Vulnerability Report

**Executive Summary**

The assessment included a rigorous of vulnerability tests on parts of drone’s radio communication and WiFi systems to identify any potential weaknesses. The system demonstrated strong resilience and effective detection mechanisms to a variety of attacks including GPS spoofing, AES encryption data interception, authentication spoofing and high packet loss creation. Furthermore, the WiFi defenses resisted password cracking attempts and deauthentication attacks. Despite these robust protections, a notable finding was the system's video feed degrading under high packet loss. All tests demonstrate that the drone is secure, yet there is still matrix of possible improvements.

**Affected Components**

1. \*\*Radiocomm (GPS Navigation):\*\* The GPS system proved resilient against spoofing and jamming resistance tests.  
   
2. \*\*Radiocomm (Data Link - Dual Frequency):\*\* The dual frequency data link can resist man-in-the-middle attacks.

3. \*\*Radiocomm (LongRange - 2.3 GHz / 2.4 GHz):\*\* The LongRange band authentication security is robust against spoofing attempts.

4. \*\*Radiocomm (Data Link - Full Digital):\*\* The Full digital data link successfully maintained control under high packet loss; though the video feed degraded.

5. \*\*WiFi (2.4 GHz / 5 GHz):\*\* The WiFi system showed resilience against password cracking, man-in-the-middle attacks, and deauthentication attacks.

**Risk Rating**

- \*\*Medium: \*\* Degradation of Video feed due to high Packet loss can be of potential risk.

All other component tests pose little to no risk as effective mitigations are in place.

**Vulnerabilities Description**

1. \*\*GPS Spoofing and Jamming:\*\* The drone’s GPS system proved resilient under tests of GPS spoofing and signal jamming.  
   
2. \*\*Interception of Dual Frequency Data Link:\*\* MIM attacks on the dual-frequency data link are resisted by AES encryption.

3. \*\*Authentication Spoofing on LongRange Band:\*\* Spoofing an authentication signal has no effect on the drone due to key-based authentication.

4. \*\*Packet Flooding on Data Link:\*\* Drone maintained control and system responsiveness despite high packet loss, however, the video feed degraded under these conditions.

5. \*\*WiFi Password Cracking, Deauthentication, and MITM Attacks:\*\* The strong WiFi WPA2/WPA3 encryption withstood password attempts, experienced brief disconnects from deauth frames but reconnected securely, and effectively blocked MITM attacks.

**Recommendations**

1. \*\*Investigate Control over High Packet Loss:\*\* While the drone maintains control during high packet loss situations, the video feed suffers degradation. Investigatory measures should be implemented to prevent or mitigate this degradation for continued visibility.

2. \*\*Continuous Security Updates:\*\* Regular security patches and software updates should be introduced regularly to combat new threats and maintain system integrity.

3. \*\*Further Simulation Testing:\*\* To ensure robustness of all systems, more extensive simulation testing is recommended, including worst-case scenarios for all components.