

| Puerto | Servicio | Versión | Vulnerabilidad | Descripción | Referencia |
|---------------|-----------------|----------------|--------------------------------|--|---|
| 22 | SSH | Open SSH 9.2p1 | CVE-2023-38408 | búsqueda poco fiable, lo que provoca la ejecución remota de código si un agente se reenvía a un sistema controlado por un atacante. | https://vulners.com/cve/CVE-2023--38408 |
| 22 | SSH | Open SSH 9.2p1 | CVE-2023-28531 | ssh-add en OpenSSH anterior a la versión 9.3 añade claves de tarjeta inteligente a ssh-agent sin las restricciones de destino por salto previstas. | https://vulners.com/cve/CVE-2023--28531 |
| 22 | SSH | Open SSH 9.2p1 | CVE-2023-6387 | Existe un posible desbordamiento de búfer en la aplicación de muestra Bluetooth LE HCI CPC en el SDK de Gecko que puede provocar una denegación de servicio o ejecución remota de código. | https://vulners.com/cve/CVE-2023--6387 |
| 80 | HTTP | Apache 2.4.62 | CVE-2021-44224 | Una URI manipulada enviada a httpd, configurada como proxy directo (ProxyRequests activado), puede provocar un fallo, en configuraciones que combinan declaraciones de proxy directo e inverso, puede permitir que las solicitudes se dirijan a un punto final de socket de dominio Unix declarado | https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Apache+2.4.7&search_type=all&isCpeNameSearch=false |
| | | | | | |
| | | | | | |
| | | | | | |