DJI Cybersecurity Assessment
Executive Summary
September 9, 2020

In 2020, FTI Consulting (FTI) completed a cybersecurity assessment of a select population of DJI's products and mobile applications. For this assessment, FTI was asked to conduct an analysis of hardware and software identified by DJI, which included select source code review of DJI applications, hardware cybersecurity review of devices, and vulnerability assessments of DJI-selected public-facing websites.

Review Scope	
Drones	DJI Matrice 210 RTK V2 v01.00.0590 DJI Phantom 4 RTK v02.02.0401 DJI Mavic 2 Pro v01.00.0510 DJI Mavic Mini v01.00.0300
Applications	DJI Go 4 App v4.3.32 (Android; iOS) DJI Pilot App v1.7.2 (Android; Crystal Sky controller [Android]) DJI Pilot Private Edition (PE) v1.6.1 (Crystal Sky controller [Android]) DJI FlightHub Enterprise v1.3.1 (Ubuntu server 18.04) DJI GS RTK v2.1.1-GSP (Phantom Cendence controller) DJI Fly v1.0.6 (Android; iOS) DJI GS Pro[1] v2.0.10 (iOS [iPad only])
Websites	active.dji.com mydjiflight.dji.com factory.fffsky.net us.djiservice.org djigo-hk.djiservice.org valueadded.djiservice.org cnblog.skypixel.com

Methodology and Access

FTI's network review of the in-scope devices focused on detecting, capturing, and analyzing network activity. All hardware was purchased independently through authorized DJI retail stores, an online retailer, and a drone retailer. All testing was conducted using industry standard tools and methods, and network traffic was captured under different scenarios.[2]

FTI used the flying configurations that were recommended by each device's user manual. Additionally, FTI tested alternative flying options, to test a broader range of flight scenarios that a user might attempt to conduct, including the option of Local Data Mode (LDM). The alternative flying options included the following:

[1] No source code assessment of DJI GS Pro was conducted.
[2] These scenarios included: collection while in idle state; collection while flying; collection while in idle state with reduced entitlements; and collection while flying with reduced entitlements.

- DJI Matrice 210 RTK v2
    - Crystal Sky Tablet
        - DJI Pilot with LDM
        - DJI Pilot with LDM and Map Request
        - DJI Pilot PE with FlightHub
    - Samsung Galaxy Tab S5e
        - DJI Pilot
        - DJI Pilot with LDM
        - DJI Pilot with LDM and Map Request
    - iPad Mini (5th Generation)
        - GS Pro
- DJI Phantom 4 RTK
    - Samsung Galaxy Tab S5e
        - DJI Pilot
        - DJI Pilot with LDM
        - DJI Pilot with LDM and Map Request
    - iPad Mini (5th Generation)
        - GS Pro

DJI provided FTI with access to more than 20 million lines of application source code, and consistent with the assessment scope, FTI conducted a targeted analysis for the in-scope products, with a focus on understanding communication protocols and destinations. Based on its hardware testing, FTI strategically targeted its source code review by focusing on specific sections of code related to communication protocols and network activity with host infrastructure. Once blocks of code were identified, FTI examined the entire file containing the code to understand the relevant functions and code logic.

FTI also conducted a web application vulnerability assessment on the in-scope public-facing websites selected by DJI, using an industry standard vulnerability scanning tool designed to assess vulnerabilities on the web application level.

Summary of Key Findings:

1. FTI observed a number of instances where DJI employed security best practices.
2. FTI found that when DJI's Local Data Mode (LDM) is enabled, no data that was generated by the application was sent externally to infrastructure operated by any third party, including DJI.
3. FTI found that Pilot PE used with FlightHub Enterprise provides an alternative method for operation that provides consumers additional control over the data they generate, as it requires installation on a local or cloud-based server. With this configuration, FTI observed no evidence of data being requested or transmitted externally.
4. FTI found some instances of low risk vulnerabilities in its application source code and website review; FTI assessed that these findings posed minimal risks to consumers.

Key Findings and Recommendations

Overall Security: FTI observed examples where DJI devices and services offer consumers configurations and options that employ security best practices, which help consumers to protect their networks and information. For example, in many observed instances, FTI found the use of the SSL pinning technique as an additional security layer for application traffic. As another example, DJI gives the consumer the option to enable HTTPS on the FlightHub server, as an additional security measure while using DJI Pilot PE.

Data Transmission: While FTI observed that use of the DJI drones in the United States can result in external data transmissions that are an expected aspect of using them, FTI also found that DJI offers options for configuration and operation that can both reduce and eliminate the generation and provision of data externally. These configurations involve the use of Local Data Mode (LDM) and DJI FlightHub Enterprise.

According to DJI[3], "when Local Data Mode is enabled, all data can only be used locally, and no network request will be initiated to send data to its own server or a third-party server." FTI's assessment confirmed that when LDM was enabled, no data that was generated by the application was sent externally to infrastructure operated by any third party, including DJI. An exception to this is when the user is operating with LDM and chooses to enable the "Map Request" feature; in this situation, FTI observed that the devices communicated with expected Mapbox[4] infrastructure for the provision of maps.

DJI Pilot PE is a custom version of DJI Pilot that is intended for users that operate FlightHub Enterprise, a version of FlightHub that is installed and hosted on a local or cloud-based server. FTI found that this configuration provides an alternative method for operation that provides consumers additional control over the data they generate, as it requires installation on a local server. With this configuration, FTI observed no evidence of data being requested or transmitted externally.[5]

FTI recommends that DJI take steps to increase availability and consumer awareness of these options. For example, providing a menu prompt to let the user know about LDM and updating the user manuals for each compatible drone would improve the consumer's ability to operate successfully using these configurations.

Potential Risks: FTI found some instances of the DJI controllers using outdated versions of Android, which could compromise the overall security of the associated devices. Alternative options for these controllers were tested and are available to consumers, reducing the risk of these vulnerabilities. FTI also identified one vulnerability on the reviewed websites, though FTI concludes this vulnerability poses little risk to DJI and its consumers.

---

[3] DJI Security White Paper, available here: https://security.dji.com/data/resources/

[4] Mapbox is an American provider of custom online maps for websites and applications.

[5] Offline maps on FlightHub Enterprise must to be downloaded and installed.