

| Puerto | Servicio | Versión detectada | Vulnerabilidad / ID (según vulners) | Descripción breve | Referencia |
|--------|---------------|-------------------------------------|---------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| 80 | HTTP (Apache) | Apache httpd 2.4.65 (Debian) | CNVD-2024-36391 (critic) | Vulnerabilidad crítica detectada en Apache; posible escale de privilegion | https://vulners.com/cnvd/CNVD-2024-36391 |
| 80 | HTTP (Apache) | Apache httpd 2.4.65 (Debian) | CNVD-2024-36388 (critic) | Otra entrada crítica relacionada con la misma versión; revisar parches y mitigaciones. | https://vulners.com/cnvd/CNVD-2024-36388 |
| 80 | HTTP (Apache) | Apache httpd 2.4.65 (Debian) | CNVD-2022-41640 (high) | Vulnerabilidad alta listada puede permitir escalado o ejecución dependiendo del módulo. | https://vulners.com/cnvd/CNVD-2022-41640 |
| 80 | HTTP (Apache) | Apache httpd 2.4.65 (Debian) | EDB-ID:46676 (exploit) | Exploit público reportado contra una vulnerabilidad en Apache | https://vulners.com/exploitdb/EDB-ID:46676 |

| | | | | | |
|----|------------------|-----------------------------------------------------|---------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 80 | HTTP (Apache) | Apache httpd 2.4.65 (Debian) | EDB-ID:4 0909 (exploit) | Exploit histórico disponible; verificar si aplica a la build Debian actual. | https://vulnerables.com/exploits/db/EDB-ID:40909 |
|----|------------------|-----------------------------------------------------|---------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|