

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80	HTTP	Apache 2.4.65	CNVD-2024-36391	Existe una vulnerabilidad de divulgación de información en el Servidor HTTP Apache, que un atacante puede explotar para obtener información confidencial, realizar ataques de falsificación de solicitudes del lado del servidor o ejecutar scripts locales.	https://vulners.com/search?query=CNVD-2024-36391
80	HTTP	Apache 2.4.65	CNVD-2022-41640	Existe una vulnerabilidad de desbordamiento de búfer en Apache HTTP Server, derivada de un sistema o producto en red que no valida correctamente los límites de datos al realizar operaciones en memoria. Un atacante podría explotar esta vulnerabilidad para sobrescribir la memoria del montón.	https://vulners.com/cnvd/CNVD-2022-41640
80	HTTP	Apache 2.4.65	CNVD-2020-46280	Existe una vulnerabilidad de desbordamiento de búfer en mod_wsgi en las versiones 2.4.32 a 2.4.44 del Servidor HTTP Apache. Un atacante podría explotar esta vulnerabilidad para obtener información y posiblemente ejecutar código.	https://vulners.com/cnvd/CNVD-2020-46280
80	HTTP	Apache 2.4.65	CNVD-2024-36388	Existe una vulnerabilidad de ejecución de código en Apache HTTP Server, que un atacante puede explotar para ejecutar scripts en directorios donde la configuración lo permita.	https://vulners.com/cnvd/CNVD-2024-36388