Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80	HTTP	Apache 2.4.65	CVE-2025-58098	Este problema afecta al servidor HTTP Apache anterior a la versión 2.4.66. Se recomienda a los usuarios actualizar a la versión 2.4.66, que soluciona el problema.	https://vulners.com/cve/CVE-2025-58098
			CVE-2025-59775	En el servidor HTTP Apache en Windows, con AllowEncodedSlashes activado y MergeSlashes desactivado, se pueden filtrar hashes NTLM a un servidor malicioso mediante SSRF y solicitudes o contenido maliciosos. Se recomienda a los usuarios actualizar a la versión 2.4.66, que soluciona el problema.	https://vulners.com/cve/CVE-2025-59775
			CVE-2025-55753	Un desbordamiento de enteros en caso de una renovación fallida del certificado ACME provoca, tras varios fallos (unos 30 días en la configuración predeterminada), que el temporizador de retardo se ponga a 0. Los intentos de renovación del certificado se repiten sin demora hasta que se realiza correctamente. Este problema afecta al servidor HTTP Apache desde la versión 2.4.30 hasta la 2.4.66. Se recomienda a los usuarios actualizar a la versión 2.4.66, que soluciona el problema.	https://vulners.com/cve/CVE-2025-55753
			CVE-2025-30837	Existe una vulnerabilidad de seguridad en las versiones 2.4.30 a 2.4.66 y anteriores del servidor HTTP Apache, que un atacante puede aprovechar para provocar intentos de renovación repetidos sin demora.	https://vulners.com/cnvd/CNVD-2025-30837
			CVE-2025-30836	El servidor HTTP Apache sufre una vulnerabilidad de falsificación de solicitud entre sitios que puede revelar hashes NTLM.	https://vulners.com/cnvd/CNVD-2025-30836
			CVE-2025-65082	Vulnerabilidad de neutralización incorrecta de secuencias de escape, metadatos o de control en Apache HTTP Server, debido a que las variables de entorno configuradas mediante Apache reemplazan inesperadamente las variables calculadas por el servidor para programas CGI. Este problema afecta a Apache HTTP Server desde la versión 2.4.0 hasta la 2.4.65. Se recomienda a los usuarios actualizar a la versión 2.4.66, que soluciona el problema.	https://vulners.com/cve/CVE-2025-65082
			CVE-2025-30833	Existe una vulnerabilidad de omisión de seguridad en las versiones 2.4.0 a 2.4.65 del servidor HTTP Apache debido a la neutralización incorrecta de secuencias de escape, metadatos o de control. Un atacante podría explotar esta vulnerabilidad para provocar una sobreescritura inesperada de una variable de programa CGI.	https://vulners.com/cnvd/CNVD-2025-30833
			CVE-2025-66200	Vulnerabilidad de omisión de mod_userdir+suexec mediante AllowOverride FileInfo en el servidor HTTP Apache. Los usuarios con acceso a la directiva RequestHeader en htaccess pueden provocar que algunos scripts CGI se ejecuten con un ID de usuario inesperado. Este problema afecta al servidor HTTP Apache desde la versión 2.4.7 hasta la 2.4.65. Se recomienda actualizar a la versión 2.4.66, que soluciona el problema.	https://vulners.com/cve/CVE-2025-66200
			CVE-2025-30835	Existe una vulnerabilidad de ejecución de código en las versiones 2.4.7 a 2.4.65 de Apache HTTP Server, que un atacante puede aprovechar para hacer que un script CGI se ejecute como un usuario inesperado.	https://vulners.com/cnvd/CNVD-2025-30835