📄 VAPT Auto-Generated Vulnerability Report

## 3.1 Test GPS spoofing resistance

|  |  |
| --- | --- |
| Clé | Valeur |
| - CVSS | 7.8 |
| - Risk Level | High |
| - Description | The penetration test revealed a severe vulnerability in the drone's GPS navigation system. HackRF One with GPS-SDR-SIM was successfully used to inject false GPS coordinates, causing the drone to be misled through its Waypoint, GoTo, or GoHome functions. The system failed to detect anomalies or enter into a safe mode, leading to an off-course drift with no subsequent correction. |
| - Risks | This vulnerability presents a real risk of malicious interference, allowing an attacker to redirect the drone from its intended course. In addition to theft or misuse of the drone itself, an attacker could potentially use the drone for unauthorized surveillance or, in a worst-case scenario, as a weapon. |
| - Complexity | Medium. The attack required the use of sophisticated tools and knowledge of GPS systems but did not seem to require advanced knowledge of the drone's specific software or hardware architecture. |
| - Priority | High. Given the potential risks involved, it's crucial that this vulnerability is addressed as soon as possible. |
| - CWE/CVE reference | This vulnerability doesn't seem to correspond directly to a specific entry in the Common Weakness Enumeration (CWE) or the Common Vulnerabilities and Exposures (CVE) databases. However, it could be considered an instance of CWE-346: Origin Validation Error, which describes situations where a software system fails to verify that data has come from a legitimate source. |
| - Reference URLs | Not available. In conclusion, immediate measures need to be taken to strengthen GPS spoofing resistance, perhaps by incorporating additional checks or fallback systems to detect and correct for GPS anomalies, and ensuring these systems are always active during operation. Stronger encryption and validation protocols for GPS data may also be required. |

## 3.2 Test GPS signal jamming resilience

|  |  |
| --- | --- |
| Clé | Valeur |

## 3.3 Test man-in-the-middle (MITM) attack on 2.4 GHz / 5 GHz

|  |  |
| --- | --- |
| Clé | Valeur |
| Vulnerability Summary |  |
| - CVSS | 8.8 (High) |
| - Risk Level | High |
| - Description | The penetration test result indicates a high-risk man-in-the-middle (MITM) vulnerability in the Radiocomm Dual Frequency Data Link. An attacker can set up a rogue access point, carry out ARP spoofing, and intercept control and video data. There is evidence of weak or non-existent AES encryption, which leads to a breach of data confidentiality and integrity. |
| - Risks | This vulnerability enables an attacker to intercept sensitive data such as video and control commands. It also allows the attacker to potentially disrupt operational capabilities or even take control of the drone system. This issue leads to significant integrity, confidentiality, and availability risks which could potentially result in unauthorized usage or manipulation of the system. |
| - Complexity | Medium. Setting up a rogue access point, performing ARP spoofing, and bypassing or breaking AES encryption require specialized technical knowledge and skill. |
| - Priority | High. This is a significant vulnerability that could potentially allow an attacker to compromise the system, thereby demanding immediate attention. |
| - CWE/CVE reference | As this vulnerability seems to be related to a lack of strong encryption during data transmission and robust authentication processes, the most appropriate Common Weakness Enumeration (CWE) would be CWE-311: Missing Encryption of Sensitive Data. A specific Common Vulnerabilities and Exposures (CVE) reference cannot be given unless the vulnerability had been officially documented in the CVE system. |
| - https | //cwe.mitre.org/data/definitions/311.html |
| - http | //zerodayinitiative.com/advisories/ZDI-20-1288/ Please note that a proper security fix must be implemented immediately. This should include employing strong, reliable encryption algorithms for data transmission, reliable authentication mechanisms, and frequent verification of network devices' integrity. The system should also be patched and updated regularly to reduce potential susceptibility to further attacks. |

## 3.4 Test LongRange band authentication security

|  |  |
| --- | --- |
| Clé | Valeur |
| Subject | Penetration Test Report - RadioComm LongRange Band Authentication Security Dear Team, Following the recently conducted penetration test on the RadioComm LongRange (2.3 GHz / 2.4 GHz) Interface, I am pleased to present our findings. Our comprehensive approach involved spoofing a control signal on the 2.3 GHz or 2.4 GHz spectrum, essentially mimicking the authentication behavior of the GCI Touch Interface. Our tool of choice was the BladeRF x40 SDR, aided by custom modulation scripts. The goal was to test the resilience of the system against potential unauthorized access that could compromise its integrity. Under these simulated attack conditions, the system's response was commendable. It robustly denied the spoofed control signal, indicating the efficiency of the key-based authentication protocol in place. The drone showcased a strong resistance by not responding to unauthorized commands. Based on this assessment, I confirm that the LongRange Interface possesses a solid defense mechanism, proving resilient during the tests. The penetration test was indeed successful, and I reaffirm the commendable security measure upheld by this system. We continue to stand by our commitment to ensure maximum system security at all times. We will proceed with further tests as scheduled, and any discovered vulnerabilities will be addressed immediately. Thank you for your cooperation and assistance during this assessment. Best regards, [Your Name] [Your Position] [Your Contact Information] |

## 3.5 Test data integrity under high packet loss

|  |  |
| --- | --- |
| Clé | Valeur |
| Vulnerability Summary |  |
| - CVSS | 7.5 (High) |
| - Attack Vector | Network |
| - Attack Complexity | Low |
| - Privileges Required | None |
| - User Interaction | None |
| - Scope | Unchanged |
| - Confidentiality | None |
| - Integrity | High |
| - Availability | High |
| - Risk level | High |
| - Description | The Radiocomm data link vulnerability under high packet loss conditions can lead to the freezing or corrupting of the video stream, delayed or dropping of control commands, and cause the drone to be unresponsive or unstable. |
| - Risks | The risks associated with this vulnerability include loss of control over the drone, which in turn could lead to damages, accidents, or security breaches if the drone is being used for surveillance or delivery purposes. Additionally, corrupted video feeds can render the drone useless for surveillance or observation tasks. |
| - Complexity | The attack complexity is low, the attacker only needs to flood the data link with malformed packets to initiate the vulnerability. |
| - Priority | Given the risks associated with this vulnerability and the wide-ranging implications for the applications of the drone, this vulnerability should be a high priority for mitigation. |
| - CWE/CVE Reference | N/A, custom vulnerability related to high packet loss conditions in Radiocomm data link, which is not common and not categorized under standard CWE/CVE. |
| - Reference URLs | N/A. |
| Mitigation Steps | 1. Improve packet loss resilience in Radiocomm data link. 2. Implement error-checking and auto-retry mechanisms for control commands. 3. Design the drone to enter a safe mode when high packet loss is detected. 4. Enhance streaming protocols to handle packet losses better, ensuring minimal degradation in video feed quality. |
| Notes | This vulnerability should not be taken lightly due to the potentially severe consequences. It is recommended that the manufacturer conduct thorough testing under high packet loss conditions to better handle such scenarios. |

## 3.6 Test WiFi authentication security

|  |  |
| --- | --- |
| Clé | Valeur |

## 3.7 Test WiFi MITM attack

|  |  |
| --- | --- |
| Clé | Valeur |
| \*\*Vulnerability Summary | \*\* |
| - \*\*CVSS | \*\* 7.8 (High) |
| - \*\*Risk Level | \*\* High |
| - \*\*Description | \*\* The WiFi access point security shows a high level of vulnerability to Man-The-Middle (MITM) attacks, which may allow unauthorized third parties to manipulate or capture any network traffic. In this test, a rogue WiFi Access Point (AP) was created using a Pineapple WiFi device, sslstrip was used to downgrade HTTPS connections and capture video/control data which puts data privacy at risk. |
| - \*\*Risks | \*\* If a real-world attacker performs such an attack, it may result in unauthorized access to sensitive data due to downgrading of HTTPS connections, along with the control of devices leading to potential misuse or damage. This vulnerability also exposes the WiFi to threat vectors such as sniffing and session hijacking. |
| - \*\*Complexity | \*\* Medium The complexity is considered medium because it requires the attacker to have specific technical knowledge, and tools like a Pineapple WiFi device, and software such as sslstrip. |
| - \*\*Priority | \*\* High Due to the potential risk of data breaches and unauthorized device control, this vulnerability should be a high priority for remediation. |
| - \*\*CWE/CVE reference | \*\* |
| While there is not an exact match CWE for this vulnerability, it closely aligns to CWE-294 | Authentication Bypass by Capture-replay. Relevant CVEs might depend on the specific product but an example could be CVE-2016-8747 concerning the vulnerability of Apache HttpComponents client in handling malicious responses during HTTPS sessions. |
| - \*\*Reference URLs | \*\* |
| 1. [CWE-294 | Authentication Bypass by Capture-replay](https://cwe.mitre.org/data/definitions/294.html) |
| 2. [CVE-2016-8747](https | //cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8747) |
| 3. [WiFi Pineapple Introduction](https | //www.wifipineapple.com/) |
| 4. [sslstrip tool introduction](https | //moxie.org/software/sslstrip/) |
| \*\*Recommendation\*\* | Given the insecure nature of the current WiFi setup, it is recommended to leverage advanced encryption techniques like WPA3, enforce HTTPS, and shield against rogue WiFi AP creation. Awareness programs should be conducted regularly for all users to identify and avoid connecting to any rogue APs. |

## 3.8 Test WiFi deauthentication attack

|  |  |
| --- | --- |
| Clé | Valeur |