

Reporte de Vulnerabilidades - Apache HTTP Server 2.4.62

1. Introducción

Este informe presenta los resultados de la búsqueda de vulnerabilidades para Apache HTTP Server versión 2.4.62, consultados en la base de datos NVD del NIST.

2. Resumen de resultados

No se han identificado vulnerabilidades registradas en la NVD para Apache HTTP Server v2.4.62 hasta la fecha de emisión de este informe. La búsqueda se realizó el 9 de mayo de 2025 y los resultados muestran cero entradas.

3. Conclusiones

La versión 2.4.62 de Apache HTTP Server no presenta vulnerabilidades conocidas en la NVD. Se confirma que el software se encuentra en un estado seguro según la base de datos consultada.

4. Recomendaciones

- – Mantener el software actualizado: aplicar parches y nuevas versiones cuando estén disponibles.
- – Implementar un proceso de monitoreo periódico de la NVD u otras fuentes de vulnerabilidad.
- – Configurar alertas automáticas para nuevas vulnerabilidades que afecten a Apache HTTP Server.
- – Realizar pruebas de seguridad internas (escaneo SAST/DAST) de forma regular.
- – Seguir buenas prácticas de configuración segura según la documentación oficial de Apache.

Fecha de emisión: 9 de mayo de 2025

Elaborado por: Cristian Hugo González Pedreira

Informe N°: 001