Research @ Cyber-Defence Campus

Default-enabled unauthenticated ADB over USB

CVE: CVE-2026-114357 ↗

Product: DJI CrystalSky ZS600C

Severity: High 7.0

Published: 21.10.2026

The device ships with `ro.adb.secure=0`, so the ADB daemon performs no host authorization, and USB ADB is enabled by default. This gives an unauthenticated shell (uid 2000) out of the box; once ADB-over-TCP is enabled (e.g., via the shipped `/system/bin/adbd_tcp.sh` or `setprop persist.adb.tcp.port 5555`), the same unauthenticated shell is reachable over the network.

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

Back to vulnerabilities list

© Cyber-Defence Campus - cydcampus.admin.ch