Sicherheitslücke im Linux-Kernel

April April, der macht, was er will. Nach dem XZ-Utils-Fiasko taucht nun eine Lücke im Kernel auf, die Angreifern mit unprivilegiertem Zugriff auf das System über eine lokale Rechteausweitung (LPE) Root-Rechte verschaffen kann. Diese wurde bereits am 21. März erstmals gemeldet. Die Lücke wurde als CVE-2023-6546 katalogisiert.

Zwei statt nur einer

Der Angriff funktioniert allerdings nur, wenn sowohl das GSM-Subsystem als auch die Xen-Virtualisierung aktiviert sind. Es existieren bereits mehrere Exploits für verschiedene Kernel und Distributionen. In einer Diskussion auf der Kernel-Liste gehen die Entwickler davon aus, dass die Lücke geschlossen sei. Letztlich scheint es aber um zwei Lücken zu gehen, wie Sicherheitsforscher Kyle Zeng auf Openwall gestern berichtete. Demnach soll eine der beiden Lücken noch ungepatched sein.