



BISHOPFOX
8240 S. KYRENE ROAD
SUITE A-113
TEMPE, AZ 85284
UNITED STATES

BISHOPFOX.COM

August 21, 2020

Parrot Drones SAS
174 quai de Jemmapes
75010 Paris
France

To Whom It May Concern:

Between July 20 and August 7, 2020, pursuant to our agreement with Parrot Drones SAS, the Bishop Fox assessment team conducted hybrid and mobile application assessments of the FreeFlight 6 mobile applications and API web services.

The assessment objective was to identify, within the designated time and scope, any data privacy and security issues in the FreeFlight 6 applications. The assessment team combined automated application vulnerability scanning, code review, and manual penetration testing techniques in order to identify data privacy concerns, locate attack vectors, and simulate real-world exploitation. The FreeFlight 6 applications used in testing were downloaded from Apple's App Store and Google's Play Store. The drones used for testing were purchased by Bishop Fox from a third-party retailer.

The assessment team reviewed the source code for both mobile applications (iOS and Android versions 6.6.9) and for the API web services hosted on `accounts.parrot.com`, `appcentral.parrot.com`, and `droneacademy.parrot.com`. The team determined that the FreeFlight 6 mobile applications available in the platform app stores appeared to match the provided source code. The provided source code did not exhibit obfuscation techniques. The assessment team did not identify any code or functionality in the applications or web services that appeared to go beyond the stated design and purpose of the application. The team did not discover any mechanisms to update or add on to the mobile applications outside of platform-released updates. Drone firmware updates are prompted to the user and are not initiated without the user's permission.

Additionally, the assessment team reviewed permissions granted by the applications against the behaviors and actions exhibited by the applications during testing. The team did not identify any suspicious activity that would indicate undisclosed data collection or data sharing beyond the permissions explicitly granted by the user through the applications. The assessment team was unable to gain unauthenticated access to any saved user data and

determined that user data saved into AWS cloud storage was purged upon user request.

The assessment team also reviewed interactions between the drones, mobile applications, and back-end API web services in the source code. The team did not discover any functions in the source code to transmit flight data to Parrot-controlled storage outside of user-approved drone flight logs. Additionally, the team did not observe any transmission of drone- or application-captured media (photos, videos, audio clips) other than user-initiated sharing to social media.

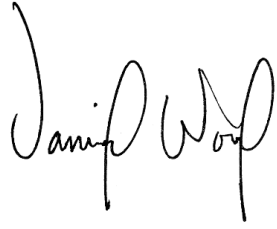
Finally, the assessment team compared their observations of the permissions and data privacy controls offered by the applications to Parrot's published privacy policy. No behaviors or functions were observed in the mobile applications, API web services, or source code that conflicted with the privacy policy available on the Parrot US corporate website, dated July 9, 2020.

Parrot Drones SAS has been provided the detailed findings and recommendations resulting from the engagement in an assessment report, which includes the following vulnerabilities:

- Medium-risk vulnerabilities
 - Authorization tokens without expiration (two instances)
 - Unencrypted application preferences files (four instances)
- Low-risk vulnerabilities
 - Hard-coded encryption key (one instance)
 - Lack of root and jailbreak detection (two instances)
 - Lack of certificate pinning (one instance)

The assessment team found no evidence that the discovered findings impacted customer privacy or allowed unauthorized access to stored user data. Parrot has accepted the risk of implementing authorization tokens without expiration, the lack of root and jailbreak detection, and the lack of certificate pinning. Parrot accepted these risks taking into account the following factors: improved consumer experience, full transparency of the FreeFlight 6 mobile application, the expectation that customers with sensitive use cases will employ external mitigations, and the low probability of Parrot customers being targeted for attack.

Sincerely,

A handwritten signature in black ink, appearing to read "Daniel Wood". The signature is fluid and cursive, with the first name "Daniel" and the last name "Wood" clearly distinguishable.

Daniel Wood
Associate VP of Consulting
Bishop Fox