INFORME DE VULNERABILIDADES
ISO 27001

Fecha del informe: 13/02/2025
Autor: Javier Pérez Gómez

---

1. Introducción

Este informe documenta la evaluación de seguridad realizada sobre el servicio web Apache HTTP Server en su versión 2.4.62, identificando vulnerabilidades potenciales y proporcionando recomendaciones de mitigación, en cumplimiento con la norma ISO 27001.

2. Identificación del Activo

- **Nombre del Activo:** Servidor Web Apache HTTP
- **Versión:** 2.4.62
- **Ubicación:** 192.168.0.53
- **Administrador Responsable:** Javier Pérez Gómez
- **Fecha de Evaluación:** 13/02/2025
- **Herramienta Utilizada:** Nmap v7.95

3. Vulnerabilidades Detectadas

CVE-2024-40725

- **Descripción:** Configuraciones heredadas basadas en el tipo de contenido pueden permitir la divulgación del código fuente de scripts PHP u otros archivos interpretables.
- **Impacto:** Un atacante podría obtener acceso al código fuente de aplicaciones web.
- **Recomendación:** Verificar la configuración del servidor y aplicar las actualizaciones más recientes de Apache HTTP Server.

CVE-2024-40898

- **Descripción:** En sistemas Windows, mod_rewrite en el contexto del servidor o host virtual puede ser vulnerable a un ataque de Server-Side Request Forgery (SSRF), lo que permite la filtración de hashes NTLM.
- **Impacto:** Un atacante podría aprovechar esta vulnerabilidad para capturar credenciales NTLM y utilizarlas en ataques de autenticación.
- **Recomendación:** Deshabilitar el uso de mod_rewrite si no es necesario y restringir el acceso a recursos internos mediante listas de control de acceso.

4. Evaluación de Riesgo

- **Nivel de Riesgo para CVE-2024-40725:** Medio
- **Nivel de Riesgo para CVE-2024-40898:** Alto
- **Probabilidad de Explotación:** Alta

5. Recomendaciones Generales

- **Actualizar a la última versión de Apache HTTP Server**, verificando los parches de seguridad disponibles.
- **Revisar configuraciones del servidor**, especialmente las relacionadas con el módulo mod_rewrite y la interpretación de archivos.
- **Monitorear fuentes oficiales**, como la NVD (National Vulnerability Database)
- **Implementar medidas de seguridad adicionales**, como restricciones en la configuración de módulos y reforzamiento de controles de acceso.

6. Conclusión

Se recomienda aplicar las mitigaciones mencionadas para reducir el riesgo de explotación de las vulnerabilidades detectadas. Además, se sugiere realizar pruebas de penetración periódicas para identificar y corregir nuevas amenazas.
