SMART CONSULTING MÉXICO

ACTA DE HECHOS

PRUEBAS DE PENETRACION Y ANALISIS DE VULNERABILIDADES

Participantes principales

- Responsable SMART CONSULTING MEXICO: **Emanuel Andres Parraga (CISSP No. 601993)**
- Responsable SENDERO FUEL: **Axel Martinez Renteria** (Oficial de Seguridad)
- Testigo SMART CONSULTING MEXICO: Gabriel Puga Escamilla
- Testigo SENDERO FUEL: **Romina Monserrat Barbosa Apodaca** (CEO / Gerente ENERGO)

Siendo las 16:00 horas del 29 de junio del 2026, se hace entrega del analisis de vulnerabilidades y pruebas de penetracion realizado por **SMART CONSULTING MEXICO** a la empresa **SENDERO FUEL**, sobre la infraestructura que soporta el monedero electronico de combustibles. Las pruebas se hicieron sobre activos de red, servidores, ambientes de produccion, QA, desarrollo, sitio alterno DRP, oficina corporativa, servicios API, Portal Clientes, componentes de aplicacion movil, repositorios, pipelines y canales conectados. El alcance fue autorizado para todos los dispositivos relacionados con la operacion del monedero de combustibles, incluyendo los siguientes equipos y servicios:

EQUIPO	IP / FQDN / RANGO
FW-FTNET-NGX-01	10.20.1.1
SW-HP-NGX-01	10.20.1.2
HST-PRLN-01/02/03	10.20.1.4 - 10.20.1.6
STR-MSA-01 / VLT-SONCE-01	10.20.1.10 / 10.20.1.30
Produccion monedero APP/SER/DB	172.16.52.10 - 172.16.52.12
QA monedero APP/SER/DB	172.16.51.10 - 172.16.51.12
Desarrollo monedero APP/SER/DB	172.16.50.10 - 172.16.50.12
FW-ASSETEL-NGX-01	10.30.1.1
HST-PRLN-04/05/06	10.30.1.13 - 10.30.1.15
FW-FG200F-03	10.100.0.1
SRV-GLPI / SRV-NAS-APP	10.100.10.10 / 10.100.30.9
Aplicacion movil / Portal Clientes / API	FQDN autorizados
Estaciones afiliadas	Rangos VPN IPSEC autorizados

Las principales herramientas de testing utilizadas fueron:

- Nmap
- Greenbone Community Edition / OpenVAS
- OWASP ZAP
- Nuclei
- Trivy
- OWASP Dependency-Check
- SonarQube Community Build

Los resultados obtenidos respecto a la severidad de las vulnerabilidades encontradas son los siguientes:

SERVIDOR / ACTIVO	CRITICA	ALTA	MEDIA	BAJA
PERIMETRO FORTIGATE / VPN	1	1		
PORTAL CLIENTES / API		3	1	
RED INTERNA / SWITCHES / NAS		2		
BASES DE DATOS QA / DESARROLLO		1	1	
VIRTUALIZACION / GESTION VMWARE			1	
ESTACIONES AFILIADAS		1		
REPOSITORIOS / CI-CD			1	
TOTAL	1	8	4	0

Vulnerabilidades de severidad Critica
Perimetro FortiGate / VPN

SF49-PT-001 - Interfaz administrativa de firewall accesible desde segmentos amplios de red interna/VPN

Se identifico que la administracion de FW-FG200F-03 / FW-FTNET-NGX-01 no se encontraba restringida exclusivamente a una red de gestion granular, con evidencia insuficiente de MFA obligatorio. La condicion incrementa el riesgo de toma de control de reglas de firewall, exposicion de trafico o afectacion a la disponibilidad del monedero electronico de combustibles.

Vulnerabilidades de severidad alta
Portal, API, red interna, bases de datos y estaciones

SF49-PT-002 - Swagger/OpenAPI y paneles de diagnostico accesibles en QA y produccion

La exposicion de rutas, modelos y parametros facilita la enumeracion de funcionalidades internas y el abuso de servicios API.

SF49-PT-003 - Headers de seguridad incompletos en Portal/API

Se observaron controles HTTP faltantes o incompletos, tales como Content-Security-Policy, Strict-Transport-Security, X-Frame-Options o Referrer-Policy.

SF49-PT-004 - SNMP v2c habilitado o comunidad debil en equipos de red

La configuracion permite obtener informacion de interfaces, rutas, nombres y caracteristicas del entorno de red.

SF49-PT-005 - Compartidos SMB con permisos amplios y firma SMB no requerida

La configuracion incrementa el riesgo de acceso no autorizado, alteracion de archivos, movimiento lateral o impacto por ransomware.

SF49-PT-006 - Puertos de base de datos visibles desde segmentos no administrativos

La exposicion de puertos de base de datos en QA/desarrollo amplia la superficie de ataque y facilita fuerza bruta o enumeracion.

SF49-PT-007 - Rate limiting no uniforme en login, recuperacion y reenvio OTP

La ausencia de limites homogeneos por IP, usuario, dispositivo y ventana temporal puede permitir abuso de OTP o enumeracion.

SF49-PT-011 - Credenciales por defecto o compartidas en componentes auxiliares de estacion

La reutilizacion de credenciales o presencia de usuarios por defecto aumenta el riesgo de manipulacion operativa o acceso no autorizado.

Vulnerabilidades de severidad media
Servicios de soporte, desarrollo, virtualizacion y CI/CD

SF49-PT-008 - Versionado visible en GLPI y servicios de soporte

La exposicion de banners y versiones facilita la seleccion de exploits contra componentes publicados o internos.

SF49-PT-009 - Certificados autofirmados o TLS debil en desarrollo

La configuracion de certificados internos sin cadena confiable y protocolos obsoletos reduce la seguridad de las comunicaciones.

SF49-PT-010 - Interfaces de gestion VMware visibles desde segmentos operativos

La visibilidad de consolas de administracion desde redes no dedicadas aumenta la superficie contra hipervisores.

SF49-PT-012 - Evidencia incompleta de rotacion y escaneo de secretos en CI/CD

La falta de evidencia periodica de secret scanning y rotacion documentada puede derivar en fuga de tokens o despliegues no autorizados.

CONCLUSION

Se propone a **SENDERO FUEL**, generar y ejecutar el plan de remediacion correspondiente para ser aplicado cuanto antes, tomando en cuenta los riesgos e impactos de cada uno de los hallazgos identificados y priorizando los riesgos de severidad critica y alta.

Asimismo **SENDERO FUEL** debera conservar la evidencia de autorizacion, ejecucion, bitacoras, reportes tecnicos, plan de remediacion, reescaneo y cierre de hallazgos. Se recomienda programar estas pruebas cuando menos dos veces por anio y despues de cambios mayores en Portal Clientes, API, aplicacion movil, infraestructura de red, VPN, bases de datos, CI/CD o sitio alterno DRP.

FIRMAS

NOMBRE	FIRMA
Axel Martinez Renteria (Oficial de Seguridad SENDERO FUEL)	
Romina Monserrat Barbosa Apodaca (CEO / Gerente ENERGO)	
Ing. Emanuel Andres Parraga (CISSP No. 601993 - SMART CONSULTING MEXICO)	
Gabriel Puga Escamilla (Testigo SMART CONSULTING MEXICO)	