puerto	servicio	versión	vulnerabilidad	descripción	referencia
80	:apache:http	:2.4.62:	CVE-2014-4210	Una vulnerabilidad no especificada en el componente Oracle WebLogic Server en Oracle Fusion Middleware 10.0.2.0 y 10.3.6.0 permite a los atacantes remotos afectar a la confidencialidad a través de vectores relacionados con WLS - Web Services.	
80	:apache:http	:2.4.62:	CVE-2023-38709	La validación de entrada defectuosa en el núcleo de Apache permite que los generadores de contenido / backend maliciosos o explotables dividan las respuestas HTTP.	
80	:apache:http	:2.4.62:	CVE-2025-53020	Vulnerabilidad de liberación tardía de memoria después de una vida útil efectiva en el servidor HTTP Apache.	
80	:apache:http	:2.4.62:	CVE-2025-49812	algunas configuraciones mod_ssl en las versiones del servidor HTTP Apache hasta la 2.4.63, un ataque de desincronización HTTP permite a un atacante de intermediario secuestrar una sesión HTTP a través de una actualización TLS.	
80	:apache:http	:2.4.62:	CVE-2025-49630	as configuraciones de proxy, un ataque de denegación de servicio contra las versiones 2.4.26 a 2.4.63 del servidor HTTP Apache puede ser desencadenado por clientes que no son de confianza y provocar una aserción en mod_proxy_http2.	
80	:apache:http	:2.4.62:	CVE-2025-23048	En algunas configuraciones de mod_ssl en Apache HTTP Server 2.4.35 a 2.4.63, es posible omitir el control de acceso por parte de clientes de confianza mediante la reanudación de la sesión TLS 1.3.	
80	:apache:http	:2.4.62:	CVE-2024-47252	te de los datos proporcionados por el usuario en mod_ssl en Apache HTTP Server 2.4.63 y versiones anteriores permite que un cliente SSL/TLS que no es de confianza inserte caracteres de escape en los archivos de registro en algunas configuraciones	
80	:apache:http	:2.4.62:	CVE-2024-43394	de solicitudes del lado del servidor (SSRF) en el servidor HTTP Apache en Windows permite potencialmente filtrar hashes NTLM a un servidor malicioso a través de mod_rewrite o expresiones Apache que pasan entradas de solicitud no validadas	
80	:apache:http	:2.4.62:	CVE-2024-43204	a un atacante enviar solicitudes de proxy salientes a una URL controlada por el atacante. Requiere una configuración poco probable en la que mod_headers esté configurado para modificar la solicitud de tipo de contenido o el encabezado de respuesta con un valor proporcionado en la solicitud HTTP.	
80	:apache:http	:2.4.62:	CVE-2024-42516	ón de respuestas HTTP en el núcleo del servidor HTTP Apache permite a un atacante que puede manipular los encabezados de respuesta de tipo de contenido de las aplicaciones alojadas o reunidas por el servidor dividir la respuesta HTTP.	