JXL Car Infotainment Vulnerability

CVE-2025-63896

Prepared By: Shubham S. Thorat

December 3, 2025

Contents

Chapter 1

Introduction

1.1 Overview

This document summarizes the vulnerabilities identified in the automotive infotainment system during the security assessment.The research focused on evaluating how the infotainment unit communicates, processes external inputs, and exposes interfaces such as BLE. The findings highlight multiple weaknesses that could enable unauthorized access, data leakage, or unintended interaction with infotainment functions.

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 focused on evaluating the infotainment system's BLE interface for unauthorized interaction possibilities. The testing involved analyzing exposed BLE services and characteristics to determine whether they permitted unintended input or command injection. Traffic behavior, pairing mechanisms, and access permissions were reviewed to identify conditions where external devices could transmit unsolicited keystroke-like inputs to the system. All observations were validated through controlled testing to confirm the impact and reproducibility of the identified vulnerabilities.

Chapter 2

Summary

Below table lists the total vulnerabilities identified during the assessment.

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

Table 2.1: Total Vulnerabilities Identified

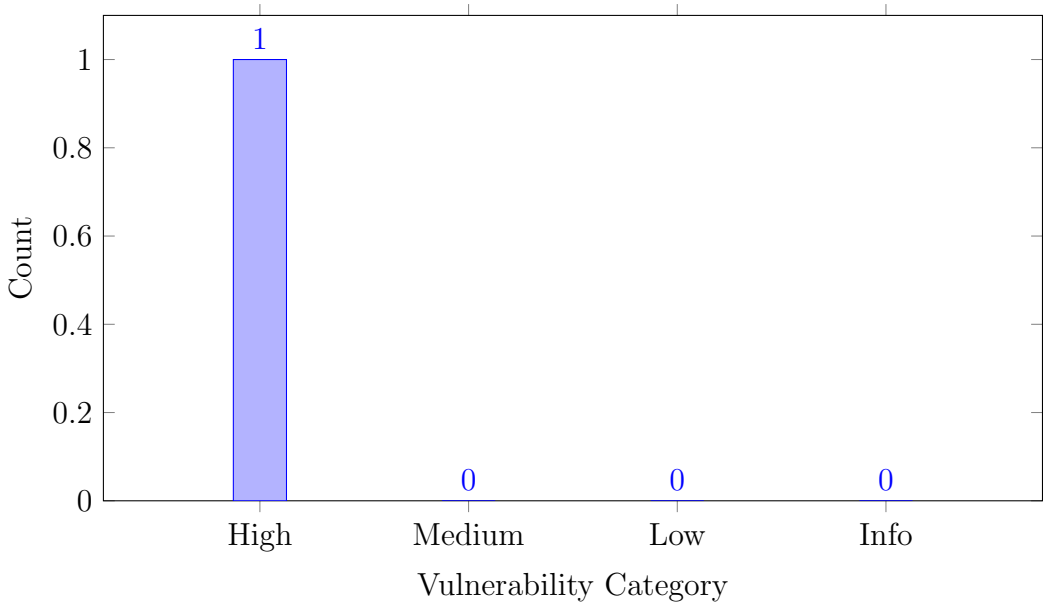


Figure 2.1: Vulnerability Distribution Bar Graph

Vulnerability ID	**Vulnerability**	**Severity**
VUL-001	Wireless Keystroke Injection	High

Table 2.2: List of Vulnerabilities with Severity

Chapter 3

Detailed Description of the Vulnerabilities and Findings

3.1 Vulnerabilities

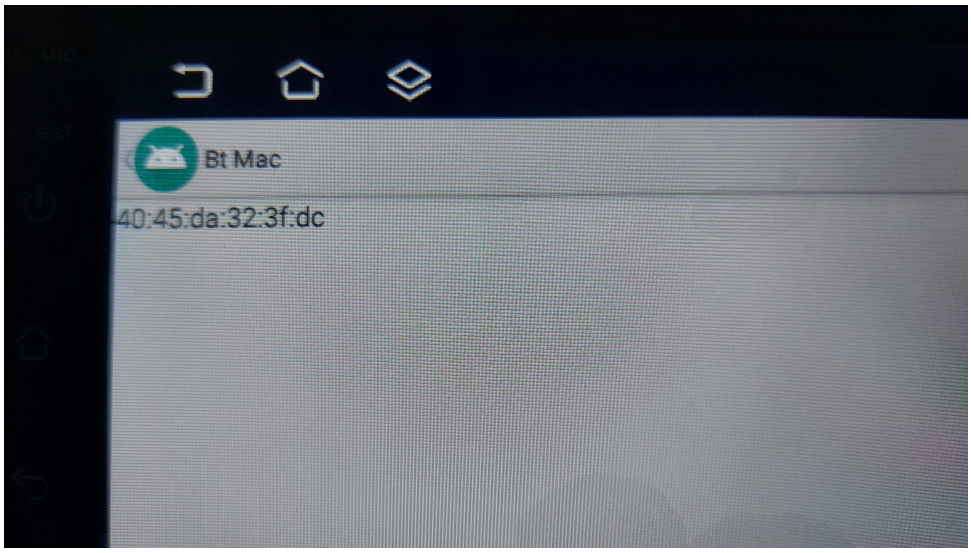
3.1.1 Vulnerability 1: Wireless Key Stroke Injection

Description :
A vulnerability was identified in the Bluetooth Human Interface Device (HID) handling mechanism of the infotainment system running Android v12.0. The BLE stack and input-processing components accept peripheral devices with insufficient verification, allowing a spoofed HID device to be recognized as a legitimate input source. As a result, the system may process unsolicited keystroke inputs originating from external, non-trusted wireless devices. This behavior exposes the infotainment unit to unauthorized interaction through its BLE interface.

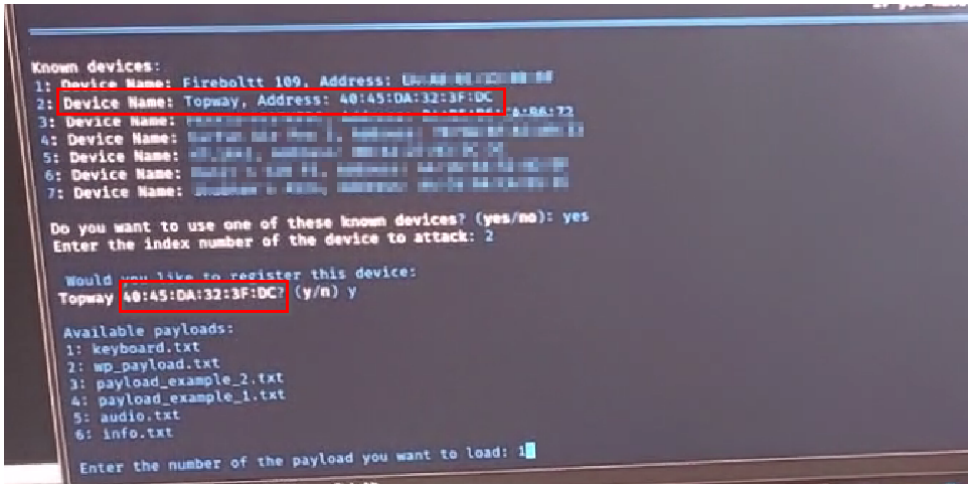
Impact :
Successful exploitation allows an attacker within Bluetooth range to inject unauthorized keystrokes into the infotainment system. This can lead to unintended menu navigation, application launches, setting modifications, and interaction with system features without user consent. Although it does not directly affect other vehicle ECUs, it poses a significant risk by enabling remote manipulation of infotainment functions.

Test Methodology :

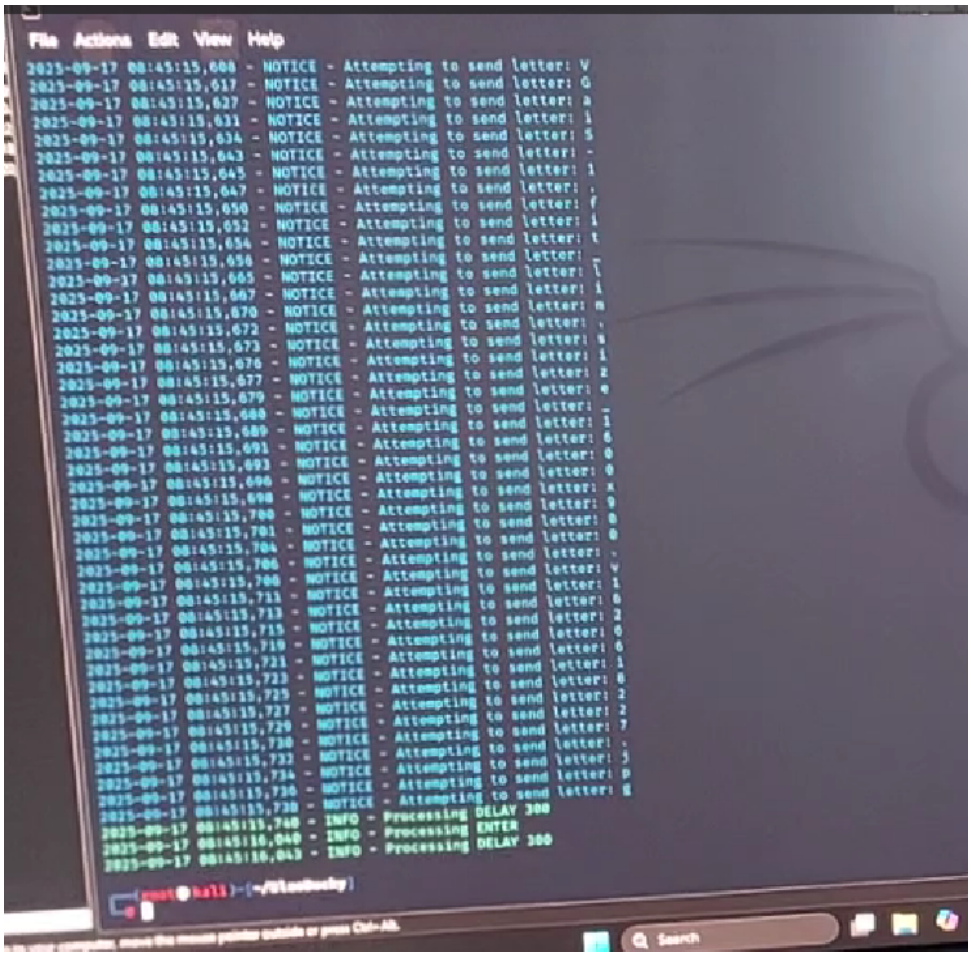
1. After basic reconnaissance, the BLE MAC address of the infotainment system was identified.



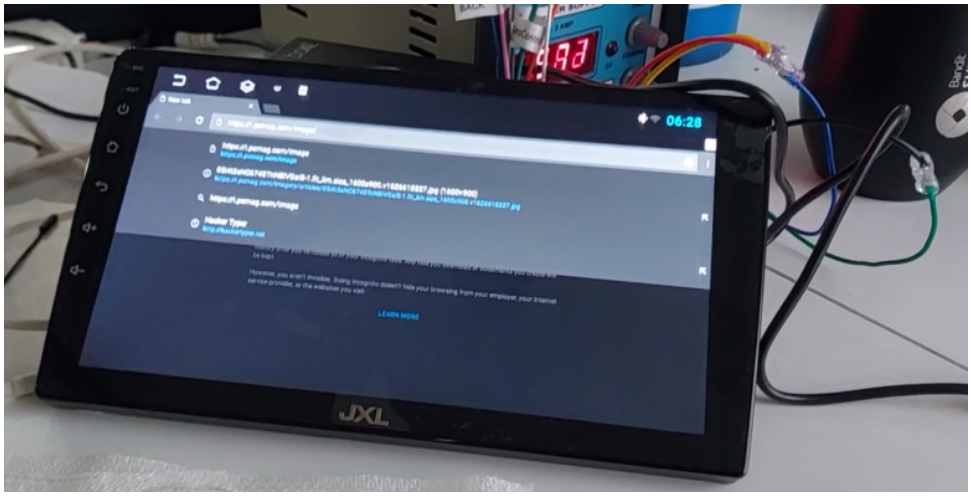
2. The target device was scanned using the obtained MAC address to confirm its presence and communication state.



3. A controlled input sequence was selected to test how the infotainment system handles external BLE-based interactions.



4. The sequence was then transmitted to the target, allowing observation of how the system processes unsolicited keystroke-like inputs.



Note: The device uses minimal pairing security, relying only on a simple Yes/No confirmation.

CVSS Base Vector: Base Core:7.6

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

CVE-2025-63896