EnerGo

FO-SF-127

Reporte de resultados de pruebas de penetración

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-127	**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 de pruebas ejecutadas

Código prueba	Activo	Vector evaluado	Resultado	Sev. máxima	Evidencia
PT-01	Portal Clientes / API	Descubrimiento web/API, headers y rutas.	Se identificaron headers de seguridad faltantes y exposición de diagnóstico en QA.	Alta	ZAP/Nuclei; SF49-PT-002, SF49-PT-003.
PT-02	Login / OTP	Rate limit, reenvío OTP, recuperación y bloqueo progresivo.	Se observó rate limiting no uniforme entre endpoints.	Alta	Pruebas controladas; SF49-PT-007.
PT-03	FortiGate / VPN	Exposición de administración y restricciones por IP.	Interfaz administrativa accesible desde segmentos amplios.	Crítica	Nmap/revisión configuración; SF49-PT-001.
PT-04	Switches / red	SNMP, banners, puertos y gestión.	SNMP v2c/comunidad débil pendiente de endurecimiento.	Alta	OpenVAS/Nmap; SF49-PT-004.
PT-05	NAS / archivos	Permisos SMB y firma.	Compartidos con permisos amplios y firma SMB no requerida.	Alta	OpenVAS/revisión ACL; SF49-PT-005.
PT-06	Repositorios / CI-CD	Secretos y dependencias.	Evidencia incompleta de rotación y escaneo de secretos.	Media	Gitleaks/Trivy; SF49-PT-012.

Hallazgos de pentest

ID	Activo	Sev.	Hallazgo validado	Impacto	Recomendación	Estatus
SF49-PT-001	FW-FG200F-03 / FW-FTNET-NGX-01	Crítica	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.	Limitar administración a red de gestión, activar MFA, restringir por ACL, deshabilitar administración por WAN/VPN general y registrar accesos.	Abierto

ID	Activo	Sev.	Hallazgo validado	Impacto	Recomendación	Estatus
SF49-PT-002	SRV-MON-APP-QA	Alta	Swagger/OpenAPI y paneles de diagnóstico accesibles en QA sin restricción suficiente.	Divulgación de rutas, modelos, parámetros y endpoints útiles para abuso de API.	Restringir por IP/VPN administrativa, requerir autenticación, desactivar en producción y limitar información de errores.	Abierto
SF49-PT-003	SRV-MON-SER-QA / Portal Clientes	Alta	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.	Configurar headers en IIS/reverse proxy, validar con ZAP/Nuclei y documentar baseline seguro.	Abierto
SF49-PT-004	SW-ARUBA-2930 / SW-HP-NGX-01	Alta	SNMP v2c habilitado o comunidad débil en equipos de red.	Obtención de información de red, interfaces, rutas y configuración; posible abuso por actores internos.	Migrar a SNMPv3, cambiar comunidades, restringir por ACL y registrar consultas.	Abierto
SF49-PT-005	SRV-NAS-APP	Alta	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.	Aplicar mínimo privilegio, grupos nominativos, SMB signing, auditoría de accesos y segregación de red.	Abierto
SF49-PT-006	SRV-MON-DB-DV / SRV-MON-DB-QA	Alta	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.	Aplicar firewall local, ACL por host autorizado, cuentas de servicio con mínimos privilegios y monitoreo de intentos fallidos.	Abierto
SF49-PT-007	Portal Clientes / API OTP	Alta	Rate limiting no uniforme en endpoints de login, recuperación y reenvío OTP.	Abuso de OTP, enumeración de usuarios o consumo de mensajería.	Aplicar límites por IP, usuario, dispositivo y ventana temporal; bloqueo progresivo y alertas.	Abierto
SF49-PT-011	Estaciones afiliadas / equipos de dispensario	Alta	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.	Eliminar usuarios por defecto, credenciales únicas por estación, MFA donde aplique y revisión de configuración por proveedor.	Abierto
SF49-PT-012	Repositorios / CI-CD	Media	Variables, tokens o cadenas de conexión sin rotación documentada; evidencia incompleta de escaneo de secretos.	Riesgo de fuga de credenciales y despliegues no autorizados.	Usar vault/secret manager, rotación programada, Gitleaks en pipeline y revisión trimestral de secretos.	Abierto

Limitaciones y exclusiones operativas

- No se ejecutaron pruebas destructivas, denegación de servicio, persistencia, borrado, modificación de datos productivos ni extracción masiva de información.
- La validación se limita a activos autorizados, ventanas aprobadas y cuentas asignadas.
- Los hallazgos con posible impacto productivo se reportan para remediación controlada antes de iniciar operación regular.