EnerGo

FO-SF-123

Reporte de resultados de análisis de vulnerabilidades

Punto 49 del Anexo 10 RMF 2026 | Monedero electrónico de combustibles

Empresa	SENDERO FUEL S.A. DE C.V.	**Fecha**	29/06/2026
Área responsable	Seguridad de la Información / TI	**Versión**	1.0
Código	FO-SF-123	**Estatus**	Preoperativo / controlado
Elaboró	Seguridad de la Información	**Revisó**	TI / Control Interno
Referencia	PR-SF-014; documentación técnica integral del monedero; reporte SF-P49	**Producto**	Monedero electrónico de combustibles

Resumen ejecutivo

Severidad	Cantidad	Descripción
Crítica	1	Interfaz administrativa de perímetro expuesta a red amplia sin endurecimiento suficiente.
Alta	6	Exposición de servicios sensibles, configuración débil en red/equipos, headers web faltantes, rate limit incompleto y permisos amplios.
Media	4	Banners técnicos, TLS/certificados internos, exposición de interfaces de gestión y secretos sin evidencia de rotación.
Baja / Informativa	1	Mejoras documentales y de hardening continuo.

Resultados por hallazgo

ID	Activo	Sev.	CVSS	Resultado / hallazgo	Riesgo principal	Estatus
SF49-PT-001	FW-FG200F-03 / FW-FTNET-NGX-01	Crítica	9.1	Interfaz administrativa accesible desde segmentos amplios de red interna/VPN, sin restricción granular por IP administrativa y sin evidencia de MFA obligatorio.	Posible toma de control de firewall, modificación de reglas, pérdida de disponibilidad o exposición de tráfico del monedero.	Abierto
SF49-PT-002	SRV-MON-APP-QA	Alta	8.2	Swagger/OpenAPI y paneles de diagnóstico accesibles en QA sin restricción suficiente.	Divulgación de rutas, modelos, parámetros y endpoints útiles para abuso de API.	Abierto
SF49-PT-003	SRV-MON-SER-QA / Portal Clientes	Alta	8.0	Faltan headers de seguridad: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options o Referrer-Policy.	Aumenta riesgo de clickjacking, downgrade, fuga de referencia y ataques de navegador.	Abierto

ID	Activo	Sev.	CVSS	Resultado / hallazgo	Riesgo principal	Estatus
SF49-PT-004	SW-ARUBA-2930 / SW-HP-NGX-01	Alta	7.5	SNMP v2c habilitado o comunidad débil en equipos de red.	Obtención de información de red, interfaces, rutas y configuración; posible abuso por actores internos.	Abierto
SF49-PT-005	SRV-NAS-APP	Alta	8.1	Compartidos SMB con permisos amplios y firma SMB no requerida.	Acceso no autorizado a paquetes, respaldos o archivos de aplicación; riesgo de alteración o ransomware.	Abierto
SF49-PT-006	SRV-MON-DB-DV / SRV-MON-DB-QA	Alta	8.3	Puertos de base de datos accesibles desde segmentos no administrativos y sin lista blanca estricta.	Riesgo de fuerza bruta, enumeración, extracción de datos de prueba y movimiento lateral.	Abierto
SF49-PT-007	Portal Clientes / API OTP	Alta	8.4	Rate limiting no uniforme en endpoints de login, recuperación y reenvío OTP.	Abuso de OTP, enumeración de usuarios o consumo de mensajería.	Abierto
SF49-PT-008	SRV-GLPI	Media	6.8	Versionado visible de plataforma y servicios; banners técnicos expuestos.	Facilita selección de exploits contra GLPI, servidor web o componentes asociados.	Abierto
SF49-PT-009	SRV-MON-APP-DV / SRV-MON-SER-DV	Media	6.5	Certificados autofirmados o TLS débil en servicios internos de desarrollo.	Riesgo de interceptación interna y falta de trazabilidad de certificados.	Abierto
SF49-PT-010	HST-PRLN-01/02/03	Media	6.4	Interfaces de gestión de virtualización visibles desde segmentos operativos.	Aumenta superficie de ataque contra hipervisores y administración de máquinas virtuales.	Abierto
SF49-PT-011	Estaciones afiliadas / equipos de dispensario	Alta	8.6	Equipos de estación con credenciales por defecto o contraseñas compartidas en componentes auxiliares.	Riesgo de manipulación de autorización, tickets o comunicación con el backend del monedero.	Abierto
SF49-PT-012	Repositorios / CI-CD	Media	6.7	Variables, tokens o cadenas de conexión sin rotación documentada; evidencia incompleta de escaneo de secretos.	Riesgo de fuga de credenciales y despliegues no autorizados.	Abierto

Evidencia técnica asociada

Herramienta	Activo / alcance	Resultado representativo	Archivo esperado
Nmap	SRV-MON-DB-QA / SRV-MON-DB-DV	Puerto de base de datos visible desde segmento no administrativo.	SF49_NMAP_DB_QA_20260629.xml
OWASP ZAP	Portal Clientes / API	Ausencia de headers de seguridad y validación de exposición web.	SF49_ZAP_PORTAL_20260629.html
Nuclei	SRV-MON-APP-QA	Swagger/OpenAPI accesible en ambiente QA.	SF49_NUCLEI_QA_20260629.txt
OpenVAS	SW-ARUBA-2930 / SW-HP-NGX-01	SNMP v2c/comunidad débil o exposición de administración.	SF49_OPENVAS_RED_20260629.pdf
Gitleaks	Repositorios / CI-CD	Patrones de secreto o token pendientes de rotación documentada.	SF49_GITLEAKS_CICD_20260629.json