Devian server, reporte de vulnerabilidad

Weiyu

July 2025

1. Introduction

Documentación sobre las vulnerabilidades del servidor debian escaneados con nmap versión 7.95.

2. Vulnerabilidades

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Ref.
22/tcp	SSH	OpenSSH 9.2p1 Debian 2+deb12u6	CVE-2014-4210	Afecta la confidencialidad a través de vectores relacionados con WLS - Servicios Web	CVE
			CVE-2024-6387	Escalado de privilegios de forma remota	CVE
			CVE-2023-38408	Ejecución remota de código si un agente se reenvía a un sistema controlado por un atacante	CVE
			CVE-2023-28531	La versión 9.3 añade claves de tarjeta inteligente a ssh-agent sin las restricciones de destino por salto previstas.	CVE

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Ref.
			CVE-2024-6387	Condición de carrera que puede provocar que sshd gestione algunas señales de forma insegura	CVE
			CVE-2025-26465	Un ataque de máquina en el medio puede ser realizado mediante una máquina maliciosa que se hace pasar por un servidor legítimo	CVE
			CVE-2023-51385	inyección del comando del sistema operativo	CVE
			CVE-2023-48795	Permite evitar las verificaciones de integridad	CVE
			CVE-2023-51384	Ciertas restricciones de destino se pueden aplicar de manera incompleta	CVE
			CVE-2025-32728	La Directiva de desactivación no se adhiere a la documentación que indica que deshabilita X11 y el reenvío de agentes.	CVE
80/tcp	http	Apache httpd 2.4.62	CVE-2014-4210	Permite a los atacantes remotos afectar la confidencialidad a través de vectores relacionados con WLS - Servicios web.	CVE
			CVE-2023-38709	Permite a los generadores de backend/contenido malicioso o explotable para dividir las respuestas HTTP.	CVE