Vulnerability Report

**EXECUTIVE SUMMARY**

The purpose of this vulnerability assessment report is to provide an analytical perspective on the drone’s cybersecurity defenses. The investigation comprised testing the GPS Navigation, Data Link Systems, and Wi-Fi. We have identified critical loopholes allowing unauthorized control and access to the drone’s internal system, risking its operational integrity and compromising confidentiality.

**AFFECTED COMPONENTS**

1. Radiocomm (GPS Navigation)  
2. Radiocomm (Data Link - Dual Frequency)  
3. Radiocomm (LongRange - 2.3 GHz / 2.4 GHz)  
4. Radiocomm (Data Link - Full Digital)  
5. WiFi (2.4/5 GHz)

**RISK RATING**

The overall risk is regarded as High. All components tested showed significant vulnerabilities, compromising drone operations and data integrity.

**VULNERABILITIES DESCRIPTION**

1. Radiocomm (GPS Navigation): The drone failed to detect false GPS coordinates and compromised waypoint functionality.   
2. Radiocomm(Data Link - Dual Frequency): Bypassed AES encryption and authentication, leading to data interception.   
3. Radiocomm (LongRange - 2.3 GHz / 2.4 GHz): Unauthorized access and control over the drone were achieved.   
4. Radiocomm (Data Link - Full Digital): High packet loss led to unfavorable operational interruptions and instability.   
5. Wifi (2.4 / 5 GHz): Significant Wi-Fi vulnerabilities enabled password cracking, data interception, and disruptions in connections.

**RECOMMENDATIONS**

1. Radiocomm (GPS Navigation): Improve algorithms to detect and discard false GPS coordinates. Consider integrating more robust anomaly detection mechanisms.  
2. Radiocomm (Data Link - Dual Frequency): Enhance AES encryption and strengthen the authentication process to prevent data interception.   
3. Radiocomm (LongRange - 2.3 GHz / 2.4 GHz): Implement strict authorization protocols preventing unauthorized control signal access.  
4. Radiocomm (Data Link - Full Digital): Enhance the digital link's resistance to packet loss or develop a failsafe mechanism for stability.  
5. WiFi (2.4/5 GHz): Adopt more robust password protocols, improve encryption standards, and secure connection re-establishment protocols to resist attacks.