MásQueSeguridad

13 de abril 2026

# LO MÁS RECIENTE

## >>> Herramientas Axios y Trivy comprometidas

Atacantes lograron "envenenar" las herramientas para programadores Axios y Trivy. Cuando un programador actualizaba su trabajo, el virus se instalaba automáticamente en los servidores.

**¿Por qué es grave?** No atacan al usuario final directamente, sino a la "fábrica" del software.

Se recomienda evitar el uso de estas herramientas mientras salen nuevos parches de correcciones.

## >>> Hallazgos históricos: Errores de 27 años descubiertos por IA

Investigadores de seguridad han logrado usar modelos de IA especializados para encontrar fallos de seguridad que llevaban décadas ocultos. Se detectó una vulnerabilidad en OpenBSD que tenía 27 años sin que nadie la viera, y otra de 16 años en la librería de video FFmpeg.

**La lección:** La IA ahora es capaz de leer millones de líneas de código en segundos y encontrar errores que a los humanos se nos pasaron por años. Esto es bueno (para arreglarlos) pero peligroso si los hackers lo usan primero.

## >>> IEl Parche de Emergencia de Fortinet (CVE-2026-35616)

Fortinet tuvo que lanzar un "parche de emergencia" para un programa llamado FortiClient EMS. Este programa es el que usan las empresas para controlar la seguridad de todas las computadoras de sus empleados desde un solo lugar.

**¿Cuál es el problema?** Se descubrió una vulnerabilidad de tipo "Zero-Day". Esta falla permite que un atacante entre al sistema sin necesidad de contraseña.

**¿Qué tan grave es?** Tiene una calificación de 9.1 sobre 10 (crítica).

FortiClient EMS
Enterprise Management Server

FORTINET