

Sicherheitsalptraum MCP: Schädlicher Code und Datenverlust

2025-08-06 08:09

Das weit verbreitete Model Context Protocol eröffnet eine Vielzahl von Angriffspunkten auf die Systeme der User. Docker hat eine Übersicht veröffentlicht.