DJI GOVERNMENT EDITION ANDROID & ASSISTANT UPDATE ANALYSIS

5/6/21

A look at what requested changes were implemented, and what changes were not made in an updated release of the DJI Government Edition Android Application, and DJI Assistant Government Edition 2

The point of contact for this report is
CW2. Adam Prater
Adam.S.Prater.mil@mail.mil

Table of Contents

Executive Summary

An analysis was done upon updated versions of DOI private build software used with DJI Government Edition drones. The evaluated software includes an updated Android application version 1.3.3, and an updated version DJI Assistant 2 for DOI, version 1.0.2. Filenames evaluated are:

- djipilot-Private-v1.3.3DOI-release-19756-20210204-1014.apk
- DA2 for DOI-V1.0.2.zip

The focus of the analysis of the updated GE private build software is only to determine if items and findings from previous audits were fixed. The audit documents used as a basis for items to verify fixed are entitled:

- DJI GOVERNMENT EDITION MAVIC PRO AUDIT – Created 7/30/20
- DJI GOVERNMENT EDITION MATRICE 600 PRO AUDIT – Created 8/14/20

The DJI Government Edition versions that were tested, show no malicious code or intent and are recommended for use by government entities and forces working with US services.

Issues Fixed in private Android DOI application:

- Application no longer explicitly allows unsecure HTTP traffic (network-security_config.xml).
- Amap is no longer an option for in-flight mapping, eliminating several issues, from data privacy concerns to insecure communication.
- The AES key to decrypt external storage log files containing PII & flight info no longer exists in public maven repositories.
- File libutmiss_jni.so that contacts Chinese domains utmiss.com / CAAC does not exist. It does not connect to domains in China
- Unencrypted log entries in an SQLite database giving PII / location are removed.
- Easter Egg displaying GE version of firmware on drone & controller removed.
- The ability to remove NFZ colors disabled; NFZ not displayed, unlike consumer version.
- GPS locations flown stored in encrypted logs in external storage are now obfuscated (counted as fixed and not fixed, as it was not removed entirely and could be reverse engineered).
- The phone permission is no longer asked for when the application first starts up.

Acceptable items in private Android DOI application

These items have been deemed not a major issue and are mitigable when needed or based on circumstances.

- External storage contains unencrypted flight records any other application can access, and that persist after the application is uninstalled.
- External storage AES encryption key
    "REDACTED" remains used, and the same key used with the consumer pilot application, and is publicly available in dependency repositories. It can be decrypted. This is for data protection.
- GPS locations flown stored in encrypted logs in external storage are now obfuscated (counted as fixed and not fixed, as it was not removed entirely and could be reverse engineered). This is for warranty support.
- Unencrypted log entries in an SQLite analytics database persist, could be removed entirely.
- Shared data and external storage can still be ADB backed up from the application.
- Excessive permissions still exist in the Android Manifest.
- The string fogger used to hide internals still uses the same key, " REDACTED". Secrets and keys such as this can still be found in libconfig.so. This is for data protection.
- Log files are still kept in external storage, and can be accessed by other applications.
- Exception handling not fixed, still throws detailed error messages.
- "NAME REDACTED" still displays as having signed the application.
- Despite Amap being disabled from the application, insecure URLs to Amap persist in the application.
- For informational purposes; Amap contains source code that could get the device ID.
- libBugly.so contains unnecessary analytics included in the private build.
- GB28181 video sharing features persist in strings.xml of Android.
- Pictures on the microSD still contain EXIF data.
- Unencrypted flight records in external storage contain GPS information where flown.
- ADB backup acquires all encrypted logs, unencrypted flight records, and more from the app due to use of external storage.

Issues Fixed in DJI Assistant 2 for DOI:

- DJI developer's name removed from package.json.

Issues Not Fixed in DJI Assistant 2 for DOI:

- Methods to contact DJI via HTTPS still exist in source code, however the code is not called by design.
- Asks for network access at first run; this should be unnecessary.
- Developer mode persists.
- Drone WebSocket encryption keys persist.
- Golang EXE with DOI references still found using the JEB reverse engineering tool.

DJI Government Edition Fix Verification Audit

Approach to Testing

- Find issue from previous audit.
- Ascertain validity of issue as candidate for fix verification. For example, new firmware was not supplied for the GE DJI drones, therefore any firmware issues from previous audits need not be verified.
- Execute the same reverse engineering technique with the same tool used in the previous audit of GE.
- Validate if the issue from the previous audit persists, or was fixed.

Findings for the android application are categorized using the OWASP Mobile Risks Top 10, available at https://owasp.org/www-project-mobile-top-10/.

Tools Used in Testing

- AndroBugs Framework https://github.com/AndroBugs/AndroBugs_Framework
- Android Backup Extractor https://github.com/nelenkov/android-backup-extractor
- Amass https://github.com/OWASP/Amass
- Android Debug Bridge https://developer.android.com/studio/command-line/adb
- Asar https://www.npmjs.com/package/asar
- AWS CLI https://aws.amazon.com/cli/
- DB Browser for SQLite https://sqlitebrowser.org/
- ExifTool https://exiftool.org/
- IntelliJ IDEA https://www.jetbrains.com/idea/
- Jeb Decompiler https://www.pnfsoftware.com/
- Kotlin https://kotlinlang.org/
- MobSF https://github.com/MobSF/Mobile-Security-Framework-MobSF
- SQLite https://sqlite.org/index.html
- Wireshark https://www.wireshark.org/

Document Layout

There are four major areas of interest covered in this audit document of the DJI Government Edition Mavic Pro drone:

Android Pilot PE

Only the private build DOI APK for the GE Pilot PE app was validated, version 1.3.3. Other versions of Pilot PE do exist, and can be public downloaded from DJI's website. It is recommended government pilots use only the 1.3.3 private build APK, and do not download Pilot PE directly from DJI, as it has less privacy safeguards, and is designed to communicate with DJI servers as expected.

Assistant GE

Version assessed was DJI Assistant 2 GE for DOI, version 1.0.2. This distribution is not available for public download.