CVE

CVE-2025-67133: Denial of Service via Unauthenticated BLE Connection

An issue in Hero Motocorp Vida V1 Pro 2.0.7 allows a local attacker to cause a denial of service via the BLE component

CVE-2025-67133

Product: Hero MotoCorp VIDA V1 Pro
Firmware: 2.0.7
Severity: Medium (5.3 CVSS v4.0)
Researcher: threadpoolx
Status: Vendor Notified
Discovery Date: 29 November 2025

---

1. Overview

Vulnerability Title

Denial of Service – Unauthenticated BLE CONNECT

Affected Product

- Hero MotoCorp VIDA V1 Pro
- Firmware Version: **2.0.7**

Severity

5.3 – Medium (CVSS v4.0)

CVE-2025-67133

---

2. Executive Summary

A denial-of-service condition exists in the VIDA V1 Pro BLE stack.
An unauthenticated device can connect to the scooter's BLE interface using nRF Connect or similar tools.
Once connected by the unauthorized device, the official **My VIDA mobile app** becomes unable to connect, effectively locking legitimate users out temporarily.

The issue arises due to a lack of authentication or bonding requirements before accepting BLE connections.

---

3. Affected Components

- **Firmware 2.0.7**
- BLE connection handling logic
- BLE authentication/bonding flow

---

4. Technical Description

The vulnerability stems from the device accepting **unauthenticated BLE connections**.
A rogue device can establish a BLE connection with the scooter without pairing or bonding, occupying the BLE session slot and preventing the legitimate app from establishing its connection.

This results in a temporary **Denial of Service (DoS)** for the user.

---

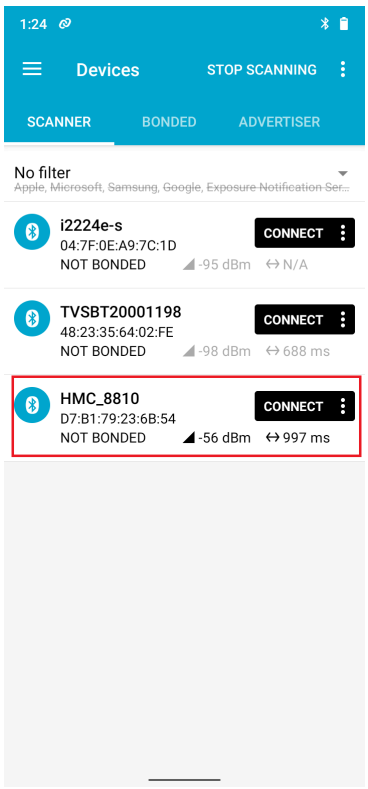
5. Proof of Concept (PoC)

5.1 Steps to Reproduce

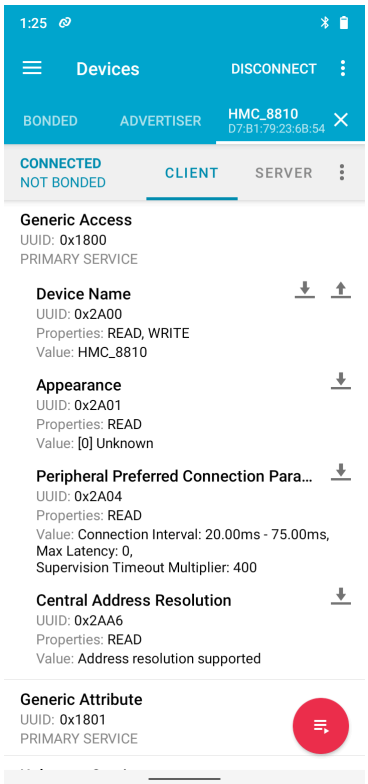
1. Open the **nRF Connect** Android application.
2. Scan for nearby BLE devices and locate **HMC_8810** (VIDA V1 Pro).
3. Tap **Connect** — connection is established **without authentication**.
4. Now open the **My VIDA** app and attempt to connect.
    - The device no longer appears or is reported as unavailable.

5.2 Evidence / Output

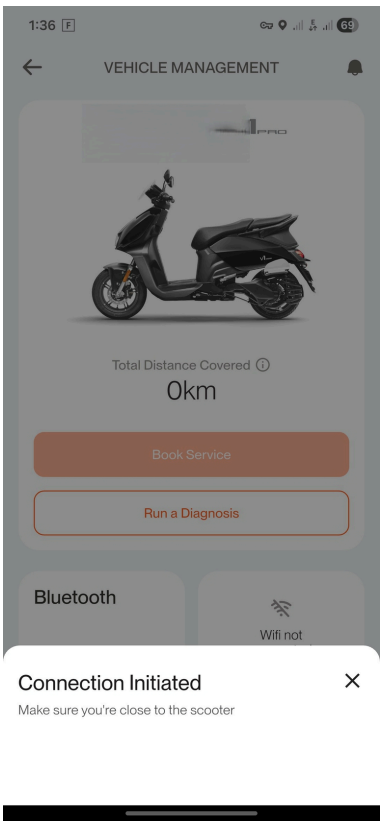
1. BLE device discovered via nRF Connect



2. Device Name characteristic visible & writeable (0x2A00)



3. My VIDA app is unable to find or connect to the scooter



5.3 Exploit Conditions

The attack is possible when:

- The scooter BLE module is **not actively connected** to any official app.
- The attacker is within **BLE range (~10 meters)**.
- No prior pairing or authentication is required.

---

6. Impact Analysis

Security Impact

Impact Type	Level
Confidentiality	None

Integrity	None
Availability	**Low** (DoS – temporary)

Attacker Capabilities

An attacker can:

- Connect to the scooter BLE module
- Block the legitimate user from connecting
- Disrupt app-based interactions temporarily

This attack does **not** grant code execution, data access, or permanent control.

---

7. CVSS Score (v4.0)

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
Base Score: 5.3 (Medium)

---

8. Suggested Remediation

The scooter should enforce:

- **BLE pairing/bonding**, or
- **Authenticated connection checks**
- Preventing connections from unauthorized/unpaired devices
- Requiring the official app to authenticate before establishing BLE sessions

Additionally:

- Reject connections without pairing
- Close stale or unauthorized connections immediately.

Previous
CVE

Last updated 3 months ago