verifikovan):

- `email-mcp-bridge-v2.js` → Vaultwarden preko `mail-native.createImapClient/createSmtpTransport` (isti put kao daemon; bw cycle-cache MC #105900 + force-refresh na stale kredencijal). `EMAIL_ACCOUNTS` env deprecated i ignorisan (WARN u logu). Backup: `.bak-106589-20260731-081108`.
- `email-mcp-launch.sh` → ne čita ni keychain ni plaintext, samo `exec node bridge`.
- `spam-recovery-notify.js` → mail-native umjesto plaintext + mrtvog `send.one.com`.
- Verifikacija: `node --check` OK; bridge start log `Vaultwarden credentials via mail-native — MC #106589`; identičan kredencijalni put testiran živo na alem INBOX (exists=2717).

Napomena o uzroku dev pada: bridge NIJE okidač #106590 — nije startovao između 17:23 i 23:00 CEST (pad počeo 20:17), i spaja se na IMAP tek na tool-poziv. Uzrok pada i dalje nerazriješen;

presuda je u Migadu adminu.

Ostaje (CEO ruke): inventar + rotacija sadržaja 3 plaintext fajla; `git rm --cached` + odluka o scrubu historije; brisanje fajlova NAKON rotacije.

AŽURIRANJE 2026-08-01 — provider rotacija i `dev` oporavak

- Migadu API preflight potvrdio je svih pet izloženih mailboxa. Provider password i odgovarajući Vaultwarden zapis rotirani su par-po-par za `alem@alai.no`, `dev@alai.no`, `john@alai.no`, `info@basicconsulting.no` i `john@basicconsulting.no`.
- Live TLS IMAP+SMTP autentikacija nakon propagacije prolazi za svih pet; nijedna testna poruka nije poslana tim provjerama. `dev@alai.no` više ne vraća `Command failed`.
- Google password za Google račun `dev@alai.no` je rotiran, Vaultwarden ažuriran, a nova prijava i providerov događaj `Password changed` potvrđeni su na Security stranici. 2-Step Verification je aktivan.
- Uklonjeno je 13 aktivnih/worktree plaintext mail kopija i jedan puni `bw` result artefakt. Naknadni exact-value containment uklonio je legacy `EMAIL_ACCOUNTS` iz 25 MCP JSON/config kopija, izbrisao sedam dodatnih Vault-export incident fajlova, redaktovao 698 checkpoint/doc/archive fajlova (971 pojava) i uklonio Gmail app-password iz četiri retired Himalaya konfiguracije (osam pojava). Scan 125.747 aktivnih fajlova sada nalazi nula exact kopija šest kanonskih runtime mail tajni. Stari Git objekti/remote historija i dalje zahtijevaju kontrolisani history rewrite; brisanje radnih kopija nije scrub historije.
- `EMAIL_TRUSTED_AUTHSERV_IDS=mx13.migadu.com,mx.google.com` konfiguriran je za email-agent i inbox-watcher nakon uzorka 166 sačuvanih topmost `Authentication-Results` polja: Migadu 118, Google 41, neparsirano 7. Niži dupli headeri nisu korišteni za trust.
- Mail servisi su bili pauzirani tokom rotacije i svih 13 je vraćeno. Postflight: inbox/outbox integrity `ok`, 18/18 current cursora `active`, 81/81 reconciliation redova i dalje netriagirano/nepovezano, tri watcher guarda prisutna.
- **Kritični otvoreni rizik:** stari Google `dev@alai.no` password, koji je sada poništen na Googleu, identično je ponovljen u sedam drugih Vault zapisa: AWS Console, Cloudflare, Figma Login, GitHub, Microsoft Azure / Founders Hub, Penpot i Vercel. Poređenje je izvršeno bez ispisivanja vrijednosti. Read-only recovery preflight potvrđuje aktivne CLI sesije za AWS, Azure, Vercel i Cloudflare; GitHub CLI nije prijavljen; Figma/Penpot nemaju provjeren lokalni account-management CLI. Provider password stanje nije potvrđeno i svih sedam se moraju tretirati kao kompromitovani dok se ne rotiraju uz odgovarajuću 2FA/ownership potvrdu.
- **Otvoreni mail rizik:** `alembasic@gmail.com` runtime koristi 16-znakovni Google app-password koji je bio u historijskom plaintext fajlu. Vault nema glavni credential tog Google računa, a Google je blokirao automatizovani recovery flow. Ne brute-forceati. Vlasnik mora iz već prijavljenog Chrome Profile 2 otvoriti Google Account → Security → App passwords, opozvati stari app-password, kreirati novi i odmah ažurirati Vault stavku `Email - alembasic@gmail.com`.

Evidence: `/Users/makinja/system/evidence/106589/provider-rotation-20260801T053700Z/` (mode 0600 za osjetljive izvještaje/screenshotove).

Referencirani izvori

- Živi mail store: `~/system/databases/email-inbox.db` (jedini pravi; kopije u tools/state/data su decoy stubovi — MC #105892)
- Logovi: `~/system/logs/email-agent-launchd.log`, `~/system/logs/mail-native.log`
- Runbook: BookStack "Email System Runbook" (kanonski alat: MCP `mcp__email__*`; alternativa `mail-native.js`; deprecated: email.js, email-monitor.js)
- Evidence trag ove sesije: MC #106589–#106592 tijela taskova

---

Revision #5
Created 2026-07-30 21:16:50 UTC by John
Updated 2026-08-01 07:41:47 UTC by John