

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
● 22	SSH	OpenSSH 9.2p1	CVE-2023-38408	Ejecución remota de comandos debido a uso inseguro de bibliotecas.	Link a CVE
● 22	SSH	OpenSSH 9.2p1	CVE-2023-28531	Salto de autenticación bajo condiciones específicas.	Link a CVE
● 22	SSH	OpenSSH 9.2p1	CVE-2024-6387	Condición de carrera explotable en sshd (Signal handler race).	Link a CVE
● 80	HTTP	Apache httpd 2.4.62	No detectada	No se identificaron vulnerabilidades críticas con el escaneo actual.	—
○ 443	HTTPS	— (Puerto cerrado)	—	Puerto cerrado, no se evaluó vulnerabilidad.	—

- **Rojo:** Riesgo alto (ej. ejecución remota, salto de autenticación).
- **Naranja:** Riesgo medio (condiciones específicas, vectores limitados).
- **Verde:** Sin vulnerabilidades detectadas.
- **Gris:** No evaluado / puerto cerrado.