ISO 27001 – Reporte de Gestión de Vulnerabilidades

Introducción

Este reporte documenta el análisis de servicios y la búsqueda de vulnerabilidades asociadas, a partir de un escaneo realizado con Nmap en un entorno controlado. El objetivo es identificar posibles riesgos en los servicios expuestos y recomendar acciones de mitigación para garantizar la confidencialidad, integridad y disponibilidad de la información.

Descripción del escaneo

- **Herramienta:** Nmap 7.95
- **Comando ejecutado:** nmap -sV 192.168.1.10
- **Resultado principal:**
    - 1 puerto TCP abierto (80/tcp)
    - Servicio HTTP (Apache httpd 2.4.62 sobre Debian)
    - Se detectó un blog WordPress en /wordpress/ y la página de login en /wordpress/wp-login.php

Servicios y versiones detectados

- **Apache HTTP Server** 2.4.62 (Debian)

Tabla de vulnerabilidades identificadas

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Enlace
80/tcp	http (Apache HTTP Server)	2.4.62	CVE-2024-39884	Una regresión en Apache HTTP Server 2.4.60 ignoraba parte de la configuración basada en AddType, lo que podía exponer código fuente local (por ejemplo, scripts PHP) en lugar de interpretarlo.	NVD CVE-2024-39884
80/tcp	http (Apache HTTP Server)	2.4.62	CVE-2024-40725	Arreglo incompleto para CVE-2024-39884 en Apache HTTP Server 2.4.61: bajo ciertas configuraciones de AddType seguía permitiendo la divulgación de contenido local.	SUSE CVE-2024-40725

Nota: Aunque la versión 2.4.62 corrige estas vulnerabilidades, es fundamental verificar la correcta aplicación de los parches y la ausencia de configuraciones heredadas que puedan reintroducir riesgos.

Recomendaciones

1. **Actualización y parches:**
    - Verificar que Apache HTTP Server esté efectivamente en versión 2.4.62 o superior y que no existan módulos o configuraciones antiguas cargadas desde rutas diferentes.
2. **Pruebas continuas de seguridad:**
    - Implementar un ciclo periódico de escaneos de vulnerabilidades (mensual) usando Nmap, OpenVAS u otras herramientas, y complementar con pruebas de penetración enfocadas en HTTP/2, proxy y módulos de terceros (WordPress).
3. **Monitoreo y alertas:**
    - Configurar un sistema de detección de intrusiones (IDS/IPS) para tráfico HTTP inusual, especialmente peticiones con múltiples cabeceras Content-Length o combinaciones Transfer-Encoding, que puedan indicar intentos de smuggling o explotación de regresiones.

Conclusiones

La identificación temprana de vulnerabilidades—incluso aquellas ya corregidas en la versión instalada— resalta la importancia de mantener un proceso riguroso de gestión de parches y de auditoría de configuraciones. La aplicación de las recomendaciones propuestas mitigará riesgos de divulgación de código y ataques de Request Smuggling, fortaleciendo la postura de seguridad del servicio web.