LAV'S INDUSTRIES

CAUCE · AUDITORÍA DE SEGURIDAD

Hallazgos — detalle técnico

Plataforma de Gestión de Casos

REPORTE DE EJEMPLO · SIN DATOS DE CLIENTE

Cliente	Cliente (sector público)
Alcance	Ejemplo basado en una auditoría real, generalizado
Referencia	«referencia de commit omitida»
Ejecución	run-1 · perfil standard
Fecha	2026-09-23
Documento	AUD-02

Contenido

1. El alta y edición de usuarios acepta un campo de rol sin validar el privilegio resultante — CRÍTICO
2. Endpoint de asignación de permisos sin verificación de techo de privilegio — CRÍTICO
3. Renombrado de roles sin lista de nombres reservados permite suplantar el rol de máximo privilegio — CRÍTICO
4. Archivos adjuntos servidos en línea con tipo de contenido inferido del archivo — ALTO
5. Directorio de identificadores nacionales accesible para cualquier cuenta autenticada — ALTO
6. El alcance por organización es opcional, no obligatorio, en listados y exportaciones — ALTO
7. El renombrado de permisos permite colisionar con nombres usados en decisiones de autorización — ALTO
8. Los sub-recursos de un expediente no heredan el control de acceso del expediente — ALTO
9. El cierre de expedientes no valida el estado previo ni la asignación — MEDIO
10. El directorio de usuarios queda expuesto a cualquier cuenta autenticada — MEDIO
11. El inicio de sesión revela el estado de la cuenta antes de verificar la contraseña — MEDIO
12. La exportación de datos no tiene límite de peticiones ni tope por usuario — MEDIO
13. La restauración de una cuenta eliminada reactiva sus credenciales previas — MEDIO
14. Las notas internas no se filtran del listado destinado al personal — MEDIO
15. Una segunda ruta de reasignación omite el bloqueo de expedientes cerrados — MEDIO
16. Una segunda ruta de reasignación omite la restricción por organización — MEDIO
17. La reasignación no valida que el destinatario esté activo y sea elegible — BAJO
18. El origen de las peticiones puede no ser confiable detrás de un proxy — POR VALIDAR
19. Los adjuntos se almacenan en una ubicación potencialmente expuesta por el servidor web — POR VALIDAR

EJEMPLO-18

El alta y edición de usuarios acepta un campo de rol sin validar el privilegio resultante

CRÍTICO Probabilidad Alto · Impacto Crítico · Confianza Alto

DESCRIPCIÓN

Las operaciones de creación y edición de usuarios aceptan un campo que asigna el rol directamente. Se valida que el rol exista, pero no que quien realiza la operación tenga derecho a otorgarlo. Un portador de los permisos ordinarios de gestión de usuarios puede asignarse el rol de máximo privilegio a sí mismo o a un tercero.

CAUSA RAÍZ

La validación de entrada confirma la existencia del valor, no la autoridad para asignarlo. Existe un endpoint dedicado a la gestión de roles correctamente restringido, pero esta segunda ruta al mismo efecto quedó sin la misma protección.

REMEDIACIÓN

Aplicar la misma verificación de techo de privilegio en ambas rutas, o remover la capacidad de asignar roles desde el endpoint genérico de usuarios y dejarla exclusivamente en el endpoint dedicado que ya está correctamente restringido.

EJEMPLO-14

Endpoint de asignación de permisos sin verificación de techo de privilegio

CRÍTICO Probabilidad Alto · Impacto Crítico · Confianza Alto

DESCRIPCIÓN

El endpoint que sincroniza los permisos de un rol no compara lo que se está otorgando contra lo que ya posee quien realiza la operación. Una cuenta con un único permiso acotado, de los que normalmente se delegan, puede asignarse a sí misma la totalidad de los permisos del sistema en una sola llamada.

CAUSA RAÍZ

La autorización se resuelve verificando la posesión de un permiso puntual, sin ninguna comprobación posterior de que el principal que actúa ya controle al menos tanto como está por conceder.

REMEDIACIÓN

Introducir una verificación de techo de privilegio compartida, invocada desde todos los puntos donde se mutan permisos: la operación se rechaza si el conjunto solicitado no está contenido en el del actor, salvo que éste tenga el rol de máximo privilegio.

EJEMPLO-13

Renombrado de roles sin lista de nombres reservados permite suplantar el rol de máximo privilegio

CRÍTICO Probabilidad Alto · Impacto Crítico · Confianza Alto

DESCRIPCIÓN

La autorización global del sistema reconoce al rol de máximo privilegio por su nombre. Como el endpoint de edición de roles no protege ese nombre, un portador de un permiso de administración intermedio puede renombrar el rol privilegiado —despojando a sus miembros— y luego renombrar el suyo para ocupar su lugar, con efecto inmediato y sin reautenticarse.

CAUSA RAÍZ

Una decisión de autorización se apoya en un atributo mutable (el nombre del rol) que el propio modelo de permisos permite editar a principales de menor privilegio.

REMEDIACIÓN

No autorizar sobre atributos que el usuario puede modificar. Anclar la verificación a un identificador inmutable y, de forma complementaria, mantener una lista de nombres reservados que el endpoint de edición rechace.

EJEMPLO-03

Archivos adjuntos servidos en línea con tipo de contenido inferido del archivo

ALTO Probabilidad Medio · Impacto Alto · Confianza Alto

DESCRIPCIÓN

Los adjuntos se validan por extensión, pero el tipo de contenido con que se sirven proviene de inspeccionar los bytes al momento de la carga, y se entregan para visualizarse dentro del navegador. Un archivo con extensión permitida cuyo contenido real es HTML se ejecuta en el contexto de la aplicación para quien abra el enlace.

CAUSA RAÍZ

La validación de carga y la decisión de cómo servir el archivo usan fuentes distintas: una confía en la extensión, la otra en el contenido. La discrepancia entre ambas es el vector.

REMEDIACIÓN

Forzar la descarga en lugar de la visualización en línea, servir un tipo de contenido genérico y entregar los adjuntos desde un dominio separado sin sesión, de modo que una ejecución no tenga contexto que aprovechar.

EJEMPLO-06

Directorio de identificadores nacionales accesible para cualquier cuenta autenticada

ALTO Probabilidad Alto · Impacto Alto · Confianza Alto

DESCRIPCIÓN

Las rutas de consulta del directorio de personas quedaron sin control de permisos: basta estar autenticado, con cero permisos asignados, para listar y buscar identificadores nacionales y datos personales de todas las personas registradas. El parámetro de paginación tampoco tiene tope, por lo que la extracción masiva es trivial.

CAUSA RAÍZ

Rutas sin el middleware de autorización que sí llevan sus rutas hermanas. Como la aplicación no tiene otra capa de autorización, la ausencia del middleware equivale a ausencia total de control.

REMEDIACIÓN

Agregar el control de permisos a las rutas afectadas, acotar la consulta al ámbito organizacional del solicitante y fijar un máximo de resultados por página.

EJEMPLO-08

El alcance por organización es opcional, no obligatorio, en listados y exportaciones

ALTO Probabilidad Alto · Impacto Alto · Confianza Alto

DESCRIPCIÓN

El filtro de organización existe como parámetro opcional de consulta, no como restricción forzada. Una cuenta operativa asignada a una sola organización puede listar y exportar los registros de todas las demás, incluyendo los datos personales embebidos en cada expediente.

CAUSA RAÍZ

El aislamiento entre organizaciones se implementó como filtro de conveniencia en la capa de consulta, no como restricción aplicada del lado del servidor.

REMEDIACIÓN

Convertir el alcance organizacional en un ámbito obligatorio aplicado en el modelo, de modo que ninguna consulta pueda devolver registros fuera de la organización del solicitante salvo para los roles que explícitamente deban ver-lo todo.

EJEMPLO-09

El renombrado de permisos permite colisionar con nombres usados en decisiones de autorización

ALTO Probabilidad Medio · Impacto Crítico · Confianza Alto

DESCRIPCIÓN

Cuando la autorización se resuelve por el nombre del permiso, poder renombrar un permiso equivale a poder otorgárselo. Un portador del permiso de edición de permisos puede renombrar uno que ya posee para hacerlo coincidir con el nombre que protege una funcionalidad sensible, y satisfacer esa verificación de inmediato.

CAUSA RAÍZ

Mismo patrón que el renombrado de roles: una decisión de seguridad depende de una cadena de texto que el modelo de permisos permite editar.

REMEDIACIÓN

Anclar las verificaciones a identificadores inmutables y tratar la edición del catálogo de permisos como una operación de máximo privilegio.

EJEMPLO-16

Los sub-recursos de un expediente no heredan el control de acceso del expediente

ALTO Probabilidad Alto · Impacto Alto · Confianza Alto

DESCRIPCIÓN

El expediente principal está correctamente protegido, pero sus sub-recursos —comentarios, historial de asignaciones y adjuntos— quedaron sin control de permisos. Una cuenta a la que se le niega ver el expediente puede leer y escribir en todos sus componentes.

CAUSA RAÍZ

La autorización se aplica ruta por ruta en lugar de derivarse del recurso padre, por lo que cada sub-recurso nuevo nace sin protección salvo que alguien recuerde agregarla.

REMEDIACIÓN

Derivar la autorización de los sub-recursos del expediente que los contiene mediante una política de acceso, en vez de declararla ruta por ruta.

EJEMPLO-15

El cierre de expedientes no valida el estado previo ni la asignación

MEDIO Probabilidad Alto · Impacto Medio · Confianza Alto

DESCRIPCIÓN

La operación de cierre no comprueba en qué estado se encuentra el expediente ni si quien la ejecuta es el responsable asignado. Cualquier cuenta del personal puede cerrar cualquier expediente, de forma repetida, generando entradas duplicadas que corrompen la trazabilidad.

CAUSA RAÍZ

La transición de estado se implementó como una escritura directa, sin una máquina de estados que defina qué transiciones son válidas y quién puede ejecutarlas.

REMEDIACIÓN

Definir explícitamente las transiciones permitidas, rechazar las que no correspondan al estado actual y exigir que quien cierre sea el responsable asignado o tenga un rol de supervisión.

EJEMPLO-19

El directorio de usuarios queda expuesto a cualquier cuenta autenticada

MEDIO Probabilidad Alto · Impacto Medio · Confianza Alto

DESCRIPCIÓN

Las rutas de consulta de usuarios son las únicas de su grupo sin control de permisos. Exponen el correo, el estado de bloqueo y la asignación de roles y permisos de todas las cuentas, lo que facilita elegir objetivo para los demás hallazgos de este reporte.

CAUSA RAÍZ

Rutas sin el middleware que sí llevan sus rutas hermanas dentro del mismo recurso.

REMEDIACIÓN

Agregar el control de permisos, y limitar los campos devueltos a los estrictamente necesarios para el caso de uso que consume ese listado.

EJEMPLO-07

El inicio de sesión revela el estado de la cuenta antes de verificar la contraseña

MEDIO Probabilidad Alto · Impacto Medio · Confianza Alto

DESCRIPCIÓN

La respuesta distingue entre cuenta inexistente, contraseña incorrecta, cuenta bloqueada y cuenta con intentos agotados, sin que el solicitante demuestre conocer la contraseña. La ruta tampoco tiene límite de peticiones, lo que permite enumerar cuentas y además forzar el bloqueo temporal de cualquier cuenta conocida del personal.

CAUSA RAÍZ

Las verificaciones de estado de la cuenta se evalúan antes que la de credenciales, y sus resultados se comunican de forma diferenciada.

REMEDIACIÓN

Evaluar el estado de la cuenta solo después de una verificación exitosa de credenciales, devolver una respuesta genérica en todos los casos de fallo y agregar límite de peticiones a la ruta.

EJEMPLO-01

La exportación de datos no tiene límite de peticiones ni tope por usuario

MEDIO Probabilidad Medio · Impacto Medio · Confianza Alto

DESCRIPCIÓN

Cualquier cuenta operativa puede encolar exportaciones sin restricción de frecuencia ni de trabajos simultáneos. Repetir la petición satura la cola de procesamiento y consume el almacenamiento del servidor.

CAUSA RAÍZ

La operación es costosa en cómputo y almacenamiento pero se trata como una petición ordinaria, sin control de consumo.

REMEDIACIÓN

Agregar límite de peticiones a la ruta y un tope de trabajos pendientes por usuario, rechazando nuevas solicitudes mientras existan exportaciones en proceso.

EJEMPLO-02

La restauración de una cuenta eliminada reactiva sus credenciales previas

MEDIO Probabilidad Medio · Impacto Medio · Confianza Alto

DESCRIPCIÓN

La operación de bloqueo revoca las credenciales de acceso activas; la de restauración de una cuenta eliminada no. Un token emitido antes de la eliminación vuelve a funcionar en silencio tras la restauración, dentro de la ventana de vigencia.

CAUSA RAÍZ

Dos operaciones del ciclo de vida de la cuenta con implicaciones de seguridad equivalentes se implementaron con criterios distintos.

REMEDIACIÓN

Revocar todas las credenciales activas en la restauración, igual que en el bloqueo, y obligar a una nueva autenticación.

EJEMPLO-05

Las notas internas no se filtran del listado destinado al personal

MEDIO Probabilidad Alto · Impacto Medio · Confianza Alto

DESCRIPCIÓN

Existe una marca que distingue las notas internas de la comunicación visible para la persona solicitante. El endpoint público la respeta; el interno no la filtra. Además, cualquier cuenta puede establecer esa marca libremente al escribir, sin verificación.

CAUSA RAÍZ

La regla de visibilidad se aplicó en un solo punto de lectura en vez de en la capa de consulta compartida por ambos.

REMEDIACIÓN

Aplicar el filtro en el ámbito de consulta compartido, y restringir quién puede marcar una nota como interna.

EJEMPLO-11

Una segunda ruta de reasignación omite el bloqueo de expedientes cerrados

MEDIO Probabilidad Alto · Impacto Medio · Confianza Alto

DESCRIPCIÓN

El endpoint principal impide reasignar un expediente ya resuelto o cerrado. La ruta alterna que produce la misma mutación no aplica ese bloqueo, permitiendo modificar expedientes que deberían estar congelados.

CAUSA RAÍZ

Mismo patrón que el hallazgo anterior: la regla vive en el endpoint, no en la operación.

REMEDIACIÓN

Mover la verificación al servicio compartido, de modo que toda ruta que reasigne la herede por construcción.

EJEMPLO-10

Una segunda ruta de reasignación omite la restricción por organización

MEDIO Probabilidad Alto · Impacto Medio · Confianza Alto

DESCRIPCIÓN

El endpoint principal de reasignación verifica que un rol de coordinación no pueda mover expedientes fuera de su propia organización. Existe una segunda ruta que produce exactamente el mismo cambio y no incluye esa verificación.

CAUSA RAÍZ

Dos endpoints distintos producen la misma mutación; la regla de negocio se implementó únicamente en uno de ellos.

REMEDIACIÓN

Centralizar la reasignación en un único servicio que concentre las verificaciones, y hacer que ambos endpoints lo invoquen.

EJEMPLO-12

La reasignación no valida que el destinatario esté activo y sea elegible

BAJO Probabilidad Bajo · Impacto Bajo · Confianza Alto

DESCRIPCIÓN

Ninguna de las rutas de reasignación comprueba que la cuenta destino esté activa, sin bloqueo y con un rol habilitado para atender expedientes. Un expediente puede quedar asignado a una cuenta bloqueada o eliminada, donde nadie lo atenderá.

CAUSA RAÍZ

Se valida que el destinatario exista, no que esté en condiciones de recibir la asignación.

REMEDIACIÓN

Validar el estado y el rol del destinatario antes de aceptar la reasignación.

EJEMPLO-17

El origen de las peticiones puede no ser confiable detrás de un proxy

POR VALIDAR Probabilidad sin asignar · Impacto sin asignar · Confianza —

DESCRIPCIÓN

No existe configuración que declare cuáles proxies son de confianza. Si el entorno productivo tiene delante un balanceador, CDN o proxy inverso no documentado, la dirección de origen que registra la bitácora de auditoría y la que usan los límites de peticiones se degradan a un único valor compartido: la auditoría deja de ser atribuible y los límites dejan de aislar.

CAUSA RAÍZ

DATO QUE FALTA PARA CONFIRMARLO

- La topología de red del entorno productivo no es observable desde el código.

CÓMO RESOLVERLO

- El equipo de infraestructura confirma si existe algún intermediario frente a la aplicación.
- Si lo hay, declarar los proxies de confianza; si no, documentar explícitamente que no existen para que el supuesto quede registrado.

EJEMPLO-04

Los adjuntos se almacenan en una ubicación potencialmente expuesta por el servidor web

POR VALIDAR Probabilidad sin asignar · Impacto sin asignar · Confianza —

DESCRIPCIÓN

Los archivos se guardan en un directorio cuya configuración está pensada para exposición pública. El modelo de descarga usa enlaces firmados con vencimiento, pero si en el despliegue se habilitó el enlace simbólico que publica ese directorio, los archivos quedan accesibles por URL predecible sin autenticación ni firma, anulando por completo el modelo de descarga.

CAUSA RAÍZ

DATO QUE FALTA PARA CONFIRMARLO

- No es posible determinar desde el repositorio si el enlace simbólico de publicación fue habilitado en el entorno productivo.

CÓMO RESOLVERLO

- El equipo de operaciones confirma en minutos si ese enlace existe en producción.
- Con independencia del resultado, mover los adjuntos a una ubicación de almacenamiento privada cierra el riesgo de forma definitiva.