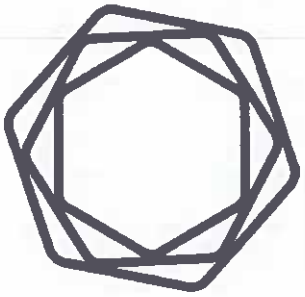
XIGA



ANALISIS DE VULNERABILIDADES

Monedero Xiga

Depto. Infraestrutura.

INTRODUCCIÓN

Con el objetivo de fortalecer la postura de seguridad de la infraestructura, se llevará a cabo un escaneo exhaustivo de vulnerabilidades en los segmentos de Monedero Xiga. Esta iniciativa permitirá identificar de manera precisa las aplicaciones y servicios expuestos a riesgos, facilitando así la implementación de medidas correctivas y preventivas oportunas.

Dichas medidas ayudarán a preservar la continuidad del negocio, por lo cual el realizar de forma periódica dichos análisis es fundamental para conocer el estatus de la infraestructura y en caso de vulnerabilidades emergentes, tener un plan de remediación el cual efectuar y así conservar la confidencialidad, integridad y disponibilidad de nuestros sistemas de información.

ALCANCE

Realizar un análisis exhaustivo de la seguridad de la infraestructura con el fin de identificar de manera precisa las posibles vulnerabilidades, basados en el marco de referencia CVS, que puedan existir en el sistema.

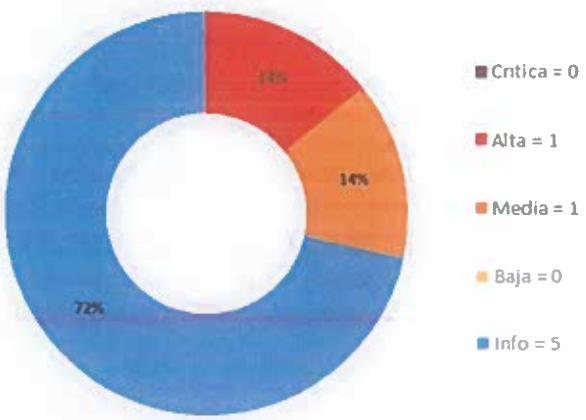
Eventualmente evaluar el nivel de riesgo asociado a dichas vulnerabilidades con la finalidad de mitigar en mayor medida la exposición de datos sensibles y posibles brechas de seguridad.

RESUMEN EJECUTIVO

Nombre de la prueba:	Análisis de Vulnerabilidades
Descripción	Evaluación de Monedero Xiga.
Tipo:	Evaluación
Tiempo y Duración:	Abril 22 de 2025 7:11 pm - Abril 22 de 2025 7:20 pm

Top Service/App/Software	Resumen Porcentual de
Se representa el top 5 herramientas, servicios o software vulnerable.	**Resumen Gráfico de vulnerabilidades.**

1. Microsoft Windows SMB Shares Unprivileged Access
2. SMB Signing not required
3. Common Platform Enumeration (CPE)
4. DCE Services Enumeration
5. HyperText Transfer Protocol (HTTP) Info.



JGAVILA-LP

Dirección	Misión de San Javier 10634-210, Zona Urbana Rio Tijuana, 22010 Tijuana, B.C.
Sistema Operativo	Windows 11
Tipo de dispositivo	Laptop
Nombre del equipo	JGAVILA-LP
Dirección IP	10.255.237.35

Vulnerabilidad y sus niveles de riesgo

0	1	1	0	5
Critica	Alta	Media	Baja	Info

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.6	0.0866	42411	Microsoft Windows SMB Shares Unprivileged Access
Media	5.3	-	-	57608	SMB Signing not required
Info	N/A	-	-	-	Common Platform Enumeration (CPE)
Info	N/A	-	-	-	DCE Services Enumeration
Info	N/A	-	-	-	HyperText Transfer Protocol (HTTP) Info.
Info	N/A	-	-	-	SSL / TLS Versiones Supported
Info	N/A	-	-	-	TightVNC Java Viewer Detection

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus.
Software dedicado al escaneo de vulnerabilidad en sistemas informaticos mediante el standar CVE (Common Vulnerabilities Exposures)

CONCLUSIÓN

En conclusión, los resultados del escaneo de vulnerabilidades en los segmentos del Monedero Xiga han revelado un panorama detallado de las posibles amenazas a las que se encuentra expuesta la infraestructura. Las tablas presentadas a lo largo de este documento evidencian la necesidad de implementar un plan de remediación urgente y eficaz. Es fundamental abordar las vulnerabilidades identificadas para garantizar la integridad y confidencialidad de los datos, así como para prevenir incidentes de seguridad que puedan comprometer la continuidad del negocio.