Auditoria de seguridad (28-08-2026)

Plataforma Kynda

1. Resumen

Los ocho problemas de la auditoría de Agosto están corregidos.
El equipo sustituyó las 22 policies de acceso a datos una por una, revocó más permisos de los que se habían recomendado y detectó por su cuenta un fallo adicional que la auditoría original no había identificado.

La corrección, sin embargo, introdujo un bug nuevo.
En el estado actual, el administrador de cualquier empresa cliente puede concederse el rol de operaciones de Kynda y acceder con él a los datos del resto de clientes. Se trata de un fallo del mismo tipo que el que acababa de cerrarse: un permiso que no queda limitado a la empresa que lo concede.

Existe además una segunda cuestión, menos visible pero de consecuencias parecidas.
Las pruebas automáticas que se escribieron para impedir que estos fallos reaparezcan no verifican lo que aparentan verificar.

Indicador	Antes	Ahora
Problemas de la auditoría de agosto sin resolver	**8**	**0**
Vulnerabilidades introducidas por la corrección	no aplica	**2 críticas y 3 altas**
Pruebas que verifican realmente las políticas de acceso	no aplica	**3 de 11**

2. Problemas corregidos

Problema de la auditoría de agosto	Solución aplicada
Las funciones de validación no comprobaban el rol de quien las invocaba	Se añadió la comprobación como primera instrucción en las once funciones del panel. De paso se cerró un fallo secundario que permitía averiguar si una evidencia existía
Un participante podía marcar su propia evidencia como aprobada	Las políticas limitan ahora qué estados puede escribir el propietario de un registro. El estado "aprobada" ya no está entre ellos
El alta de usuario permitía asignarse a una empresa ajena	Una función nueva valida el alta contra tres fuentes legítimas, y exige además que la empresa esté activa y sea de tipo cliente
El registro de auditoría admitía entradas falsificadas	Se revocó el permiso de escritura y la política quedó restringida al proceso del servidor
La empresa activa se deducía de datos que el propio usuario controlaba	Ahora se lee únicamente de datos que solo el servidor puede escribir
Los indicadores de impacto se truncaban en silencio	Las consultas filtran por campaña en la base de datos y recorren los resultados por páginas. Se pasó de un uso de paginación a nueve
La subida de evidencias no comprobaba la pertenencia del usuario	Se añadió la comprobación de ámbito
El escaneo de un código QR reactivaba accesos previamente revocados	La operación devuelve ahora un error en lugar de restaurar la membresía

- La revocación de permisos de escritura alcanzó no solo al rol anónimo sino también al autenticado, sobre todas las tablas de la base de datos. La auditoría de Agosto daba ese problema por resuelto parcialmente; con este cambio queda cerrado por completo.

- El equipo identificó por su cuenta una suplantación de identidad de empresa que se producía en cinco rutas concretas de la aplicación, aquellas cuyo nombre contiene un punto y que por ese motivo quedaban fuera del filtro de seguridad general. El fallo está corregido y documentado en el código.

3. Problemas introducidos por la corrección

3.1 Un administrador de empresa puede obtener acceso de operaciones

Severidad: CRITICA

La secuencia se verificó paso a paso y funciona en el código actual.

1. La función que asigna roles a un usuario declara que solo admite dos valores, "usuario" y "administrador de empresa". Esa declaración, existe únicamente en el código fuente y desaparece al compilar. En ejecución no hay ninguna validación. Como la función es accesible por red, cualquiera puede invocarla con un valor distinto.
2. La función que traduce el nombre del rol a su identificador interno acepta cualquier texto y lo busca en la tabla de roles. El rol de operaciones figura en esa tabla, con alcance global.
3. La asignación se aplica sobre la propia empresa del atacante, de modo que la comprobación de pertenencia no la bloquea.
4. Al terminar, el sistema actualiza la credencial del usuario afectado con el rol recién asignado.
5. La comprobación de personal interno consulta esa credencial sin verificar a qué empresa corresponde el rol. Pasa a ser válida en todas, y con ella se abren las políticas de acceso de unas 40 tablas.
6. El control de entrada al panel interno busca una membresía con rol de plataforma, pero tampoco comprueba de qué empresa procede. Concede el acceso.
7. En la base de datos no existe ninguna restricción que impida asociar un rol de alcance global a una empresa cliente.

El sistema incorpora una protección que impide a un usuario modificar su propio rol.Con una segunda cuenta se puede entrar… el código documenta ese fix como conocido en otro apartado.

El cierre requiere tres fixes: validar el rol en ejecución, exigir que la membresía de personal interno pertenezca a la empresa de sistema, y añadir una restricción en la base de datos que rechace roles globales sobre empresas cliente.

3.2 Un operador puede revocar el acceso de un SuperAdmin

Severidad: ALTA. **De las cinco funciones que gestionan empresas en el panel, cuatro restringen su alcance a las de tipo cliente. Una no lo hace.**
El identificador de la empresa interna de Kynda, además, figura como constante visible en el repo.

Con ambos elementos, un OP puede revocar la membresía de cualquier compañero, incluido un Superadmin. La sesión de la persona afectada se invalida de inmediato ya que la propia función se encarga de actualizar su credencial.

3.3 El ataque original permanece activo en parte

Severidad: ALTA. **La función que valida el alta de usuarios admite tres vías: invitación pendiente, lista de correos autorizados y portal de acceso público. Las dos primeras se comprobaron y no son falsificables.**

La tercera sí lo es. La columna que determina el modo de alta tiene valor predeterminado "público", de manera que toda empresa creada antes del panel nuevo lo mantiene salvo modificación manual. Un administrador de empresa puede además restablecerlo cuando lo desee.

Contra esas empresas, el registro utilizando el identificador de otra sigue concediendo membresía activa sin haber accedido nunca a su portal. El rol obtenido es de usuario, no de administrador, pero permite consultar sus campañas y sus acciones.

3.4 Existe una cuenta de operaciones de pruebas en el entorno productivo (Temporal??)

Severidad: ALTA. **La actualización que crea las cuentas de personal interno incluye una dirección destinada a pruebas, acompañada de un comentario que indica que solo la emplean los entornos no productivos. La actualización, no obstante, se ejecuta en todos ellos.**

Quien se registre con esa dirección obtiene el rol de operaciones con alcance global. El dominio pertenece a un espacio de nombres reservado, por lo que la cuenta resulta inalcanzable siempre que la confirmación de correo esté activada. La seguridad de una cuenta con acceso a todos los clientes depende, por tanto, de una opción de panel que el repositorio ni controla ni verifica.

3.5 Una función que no verifica quién la invoca

Severidad: MEDIA. **En el esquema interno de la base de datos existe una función con privilegios elevados que concede membresías de personal a cualquier identificador de usuario que reciba, sin comprobación alguna sobre quien la ejecuta.**

4. Pruebas automáticas no respaldadas

Se añadieron cuatro conjuntos de pruebas de regresión y el total pasó de 57 a 93. El planteamiento es correcto; el resultado, en su mayor parte, no verifica lo que aparenta.

La causa resulta difícil de detectar. Al revocarse los permisos de escritura al rol autenticado, los ataques que las pruebas simulan fallan con un error de permisos antes de que la base de datos llegue a evaluar ninguna política de acceso. Y ninguna prueba comprueba el código de error devuelto: la búsqueda arroja cero coincidencias en todo el conjunto.

La consecuencia práctica es que las 22 policies reescritas, que constituyen la corrección principal del informe, podrían revertirse por completo y solo fallaría una de las once pruebas de escritura.

Solo tres pruebas verifican algo real: la de resolución de dominios, que opera sobre una función sin dependencias externas y está bien construida, una de lectura de membresías y una tercera que declara explícitamente que su objeto es la revocación de permisos, que es en efecto lo que comprueba.

La preocupación no se refiere al estado actual sino al futuro.
Si una actualización posterior volviera a conceder permisos de forma predeterminada, situación que ya se produjo en junio a raíz de un incidente real, las políticas quedarían como única defensa y nadie advertiría que están rotas.

5. Actuaciones recomendadas

1. Validar el rol en ejecución durante su asignación, restringir el control de acceso al panel a la empresa de sistema y añadir la restricción correspondiente en la base de datos.
2. Incorporar el filtro de empresa cliente a la gestión de administradores y protegerla frente a la automodificación.
3. Retirar la cuenta de pruebas del conjunto de datos que se ejecuta en producción, y verificar hoy mismo si la confirmación de correo está activada en el proyecto productivo.
4. Establecer el modo de alta restringido en las empresas existentes y modificar el valor predeterminado de la columna.
5. Comprobar el código de error en cada prueba de ataque, y habilitar un rol de pruebas con permisos de escritura para que las políticas se evalúen realmente.
6. Cubrir los dos vectores que carecen de pruebas.
7. Revocar los permisos de ejecución también en el esquema interno, concediendo únicamente los estrictamente necesarios.
8. Trasladar la comprobación de personal interno a lectura de tabla, tal como ya se hizo con el rol de empresa.