Research @ Cyber-Defence Campus

Cleartext Transmission of Wi-Fi Credentials over Bluetooth

CVE: CVE-2026-77812 ↗

Product: DJI Quicktransfer procotol

Severity: Medium 5.7

Published: 21.08.2026

Advisory: Read the advisory ↗

The Bluetooth communication component used by the `QuickTransfer` feature of several DJI drone models transmits the WPA2 pre-shared key of the drone's Wi-Fi network in cleartext (CWE-319). An attacker within Bluetooth range can capture the BLE traffic and recover the passphrase in plaintext. Because the credential is static and re-sent on every `QuickTransfer` session, it can be captured repeatedly and reused indefinitely.

With the recovered key an attacker can authenticate to the drone's Wi-Fi access point as a legitimate client, interact with the network services the drone exposes, intercept the Wi-Fi traffic exchanged between the drone and the operator's Android/iOS device during `QuickTransfer` mode and also access live video stream from the drone among other functionalities. Successful authentication additionally allows downloading stored photos and videos without user's content without hte victim noticing.

Back to vulnerabilities list

© Cyber-Defence Campus - cydcampus.admin.ch