Research @ Cyber-Defence Campus

`assistant` daemon hard-coded USB backdoor

CVE: CVE-2026-114353 ↗

Product: DJI CrystalSky ZS600C

Severity: High 7.0

Published: 21.10.2026

The root-privileged `assistant` daemon listens on the device's USB-gadget serial port (`/dev/ttyGS0`) and, upon receiving the hard-coded magic string `dji26656677`, enters a mode where each subsequent line is passed to `system()` and executed as root. A physically-present attacker with USB access can execute arbitrary OS commands on the device without authentication.

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

Back to vulnerabilities list

© Cyber-Defence Campus - cydcampus.admin.ch