heise+ | Die Sicherheitsprobleme des Model Context Protocols

2025-08-11 13:00

Das Model Context Protocol verschafft KI-Agenten zahlreiche Fähigkeiten. Sicherheitsmaßnahmen wurden allerdings oft weder implementiert noch überhaupt bedacht.