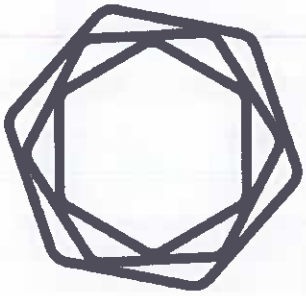
XIGA



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 3:57 pm - Abril 22 de 2025 4:04 pm

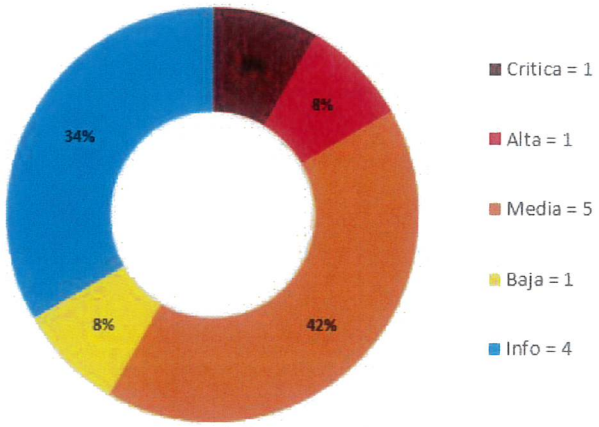
Top Service/App/Software

Se representa el top 5 herramientas, servicios o software vulnerable.

1. Firebird DataBase Server fbserver.exe p_cnct_count Value Remote Overflow
2. SSL Medium Strenght Cipher Suites Supported (SWEET32)
3. SSL Certificate Cannot Be Trusted
4. SSL Self-Signed Certificate
5. TLS Version 1.0 Protocol Detection

Resumen Porcentual de Vulnerabilidades

Resumen Gráfico de vulnerabilidades.



SRV-XIGA-APP-DEV

Dirección	Ave. Circunvalación San Francisco #31, San Carlos Primera Etapa. 84090 Heroica Nogales. Son.
Sistema Operativo	Windows Server
Tipo de dispositivo	Servidor
Nombre del equipo	SRV-XIGA-APP-DEV
Dirección IP	10.255.243.19

Vulnerabilidad y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
1	1	5	1	4

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Critica	10.0	6.7	0.2819	25492	Firebird DataBase Server fbserver.exe p_cnct_count Value Remote Overflow
Alta	7.5	5.1	0.406	42873	SSL Medium Strenght Cipher Suites Supported (SWEET32)
Media	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
Media	6.5	-	-	57582	SSL Self-Signed Certificate
Media	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
Media	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
Media	5.3	-	-	57508	SMB Signing not required
Baja	2.1	2.2	0.0037	10114	ICMP Timestamp Reques Remote Data Disclosure
Info	N/A	-	-	-	Remote Desktop Protocol Service Detection
Info	N/A	-	-	-	Common Plataform Enumeration (CPE)
Info	N/A	-	-	-	MSSQL Host Information in NTLM SSP
Info	N/A	-	-	-	Microsoft Windows SMB Service Detection

Herramientas utilizadas en la prueba de auditoría

Tenable Nessus.

Software dedicado al escaneo de vulnerabilidades 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.