Debian 13 (Trixie) – Säkerhetsöversikt

Detta dokument sammanfattar verifierbara säkerhetsförändringar i Debian 13 baserat på officiella release notes. Fokus ligger på vad som lagts till, tagits bort och vilka säkerhetsytor som minskats respektive kvarstår.

Kärnidé

Debian 13 representerar ett arkitektoniskt steg framåt: modern kernel, tydligare firmware-separation och borttagning av legacy-komponenter. Resultatet är minskad attackyta men högre krav på korrekt firmware.

Viktiga tillägg

Linux kernel 6.12 (LTS)

- Förbättrad KASLR och minnesisolering
- Starkare skydd mot Spectre/Meltdown-varianter
- Bättre IOMMU- och DMA-skydd

Separat non-free-firmware

Firmware är nu isolerat från övrig non-free-mjukvara, vilket förbättrar auditbarhet och minskar implicit exponering av binära blobs.

Borttaget och avvecklat

- Föråldrade paket utan aktiv upstream
- Äldre kryptografiska standarder
- Delar av legacy i386-stödet för desktop

Säkerhetseffekt

Debian 13 reducerar flera historiska sårbarhetsklasser: legacy TLS, föråldrade syscall-vägar och osäkra standardinställningar. Nyare toolchains (OpenSSL 3.2, GCC 14, systemd 256) eliminerar hela klasser av kända CVE-problem.

Kvarstående risker

- OEM-BIOS och ACPI-implementationer
- Proprietär firmware som inte kan fullständigt granskas
- Proprietära GPU-drivrutiner (t.ex. Nvidia)