JXL Car Infotainment Vulnerability

CVE-2025-69515

Prepared By: Shubham S. Thorat

April 7, 2026

Contents

Chapter 1

Introduction

1.1 Overview

This document summarizes a vulnerability identified in the automotive infotainment system during the security assessment. The research focused on how the infotainment unit processes GPS signals and handles externally received satellite data. It was observed that the JXL 9 Inch Car Android Double Din Player running Android v12.0 accepts spoofed GPS signals without proper validation, allowing an attacker to broadcast falsified signals and force the device to report a fixed or incorrect location instead of the vehicle's actual position.

1.2 Research Team

This research was carried out by **Shubham S. Thorat**, an automotive security researcher with over three years of professional experience in wireless communication security, in-vehicle network (IVN) assessments, and hardware-level analysis.

1.3 Methodology

The assessment evaluated how the infotainment system processes GPS signals and determines its location by transmitting crafted GPS signals using an external RF setup. These signals mimicked legitimate satellite transmissions but contained predefined coordinates. During testing, the JXL 9 Inch Car Android Double Din Player running Android v12.0 locked onto the spoofed signals and reported the injected static location instead of the actual position, confirming susceptibility to static GPS spoofing due to lack of proper signal validation.

Chapter 2

Summary

Below table lists the total vulnerabilities identified during the assessment.

Vulnerability Category	**Count**
High Severity Vulnerabilities	0
Medium Severity Vulnerabilities	1
Low Severity Vulnerabilities	0
Informational Findings	0
Total	**1**

Table 2.1: Total Vulnerabilities Identified

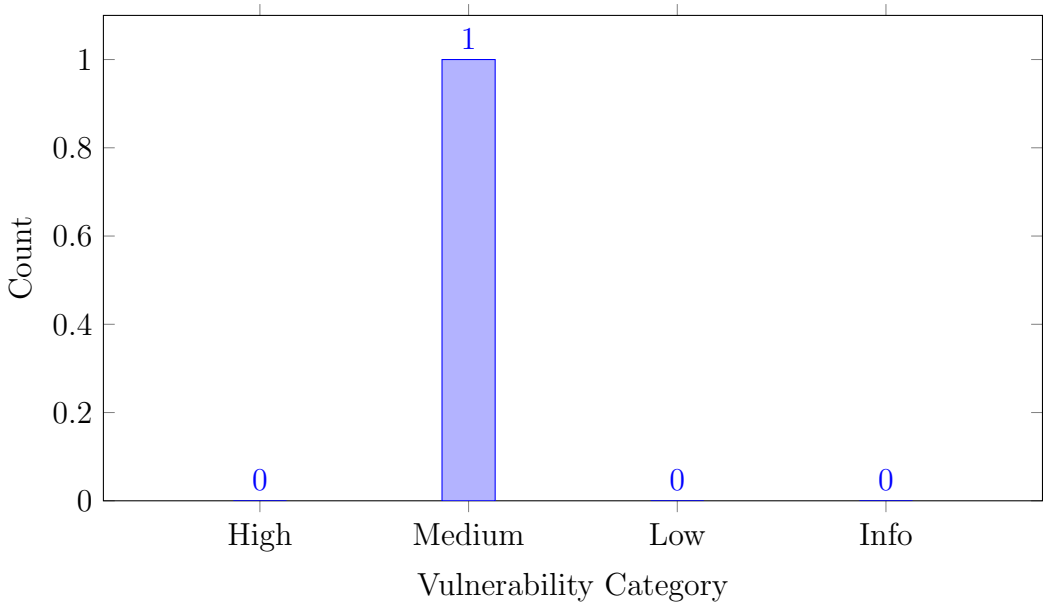


Figure 2.1: Vulnerability Distribution Bar Graph

Vulnerability ID	**Vulnerability**	**Severity**
VUL-001	Static GPS spoofing on Infotainment System	Medium

Table 2.2: List of Vulnerabilities with Severity

Chapter 3

Detailed Description of the Vulnerabilities and Findings

3.1 Vulnerabilities

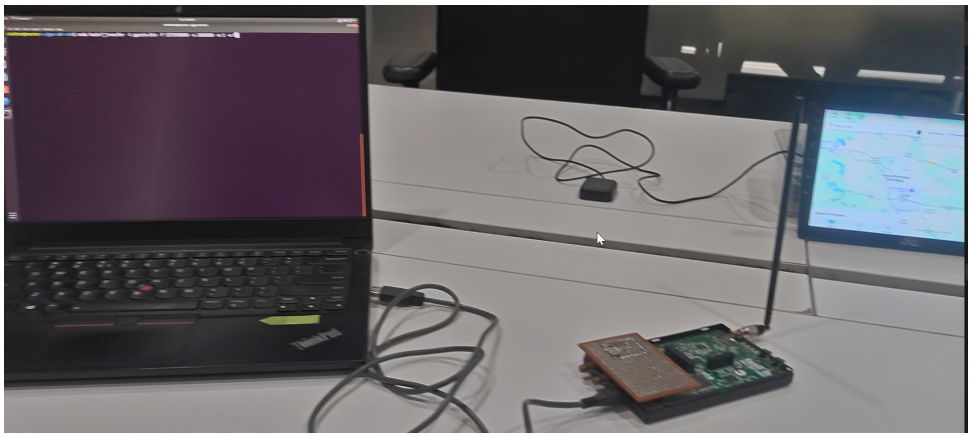
3.1.1 Vulnerability 1: Static GPS Spoofing

Description :
A vulnerability was identified in the GPS signal processing of the JXL Infotainment System, which relies on standard civilian GPS signals for location determination without performing sufficient validation or authenticity checks on the received data. Due to this lack of verification, an attacker in proximity can transmit forged GPS signals using a Software Defined Radio (SDR) device such as the HackRF One, mimicking legitimate satellite transmissions and overriding genuine signals. As a result, the infotainment system processes these spoofed inputs and computes an incorrect, attacker-controlled static location without detecting anomalies, leading to potential impacts such as inaccurate navigation, unintended geofencing behavior, and misuse of location-based functionalities, all without requiring direct access or authentication.

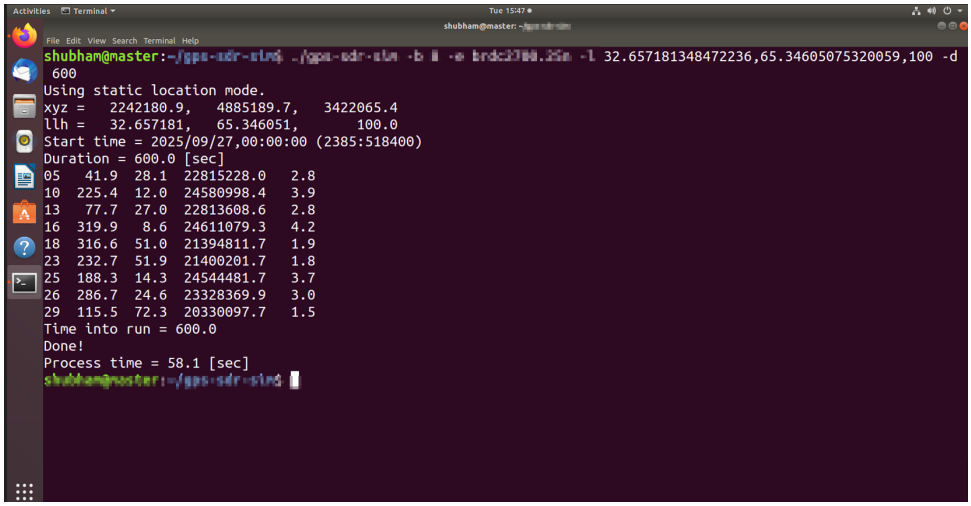
Impact :
Successful exploitation of this vulnerability allows an attacker to manipulate the perceived geographic location of the JXL Infotainment System. By forcing the system to compute a falsified static position, the attacker can cause incorrect navigation routes, misleading map information, and unintended behavior in location-based features such as geofencing. This may result in disruption of normal system functionality, reduced reliability of navigation services, and potential safety concerns if users rely on incorrect location data. Additionally, any applications or services dependent on accurate GPS input may behave unpredictably, leading to improper decision-making or misuse of location-dependent features.

Test Methodology :

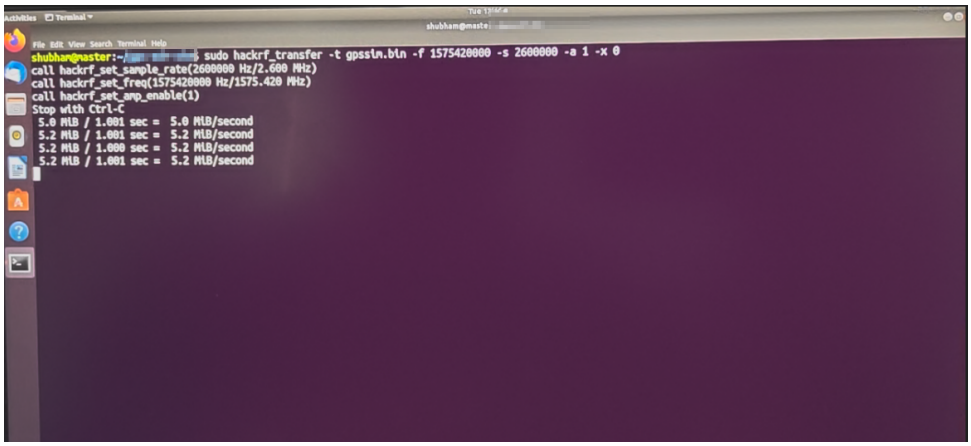
1. Connect the HackRF One to a host system and ensure required drivers and tools are properly configured.



2. Generate a GPS signal file with predefined (attacker-controlled) coordinates representing the target spoofed location.



3. Start broadcasting the crafted GPS signals over the air using the SDR device.



CVSS Base Vector: Base Core:5.4

AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L

CVE-2025-69515