LAV'S INDUSTRIES

CAUCE · SECURITY AUDIT

Findings — technical detail

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-02

Contents

1. Permission-assignment endpoint with no privilege-ceiling check — CRITICAL
2. Role rename with no reserved-name list allows impersonating the highest-privilege role — CRITICAL
3. User create and edit accepts a role field without validating the resulting privilege — CRITICAL
4. Attachments served inline with a content type inferred from the file — HIGH
5. Case sub-resources do not inherit the access control of the case — HIGH
6. National-identifier directory readable by any authenticated account — HIGH
7. Organization scoping is optional rather than enforced on lists and exports — HIGH
8. Permission rename allows colliding with names used in authorization decisions — HIGH
9. A second reassignment route skips the closed-case lock — MEDIUM
10. A second reassignment route skips the organization restriction — MEDIUM
11. Closing a case validates neither the prior state nor the assignment — MEDIUM
12. Data export has neither rate limiting nor a per-user cap — MEDIUM
13. Internal notes are not filtered out of the staff-facing listing — MEDIUM
14. Restoring a deleted account reinstates its previous credentials — MEDIUM
15. Sign-in reveals account state before verifying the password — MEDIUM
16. The user directory is exposed to any authenticated account — MEDIUM
17. Reassignment does not validate that the recipient is active and eligible — LOW
18. Attachments stored in a location the web server may be exposing — NEEDS VALIDATION
19. Request origin may not be trustworthy behind a proxy — NEEDS VALIDATION

SAMPLE-14

Permission-assignment endpoint with no privilege-ceiling check

CRITICAL Likelihood High · Impact Critical · Confidence High

DESCRIPTION

The endpoint that syncs a role's permissions never compares what is being granted against what the person performing the operation already holds. An account with a single narrow permission — the kind that gets delegated routinely — can grant itself every permission in the system in one call.

ROOT CAUSE

Authorization is resolved by checking for one specific permission, with no further check that the acting principal already controls at least as much as they are about to grant.

REMEDIATION

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.

SAMPLE-13

Role rename with no reserved-name list allows impersonating the highest-privilege role

CRITICAL Likelihood High · Impact Critical · Confidence High

DESCRIPTION

The application's global authorization recognizes the highest-privilege role by its name. Because the role-editing endpoint does not protect that name, a holder of an intermediate administrative permission can rename the privileged role — stripping its members — and then rename their own to take its place, effective immediately and with no re-login.

ROOT CAUSE

An authorization decision rests on a mutable attribute (the role name) that the permission model itself lets lower-privileged principals edit.

REMEDIATION

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.

SAMPLE-18

User create and edit accepts a role field without validating the resulting privilege

CRITICAL Likelihood High · Impact Critical · Confidence High

DESCRIPTION

The user create and edit operations accept a field that assigns the role directly. The role is validated to exist, but not that the caller is entitled to grant it. A holder of the ordinary user-management permissions can assign the highest-privilege role to themselves or to a third party.

ROOT CAUSE

Input validation confirms the value exists, not the authority to assign it. A dedicated role-management endpoint does exist and is correctly restricted, but this second route to the same effect was left without the same guard.

REMEDIATION

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.

SAMPLE-03

Attachments served inline with a content type inferred from the file

HIGH Likelihood Medium · Impact High · Confidence High

DESCRIPTION

Attachments are validated by extension, but the content type they are served with comes from sniffing the bytes at upload time, and they are delivered for rendering inside the browser. A file with an allowed extension whose real content is HTML executes in the application's context for anyone who opens the link.

ROOT CAUSE

Upload validation and the decision of how to serve the file use different sources: one trusts the extension, the other the content. The gap between them is the vector.

REMEDIATION

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.

SAMPLE-16

Case sub-resources do not inherit the access control of the case

HIGH Likelihood High · Impact High · Confidence High

DESCRIPTION

The parent case is correctly protected, but its sub-resources — comments, assignment history and attachments — were left with no permission check. An account denied access to the case can read and write every one of its components.

ROOT CAUSE

Authorization is applied route by route rather than derived from the parent resource, so every new sub-resource is born unprotected unless someone remembers to add it.

REMEDIATION

Derive sub-resource authorization from the case that contains them through an access policy, instead of declaring it route by route.

SAMPLE-06

National-identifier directory readable by any authenticated account

HIGH Likelihood High · Impact High · Confidence High

DESCRIPTION

The people-directory read routes were left with no permission check: being authenticated, with zero permissions assigned, is enough to list and search national identifiers and personal data for everyone on record. The pagination parameter has no cap either, so bulk extraction is trivial.

ROOT CAUSE

Routes missing the authorization middleware their sibling routes carry. Since the application has no other authorization layer, a missing middleware means no control at all.

REMEDIATION

Add the permission check to the affected routes, scope the query to the caller's organization, and cap results per page.

SAMPLE-08

Organization scoping is optional rather than enforced on lists and exports

HIGH Likelihood High · Impact High · Confidence High

DESCRIPTION

The organization filter exists as an optional query parameter, not as an enforced restriction. An operational account assigned to a single organization can list and export records belonging to every other one, including the personal data embedded in each case file.

ROOT CAUSE

Isolation between organizations was implemented as a convenience filter in the query layer rather than as a restriction enforced server-side.

REMEDIATION

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.

SAMPLE-09

Permission rename allows colliding with names used in authorization decisions

HIGH Likelihood Medium · Impact Critical · Confidence High

DESCRIPTION

When authorization resolves by permission name, being able to rename a permission is equivalent to being able to grant it. A holder of the permission-editing permission can rename one they already hold so it matches the name guarding a sensitive feature, satisfying that check immediately.

ROOT CAUSE

Same pattern as the role rename: a security decision depends on a string the permission model allows to be edited.

REMEDIATION

Anchor checks to immutable identifiers and treat editing the permission catalog as a highest-privilege operation.

SAMPLE-11

A second reassignment route skips the closed-case lock

MEDIUM Likelihood High · Impact Medium · Confidence High

DESCRIPTION

The primary endpoint refuses to reassign a case that is already resolved or closed. The alternate route producing the same mutation does not apply that lock, allowing cases that should be frozen to be modified.

ROOT CAUSE

Same pattern as the previous finding: the rule lives on the endpoint, not on the operation.

REMEDIATION

Move the check into the shared service so every route that reassigns inherits it by construction.

SAMPLE-10

A second reassignment route skips the organization restriction

MEDIUM Likelihood High · Impact Medium · Confidence High

DESCRIPTION

The primary reassignment endpoint verifies that a coordinating role cannot move cases outside its own organization. A second route produces exactly the same change and carries no such check.

ROOT CAUSE

Two separate endpoints produce the same mutation; the business rule was implemented in only one of them.

REMEDIATION

Centralize reassignment in a single service that holds the checks, and have both endpoints call it.

SAMPLE-15

Closing a case validates neither the prior state nor the assignment

MEDIUM Likelihood High · Impact Medium · Confidence High

DESCRIPTION

The close operation does not check what state the case is in, nor whether the caller is the assigned owner. Any staff account can close any case, repeatedly, producing duplicate entries that corrupt the audit trail.

ROOT CAUSE

The state transition was implemented as a direct write, with no state machine defining which transitions are valid and who may perform them.

REMEDIATION

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.

SAMPLE-01

Data export has neither rate limiting nor a per-user cap

MEDIUM Likelihood Medium · Impact Medium · Confidence High

DESCRIPTION

Any operational account can queue exports with no restriction on frequency or concurrent jobs. Repeating the request saturates the processing queue and consumes server storage.

ROOT CAUSE

The operation is expensive in compute and storage but is treated as an ordinary request, with no consumption control.

REMEDIATION

Add rate limiting to the route and a cap on pending jobs per user, refusing new requests while exports are still in flight.

SAMPLE-05

Internal notes are not filtered out of the staff-facing listing

MEDIUM Likelihood High · Impact Medium · Confidence High

DESCRIPTION

A flag distinguishes internal notes from communication visible to the requester. The public endpoint respects it; the internal one does not filter on it. On top of that, any account can set the flag freely when writing, with no check.

ROOT CAUSE

The visibility rule was applied at a single read site instead of in the query scope shared by both.

REMEDIATION

Apply the filter in the shared query scope, and restrict who may mark a note as internal.

SAMPLE-02

Restoring a deleted account reinstates its previous credentials

MEDIUM Likelihood Medium · Impact Medium · Confidence High

DESCRIPTION

The block operation revokes active access credentials; restoring a soft-deleted account does not. A token issued before deletion silently works again after restoration, within its validity window.

ROOT CAUSE

Two account-lifecycle operations with equivalent security implications were implemented to different standards.

REMEDIATION

Revoke all active credentials on restore, exactly as on block, and require a fresh authentication.

SAMPLE-07

Sign-in reveals account state before verifying the password

MEDIUM Likelihood High · Impact Medium · Confidence High

DESCRIPTION

The response distinguishes between nonexistent account, wrong password, blocked account and lockout, without the caller proving they know the password. The route also has no rate limit, which allows enumerating accounts and additionally forcing a temporary lockout of any known staff account.

ROOT CAUSE

Account-state checks are evaluated before the credential check, and their outcomes are communicated distinguishably.

REMEDIATION

Evaluate account state only after a successful credential check, return a generic response in every failure case, and add rate limiting to the route.

SAMPLE-19

The user directory is exposed to any authenticated account

MEDIUM Likelihood High · Impact Medium · Confidence High

DESCRIPTION

The user-lookup routes are the only ones in their group without a permission check. They expose the email, block state and role and permission assignment of every account, which makes picking a target for the other findings in this report straightforward.

ROOT CAUSE

Routes missing the middleware their sibling routes carry within the same resource.

REMEDIATION

Add the permission check, and limit the returned fields to what the consuming use case strictly needs.

SAMPLE-12

Reassignment does not validate that the recipient is active and eligible

LOW Likelihood Low · Impact Low · Confidence High

DESCRIPTION

Neither reassignment route checks that the destination account is active, unblocked, and holds a role able to handle cases. A case can end up assigned to a blocked or deleted account, where nobody will work it.

ROOT CAUSE

The recipient is validated to exist, not to be in a position to receive the assignment.

REMEDIATION

Validate the recipient's state and role before accepting the reassignment.

SAMPLE-04

Attachments stored in a location the web server may be exposing

NEEDS VALIDATION Likelihood not assigned · Impact not assigned · Confidence —

DESCRIPTION

Files are written to a directory whose configuration is intended for public exposure. The download model uses signed, expiring links, but if the deployment enabled the symbolic link that publishes that directory, the files are reachable at a predictable URL with no authentication or signature, defeating the download model entirely.

ROOT CAUSE

THE FACT THAT IS MISSING

- It is not possible to determine from the repository whether the publishing symlink was enabled in the production environment.

HOW TO RESOLVE IT

- Your operations team can confirm in minutes whether that link exists in production.
- Regardless of the answer, moving attachments to private storage closes the risk permanently.

SAMPLE-17

Request origin may not be trustworthy behind a proxy

NEEDS VALIDATION Likelihood not assigned · Impact not assigned · Confidence —

DESCRIPTION

There is no configuration declaring which proxies are trusted. If the production environment sits behind an undocumented load balancer, CDN or reverse proxy, the source address recorded in the audit log and used by rate limits collapses to a single shared value: the audit stops being attributable and the limits stop isolating anyone.

ROOT CAUSE

THE FACT THAT IS MISSING

- The production network topology is not observable from the code.

HOW TO RESOLVE IT

- Your infrastructure team can confirm whether anything sits in front of the application.
- If something does, declare the trusted proxies; if nothing does, document that explicitly so the assumption is on record.