Research @ Cyber-Defence Campus

DJIUpdateService Binder exposes privileged operations without authorization

CVE: CVE-2026-114356 ↗

Product: DJI CrystalSky ZS600C

Severity: High 7.0

Published: 21.10.2026

The system-privileged `DJIUpdateService` binder performs no caller-identity or permission check in `onTransact()` (CWE-862). A local application with no permissions can invoke privileged operations including clock/timezone change (transactions 101/123), shutdown (105), factory reset with user-data wipe (153), and the firmware-apply hand-off (151).

Affected firmware: v0.3.9.7 through v0.6.6.9 (last release; device is EOL/unsupported). Verified non-destructively (code 101 changed the system clock).

Back to vulnerabilities list

© Cyber-Defence Campus - cydcampus.admin.ch