

"Erfolgreiche Jailbreak-Angriffe auf GenAI arbeiten mit schädlichen Prompts"

2025-08-12 06:43

Angriffe auf das Model Context Protocol häufen sich – keine Wunder, denn Anthropic hat es nicht in Hinblick auf Systemsicherheit entworfen, meint Mirko Ross.