Vulnerabilidades IP 192.168.0.25 Debian

Puerto	Servicio	Versión	Vulnerabilidad	Descripción
21	FTP	vsftpd 3.0.3	CVE-2021-30047	Denegación de servicio (DoS) por mala gestión de memoria.
21	FTP	vsftpd 3.0.3	CVE-2021-3618	Ejecución de comandos arbitrarios mediante entrada maliciosa.
80	HTTP	Apache 2.4.62 (Debian)	CVE-2025-53020	CVE reciente, aún sin análisis de impacto.
80	HTTP	Apache 2.4.62 (Debian)	CVE-2024-47252	Posible vulnerabilidad detectada en Apache (en evaluación).
80	HTTP	Apache 2.4.62 (Debian)	CVE-2025-49812	Versiones de HTTP server hasta la 2,4,63 vulnerables a desincronización HTTP para actualizaciones de TLS.
80	HTTP	Apache 2.4.62 (Debian)	CVE-2025-49630	Denegación de servicio (DoS) debido a clients no fiables.
80	HTTP	Apache 2.4.62 (Debian)	CVE-2025-23045	Omisión de control de acceso afectando mod_ssl con reanudación de sesión TLS 1.3
80	HTTP	Apache 2.4.62 (Debian)	CVE-2024-43394	La falsificación de solicitud del lado del servidor en el servidor HTTP Apache en Windows puede filtrar hashes NTLM a través de entradas no validadas.
80	HTTP	Apache 2.4.62 (Debian)	CVE-2024-43204	La vulnerabilidad SSRF en mod_headers del servidor HTTP Apache requiere una actualización a la versión 2.4.64.
80	HTTP	Apache 2.4.62 (Debian)	CVE-2024-42516	El servidor HTTP Apache permite la división de respuestas HTTP debido a la manipulación del encabezado Content-Type. Actualice a la versión 2.4.64.

Referencia
https://vulners.com/cve/CVE-2021-30047
https://vulners.com/cve/CVE-2021-3618
https://vulners.com/cve/CVE-2025-53020
https://vulners.com/cve/CVE-2024-47252
https://vulners.com/cve/CVE-2025-49812
https://vulners.com/cve/CVE-2025-49630
https://vulners.com/cve/CVE-2025-23048
https://vulners.com/cve/CVE-2024-43394
https://vulners.com/cve/CVE-2024-43204
https://vulners.com/cve/CVE-2024-42516