

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencias
80	HTTP	Apache 2.4.65	CVE-2025-58098	Vulnerabilidad de apache afecta a versiones anteriores	https://vulners.com/cve/CVE-2025-58098
80	HTTP	Apache 2.4.65	CVE-2025-59775	Vulnerabilidad SSRF filtra hashes en ciertas configuraciones	https://vulners.com/cve/CVE-2025-59775
80	HTTP	Apache 2.4.65	CVE-2025-55753	Vulnerabilidad que elimina el backoff, que causa reintentos rápidos y repetidos.	https://vulners.com/cve/CVE-2025-55753
80	HTTP	Apache 2.4.65	CNVD-2025-30837	Vulnerabilidad en apache que permite forzar, intentos repetidos de renovación entre la versión 2.4.30 y 2.4.66	https://vulners.com/cnvd/CNVD-2025-30837
80	HTTP	Apache 2.4.65	CNVD-2025-30836	Vulnerabilidad en apache CSRF capaz de filtrar hashes NTLM	https://vulners.com/cnvd/CNVD-2025-30836
80	HTTP	Apache 2.4.65	CVE-2025-65082	Error en manejo de variables CGI que otorga la capacidad de sobrescribir variables de el entorno en versiones 2.4.0	https://vulners.com/cve/CVE-2025-65082
80	HTTP	Apache 2.4.65	CNVD-2025-30833	Vulnerabilidad bypass de seguridad	https://vulners.com/cnvd/CNVD-2025-30833
80	HTTP	Apache 2.4.65	CVE-2025-66200	Vulnerabilidad alta con capacidad de otorgar permisos para ejecutar CGi con usuario remoto.	https://vulners.com/cve/CVE-2025-66200
80	HTTP	Apache 2.4.65	CNVD-2025-30835	Vulnerabilidad de apache que otorga permisos para ejecutar código en CGI en múltiples versiones.	https://vulners.com/cnvd/CNVD-2025-30835