LAV'S INDUSTRIES

CAUCE · SECURITY AUDIT

Remediation plan

Case Management Platform

SAMPLE REPORT · NO CLIENT DATA

Client	Client (public sector)
Scope	Sample based on a real audit, generalized
Reference	«commit reference withheld»
Run	run-1 · profile standard
Date	2026-09-23
Document	AUD-03

Remediation plan

Order of attention derived from severity and estimated effort. The blocks are worked in sequence: each one removes more risk per hour spent than the next.

Recommended structural fix

Five endpoints share a single cause: nothing checks whether the person editing already controls at least as much as they are about to grant. Patching each site separately is the minimum acceptable fix; the durable one is a shared authorization primitive called from every mutation point. The audit itself surfaced a new instance in three consecutive rounds — that is the evidence the structural fix is worth it.

Block 1 — Contain privilege escalation

These let an account with one ordinary permission take full control of the application. · **Estimated effort:** 1–2 days

SEVERITY	FINDING AND ACTION	FILES TO TOUCH
CRITICAL	**Permission-assignment endpoint with no privilege-ceiling check** SAMPLE-14 Introduce a shared privilege-ceiling check, called from every point where permissions are mutated: the operation is refused when the requested set is not contained in the actor's own, unless the actor holds the highest-privilege role.	–
CRITICAL	**Role rename with no reserved-name list allows impersonating the highest-privilege role** SAMPLE-13 Do not authorize on attributes the user can modify. Anchor the check to an immutable identifier and, as a complement, keep a reserved-name list the editing endpoint refuses.	–
CRITICAL	**User create and edit accepts a role field without validating the resulting privilege** SAMPLE-18 Apply the same privilege-ceiling check on both routes, or remove role assignment from the generic user endpoint and keep it only in the dedicated endpoint that is already correctly restricted.	–

Block 2 — Close the unauthorized routes

Routes that were left without middleware; the fix is one line and the risk is high. · **Estimated effort:** Hours

SEVERITY	FINDING AND ACTION	FILES TO TOUCH
HIGH	**Attachments served inline with a content type inferred from the file** SAMPLE-03 Force download instead of inline rendering, serve a generic content type, and deliver attachments from a separate cookieless domain so any execution has no context to abuse.	–
HIGH	**Case sub-resources do not inherit the access control of the case** SAMPLE-16 Derive sub-resource authorization from the case that contains them through an access policy, instead of declaring it route by route.	–
HIGH	**National-identifier directory readable by any authenticated account** SAMPLE-06 Add the permission check to the affected routes, scope the query to the caller's organization, and cap results per page.	–
HIGH	**Organization scoping is optional rather than enforced on lists and exports** SAMPLE-08 Make organization scope a mandatory scope applied at the model, so no query can return records outside the caller's organization except for the roles that are explicitly meant to see everything.	–
HIGH	**Permission rename allows colliding with names used in authorization decisions** SAMPLE-09 Anchor checks to immutable identifiers and treat editing the permission catalog as a highest-privilege operation.	–
MEDIUM	**A second reassignment route skips the closed-case lock** SAMPLE-11 Move the check into the shared service so every route that reassigns inherits it by construction.	–
MEDIUM	**A second reassignment route skips the organization restriction** SAMPLE-10 Centralize reassignment in a single service that holds the checks, and have both endpoints call it.	–
MEDIUM	**Closing a case validates neither the prior state nor the assignment** SAMPLE-15 Define the permitted transitions explicitly, refuse those that do not match the current state, and require that whoever closes is the assigned owner or holds a supervisory role.	–
MEDIUM	**Data export has neither rate limiting nor a per-user cap** SAMPLE-01 Add rate limiting to the route and a cap on pending jobs per user, refusing new requests while exports are still in flight.	–
MEDIUM	**Internal notes are not filtered out of the staff-facing listing** SAMPLE-05 Apply the filter in the shared query scope, and restrict who may mark a note as internal.	–

SEVERITY	FINDING AND ACTION	FILES TO TOUCH
MEDIUM	**Restoring a deleted account reinstates its previous credentials** SAMPLE-02 Revoke all active credentials on restore, exactly as on block, and require a fresh authentication.	–
MEDIUM	**Sign-in reveals account state before verifying the password** SAMPLE-07 Evaluate account state only after a successful credential check, return a generic response in every failure case, and add rate limiting to the route.	–
MEDIUM	**The user directory is exposed to any authenticated account** SAMPLE-19 Add the permission check, and limit the returned fields to what the consuming use case strictly needs.	–

Block 3 — Harden the case lifecycle

These affect workflow integrity and availability, not data exposure. · **Estimated effort:** 2–4 days

SEVERITY	FINDING AND ACTION	FILES TO TOUCH
LOW	**Reassignment does not validate that the recipient is active and eligible** SAMPLE-12 Validate the recipient's state and role before accepting the reassignment.	–

Block 4 — Confirm the pending items with your infrastructure team

They depend on a deployment fact that is not in the code. Confirming them is quick. · **Estimated effort:** 1 hour

SEVERITY	FINDING AND ACTION	FILES TO TOUCH
NEEDS VALIDATION	**Attachments stored in a location the web server may be exposing** SAMPLE-04 –	–
NEEDS VALIDATION	**Request origin may not be trustworthy behind a proxy** SAMPLE-17 –	–

Tracking

`remediation-tracker.csv` holds the same list in a format you can import into Jira, Linear or Trello: one row per finding, with severity, block, affected files and the closing criterion.

The `recommendations/` folder has one sheet per finding with the strategy, the proposed code change and the regression test that keeps it from coming back.

Closing criterion

A finding counts as closed when (1) the change is deployed, (2) an automated test exists that fails without the change and passes with it, and (3) you have verified there is no other route to the same effect. Point (3) is the one most often skipped: several findings in this report are second routes to an effect that was already guarded on its primary path.