Research @ Cyber-Defence Campus

Binder transaction allows root command execution

CVE: CVE-2026-114354 ↗

Product: DJI CrystalSky ZS600C

Severity: High 8.6

Published: 21.10.2026

The native binder service `android.dji.server`, registered by the root-privileged `assistant` daemon, exposes transaction code 1018, which passes a caller-supplied string directly to `system()` without any caller-identity or permission check. Any locally installed application with zero permissions can execute arbitrary OS commands as root.

Affected firmware: v0.3.9.7 through v0.6.6.9 (last release; device is EOL/unsupported). Verified from a permissionless APK (`uid=0`).

Back to vulnerabilities list

© Cyber-Defence Campus - cydcampus.admin.ch