Microservicio Auth

Propietario: Miguel Pilamunga
Revisor: modelado amenasas de auth
Colaboradores:
Generado en fecha: Sun Jan 12 2025

Resumen Ejecutivo

Descripción de alto nivel del sistema (high level system)

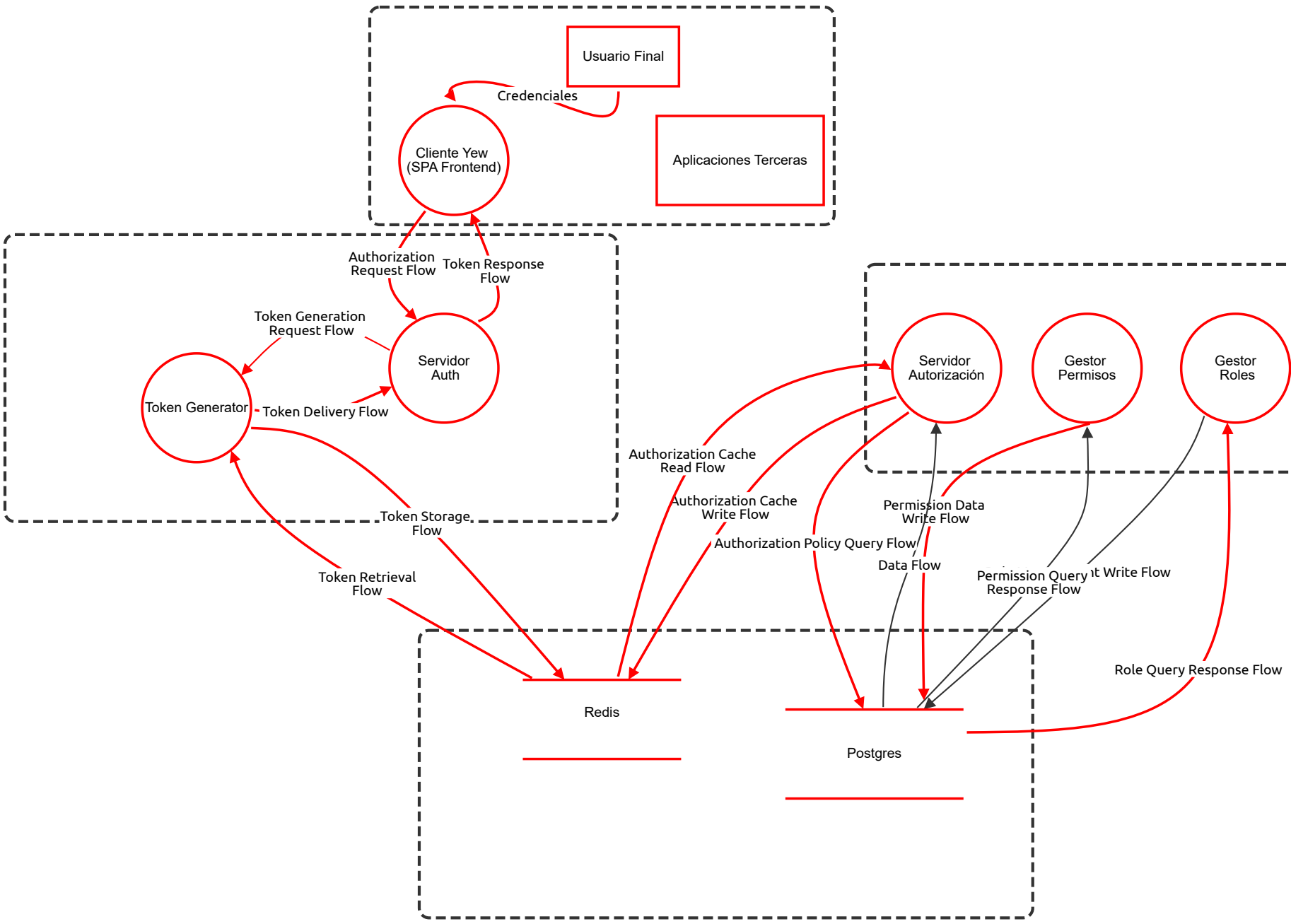
es un sistema de control de roles y permisos

Resumen

Total amenazas	48
Total amenazas mitigadas	14
No Mitigadas	34
Abierto / Alta Prioridad	20
Abierto / Prioridad Media	14
Abierto / Baja Prioridad	0
Abierto / Prioridad Desconocida	0

model

model


Usuario Final
Credenciales
Cliente Yew
(SPA Frontend)
Aplicaciones Terceras
Authorization
Request Flow
Token Response
Flow
Token Generation
Request Flow
Servidor
Auth
Token Generator
Token Delivery Flow
Token Storage
Flow
Token Retrieval
Flow
Servidor
Autorización
Gestor
Permisos
Gestor
Roles
Authorization Cache
Read Flow
Authorization Cache
Write Flow
Authorization Policy Query Flow
Permission Data
Write Flow
Data Flow
Permission Query
Response Flow
Role Query Response Flow
Redis
Postgres

model

Credenciales (Flujo de datos)

Descripción: Nombre del Flujo: "Canal de Transmisión Usuario-Cliente"
Descripción Técnica:
Canal de comunicación HTTPS entre el navegador del usuario y la aplicación Yew para transmisión de credenciales de autenticación y datos de sesión.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
1	Cross-Site Request Forgery (CSRF) [CWE-352]	Linkability / Facilidad de vinculación	High	Open	8.6	Explotación de confianza del navegador para ejecutar acciones no autorizadas en nombre del usuario autenticado.	Implementar tokens CSRF, validar Origin/Referer headers, SameSite cookies
5	Man-in-the-Middle Attack (MITM)" [CWE-300]	Identifiability / Identificabilidad	High	Mitigated	7.4	Intercepción activa de comunicación entre usuario y cliente web.	HSTS, Certificate Pinning, TLS 1.3 obligatorio
6	"SSL/TLS Protocol Downgrade" [CWE-757]	Non-repudiation / No-repudiación	Medium	Open	7.5	Forzar uso de versiones antiguas de SSL/TLS con vulnerabilidades conocidas.	Deshabilitar protocolos antiguos, implementar TLS_FALLBACK_SCSV

Authorization Request Flow (Flujo de datos)

Descripción: Transmisión de solicitudes de autenticación/autorización vía HTTPS/TLS 1.3

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Authorization Code Interception [CWE-598]	Disclosure of information / Brecha de información	High	Open	8.3	Interceptación de código durante redirección OAuth2	PKCE obligatorio, validación state param, timeouts cortos
7	Authorization Code Injection [CWE-384]	Non-repudiation / No-repudiación	High	Mitigated	7.4	Inyección de códigos de autorización maliciosos	Validación de callback URLs, timeouts cortos

Token Response Flow (Flujo de datos)

Descripción: Envío de tokens JWT y datos de sesión post-autenticación

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Token Disclosure [CWE-200]	Disclosure of information / Brecha de información	High	Open	8.7	Exposición de tokens en respuestas HTTP	JWE, secure headers, token binding
19	Token Injection [CWE-290]	Non-repudiation / No-repudiación	Medium	Open	7.8	Inyección de tokens maliciosos en respuesta	Firma verificable, validación de claims

Token Generation Request Flow (Flujo de datos)

Descripción: Solicitudes de generación de tokens con parámetros y claims

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Access Pattern Disclosure	Linkability / Facilidad de vinculación	High	Open	8.5	Vinculación de patrones de generación de tokens	Aleatorización de tiempos, padding de requests

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Token Parameter Exposure	Disclosure of information / Brecha de información	High	Mitigated	7.8	Exposición de datos sensibles en generación	Canal cifrado interno, minimización de datos

Token Storage Flow (Flujo de datos)

Descripción: Persistencia de tokens en cache distribuida

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Token Storage Correlation	Linkability / Facilidad de vinculación	High	Open	7.4	Vinculación de tokens almacenados	Particionamiento, keys aleatorias

Token Delivery Flow (Flujo de datos)

Descripción: Retorno de tokens generados y metadatos asociados

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Token Correlation	Linkability / Facilidad de vinculación	High	Open	7.9	Correlación entre tokens y sesiones	Tokens efímeros, rotación de IDs

Token Retrieval Flow (Flujo de datos)

Descripción: Consulta y recuperación de tokens almacenados

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Token Access Pattern	Detectability / Detectabilidad	Medium	Open	6.8	Detección de patrones de acceso a tokens	Caching multinivel, accesos aleatorios

Authorization Cache Write Flow (Flujo de datos)

Descripción: Persistencia de decisiones de autorización y estado de tokens

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Cache Write Pattern Analysis	Detectability / Detectabilidad	High	Open	8.4	Patrones de escritura revelan información sobre decisiones de autorización	Escrituras diferidas Padding aleatorio Distribución de cache

Authorization Cache Read Flow (Flujo de datos)

Descripción: Recuperación de estado de autorización y validación de tokens

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Cache Policy Information Leakage	Disclosure of information / Brecha de información	High	Open	7.9	Fuga de información de políticas a través de consultas a cache	Encriptación de datos en caché TTL dinámico Segmentación de datos sensibles

Role Management Write Flow (Flujo de datos)

Descripción:

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
48	Role Operation Linkability [MITRE T1069]	Linkability / Facilidad de vinculación	High	Mitigated	7.8	Vinculación de operaciones de roles entre sí	Transaction batching Operation anonymization Random delays

Role Query Response Flow (Flujo de datos)

Descripción:

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
54	Role Hierarchy Exposure [CVE-2023-32004]	Disclosure of information / Brecha de información	Medium	Open	7.8	Exposición de relaciones jerárquicas en consultas	View-based access Hierarchical masking Response sanitization

Permission Query Response Flow (Flujo de datos)

Descripción:

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
48	Query Result Inference [CVE-2023-36891]	Linkability / Facilidad de vinculación	High	Mitigated	8.2	Exposición de metadatos en resultados de consultas	Data masking Result set filtering Column encryption

Permission Data Write Flow (Flujo de datos)

Descripción:

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
47	Permission Write Pattern [MITRE T1213]	Linkability / Facilidad de vinculación	Medium	Open	7.5	Correlación de patrones de escritura de permisos	Batch operations Transaction padding Timing normalization

Data Flow (Flujo de datos)

Descripción:

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones

Authorization Policy Query Flow (Flujo de datos)

Descripción:

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
58	Policy Query Pattern Analysis [CVE-2023-35784]	Linkability / Facilidad de vinculación	High	Open	8.3	Análisis de patrones de consultas revela estructura de políticas	Query normalization Policy caching Request batching
58	Authorization State Disclosure [MITRE T1552]	Disclosure of information / Brecha de información	High	Mitigated	7.8	Exposición de estado de autorización en consultas	Column-level encryption Policy abstraction layers Result set filtering

Usuario Final (Actor)

Descripción: Actor que inicia el flujo de autenticación enviando credenciales al Cliente Yew.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
1	Control de Identidad de Usuario Final	Linkability / Facilidad de vinculación	High	Open	8.2	Actor que inicia el flujo de autenticación enviando credenciales al Cliente Yew. Existe riesgo de vinculación entre diferentes sesiones del mismo usuario.	Implementar rotación de identificadores de sesión y limitar metadatos almacenados por sesión.
2	Exposición de Identidad de Usuario	Identifiability / Identificabilidad	High	Open	7	Riesgo de identificación del usuario a través de patrones de comportamiento y metadatos del navegador.	Implementar técnicas de anonimización de datos y minimizar recolección de información del navegador.
3	Falta de Transparencia en Procesamiento	Unawareness / Falta de Conciencia	Medium	Open	6	Usuario puede no ser consciente del alcance del procesamiento de sus datos personales durante la autenticación.	Implementar avisos claros de privacidad y consentimientos explícitos antes de la autenticación.

Aplicaciones Terceras (Actor)

Descripción:

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Client Application Impersonation [CWE-287]	Identifiability / Identificabilidad	High	Open	8.5	Suplantación de aplicaciones cliente OAuth2 registradas	Client secrets robustos, validación de redirects
7	Unauthorized Application Access [CWE-285]	Linkability / Facilidad de vinculación	High	Mitigated	7.8	Vinculación de múltiples solicitudes a una misma aplicación	Rate limiting por client_id, rotación de secrets

Cliente Yew (SPA Frontend) (Proceso)

Descripción: Aplicación web desarrollada en Yew/WebAssembly que maneja interfaz de autenticación y gestión de tokens.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Cross-Site Scripting (XSS) [CWE-79]	Linkability / Facilidad de vinculación	High	Open	8.2	Ejecución de scripts maliciosos permitiendo vincular sesiones de usuarios	CSP headers, sanitización inputs, escape HTML
8	Nueva amenaza LINDDUN	Identifiability / Identificabilidad	Medium	Open		Introduzca una descripción para esta amenaza	Introduzca la mitigación o prevención para esta amenaza
7	DOM Based XSS [CWE-79]	Linkability / Facilidad de vinculación	High	Open	7.5	Manipulación del DOM exponiendo información sensible del proceso	Validación datos, encapsulación componentes
7	Insufficient Session Management [CWE-613]	Non-repudiation / No-repudiación	Medium	Open	6.8	Gestión inadecuada de sesiones permitiendo repudio de acciones	Logs seguros, rotación tokens, validación timestamps

Servidor Auth (Proceso)

Descripción: Servidor de autenticación OAuth2/OpenID Connect implementado en Rust que gestiona el ciclo de vida de autenticación, emisión y validación de tokens JWT. Maneja múltiples flujos de autenticación incluyendo Authorization Code con PKCE, Client Credentials y Refresh Token.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
7	Broken Authentication [CWE-287]	Disclosure of information / Brecha de información	High	Open	9.1	Fallas en el proceso de autenticación permitiendo acceso no autorizado. Incluye validación incorrecta de credenciales, gestión inadecuada de sesiones y tokens JWT mal configurados	Implementación de rate limiting por IP/usuario Validación rigurosa de JWT claims Rotación automática de claves de firma Monitoreo de intentos fallidos Logs detallados de autenticación
7	Missing Endpoint Authorization [CWE-862]	Non-repudiation / No-repudiación	High	Mitigated	7.8	Endpoints de autenticación expuestos sin la debida autorización permitiendo accesos indebidos a funcionalidades críticas del servidor. Incluye endpoints de revocación de tokens, registro de clientes y gestión de secretos	Middleware de autorización en todos los endpoints Validación de scopes OAuth2 Autenticación mutua TLS Auditoría de accesos administrativos
7	Token Information Disclosure [CWE-200]	Detectability / Detectabilidad	Medium	Open	7.8	Exposición de información sensible en tokens JWT como roles, permisos o datos personales. Incluye tokens sin encriptar, claims innecesarios y metadatos expuestos	Encriptación de tokens sensibles con JWE Minimización de claims en JWT Validación de audiencia Sanitización de datos en tokens

Token Generator (Proceso)

Descripción: Servicio especializado en la generación de JWTs con firma RSA/ECDSA, implementando rotación de claves y gestión de ciclo de vida de tokens. Responsable de firma criptográfica y generación de claims según OpenID Connect.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Token Collection Inference [CVE-2023-35165]	Linkability / Facilidad de vinculación	Medium	Open	8.4	Análisis de patrones en la generación de tokens permite vincular múltiples tokens al mismo usuario	Aleatorización de JTI Rotación de kid Padding aleatorio en tokens Normalización de tiempos de respuesta

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Sensitive Claims Disclosure [CVE-2023-28867]	Disclosure of information / Brecha de información	Medium	Mitigated	7.9	Exposición de información sensible en claims no esenciales del JWT	Encriptación de claims sensibles Minimización de datos expuestos Validación estricta de claims requeridos
26	Non-repudiable Token Generation [MITRE T1552]	Non-repudiation / No-repudiación	Medium	Open	7.6	Falta de trazabilidad en la generación de tokens impide repudiar creaciones no autorizadas	Logging seguro de generación Firmas de auditoría Monitorización de anomalías

Redis (Dispositivo de almacenamiento)

Descripción: Sistema de caché distribuido para almacenamiento de tokens JWT, implementando TTL automático y particionamiento. Utiliza Redis Cluster con TLS para comunicaciones.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Token Correlation Attack [CVE-2023-28424]	Linkability / Facilidad de vinculación	Medium	Open	8.2	Correlación de tokens almacenados permite vincular sesiones de usuario	Particionamiento por tenant Hashing de keys Aislamiento de namespaces
30	Token Correlation Attack [CVE-2023-28424]	Identifiability / Identificabilidad	Medium	Open	8.2	Correlación de tokens almacenados permite vincular sesiones de usuario	Particionamiento por tenant Hashing de keys Aislamiento de namespaces
31	Cache Access Pattern [MITRE T1213]	Non-repudiation / No-repudiación	Medium	Mitigated	8.2	Patrones de acceso a caché revelan información sobre uso de tokens	Accesos aleatorios Padding de datos Cache warming
32	Token Metadata Exposure [CVE-2023-32004]	Disclosure of information / Brecha de información	High	Open	8.2	Metadata de tokens expuesta en caché permite inferir información sensible	Encriptación en reposo Sanitización de metadata Control de acceso granular

Postgres (Dispositivo de almacenamiento)

Descripción: Base de datos relacional que almacena usuarios, roles, permisos y mapeos de relaciones usando estructuras RBAC/ABAC. Implementa encriptación a nivel de columna y row-level security.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Database Schema Inference [CVE-2023-39417]	Linkability / Facilidad de vinculación	High	Open	8.3	Posibilidad de vincular relaciones entre tablas mediante análisis de consultas	Encriptación de foreign keys Views dinámicas Particionamiento por tenant
26	Sensitive Data Exposure [MITRE T1213]	Disclosure of information / Brecha de información	High	Mitigated	8.5	Exposición de datos sensibles en logs y backups	Encriptación transparent data encryption (TDE) Data masking Auditoría de accesos

Servidor Autorización (Proceso)

Descripción:

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Authorization Policy Inference [CVE-2023-22365]	Linkability / Facilidad de vinculación	High	Open	8.7	Vinculación de decisiones de autorización permite inferir políticas de acceso	Aleatorización de respuestas Normalización de tiempos Cacheo de decisiones
26	Role Hierarchy Disclosure [MITRE T1069]	Identifiability / Identificabilidad	High	Mitigated	8.2	Exposición de jerarquía de roles a través de decisiones de autorización	Enmascaramiento de roles Minimización de información en respuestas Aislamiento de contextos
26	Non-repudiable Access Decisions [CVE-2023-28755]	Non-repudiation / No-repudiación	Medium	Open	7.8	Imposibilidad de repudiar decisiones de autorización tomadas	Logging cifrado Firmas de auditoría Versionado de políticas

Gestor Permisos (Proceso)

Descripción: Servicio especializado en la gestión CRUD de permisos, validación de políticas y aplicación de restricciones de acceso.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Permission Relationship Mining [MITRE T1069.001]	Linkability / Facilidad de vinculación	High	Open	7.8	Minería de relaciones entre permisos y recursos	Aislamiento de contextos Permisos dinámicos Rotación de identificadores
26	Permission Assignment Disclosure [CVE-2023-22654]	Disclosure of information / Brecha de información	High	Mitigated	7.6	Exposición de asignaciones de permisos durante operaciones CRUD	Filtrado de respuestas Logs sanitizados Encriptación en tránsito

Gestor Roles (Proceso)

Descripción: Servicio para administración de roles, jerarquías y heredabilidad de permisos según modelo RBAC.

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
26	Role Hierarchy Analysis [MITRE T1069.002]	Linkability / Facilidad de vinculación	High	Open	8.1	Análisis de jerarquía de roles mediante patrones de acceso	Flatten de jerarquías en caché Normalización de consultas Tiempo constante en validaciones
26	Administrative Role Exposure [CVE-2023-35632]	Non-repudiation / No-repudiación	High	Mitigated	8.4	Imposibilidad de repudiar cambios administrativos en roles	Firma digital de cambios Versionado de modificaciones Auditoría detallada