DRONA CYBER SOLUTIONS

DRONA CYBER SOLUTIONS PVT LTD

BMS-STALL: Unauthorized Over-the-Air BLE Disruption of EV Battery Management Systems

An active, widespread operational threat targeting India's electric vehicle (EV) micro-mobility ecosystem specifically impacting commercial three-wheelers (e-rickshaws). Malicious actors exploit unauthenticated Bluetooth Low Energy (BLE) interfaces to remotely manipulate critical battery switches, forcing instant propulsion loss mid-ride and creating severe kinetic public safety hazards.

PREPARED BY
Drona Cyber Solutions

DATE OF ISSUE
July 4, 2026

CLASSIFICATION
UNRESTRICTED

CYBERSECURITY ADVISORY REPORT

BMS-STALL: Over-the-Air EV Disruption

RED // CRITICAL RISK

Issuer: Drona Cyber Solutions Pvt Ltd | **Classification:** UNRESTRICTED | **Target Sector:** EV Micro-Mobility

1. Executive Summary

An active and widespread operational security threat has been identified within India's electric vehicle (EV) micro-mobility ecosystem, specifically targeting commercial three-wheelers (e-rickshaws) [cite: 286]. Unauthorized third parties are executing remote over-the-air disruptions to disable moving vehicles mid-ride, generating extreme public safety hazards [cite: 287].

This vector does not require advanced software exploits, cloud infrastructure hijacking, or cryptographic compromise [cite: 288]. Instead, it exploits a foundational architectural vulnerability: completely unauthenticated Bluetooth Low Energy (BLE) interfaces exposed by mass-market Battery Management Systems (BMS) [cite: 289]. Utilizing readily available mobile diagnostic applications—such as `BAT-BMS`, `LOSSIGY`, and `XiaoXiangElectric`—any adversary within a 10-to-15-meter range can establish an unauthenticated peer-to-peer connection to a vulnerable vehicle's battery pack and instantly toggle the power discharge state to OFF [cite: 290].

> **[!!] CRITICAL ALERT: SYSTEMIC SUPPLY CHAIN EXPOSURE**
>
> The underlying issue affects an estimated **2.5 to 3.5 million e-rickshaws** across India, representing **60% to 70% of the active transit fleet** [cite: 513]. Due to widespread reliance on unregulated component assemblies, imported smart BMS units are integrated without altering factory firmware configurations or implementing standard link-layer authentication profiles [cite: 366].

2. Threat Landscape & Attack Mechanics

2.1 The Underlying Vulnerability

Modern lithium-ion battery packs require an internal monitoring and balancing circuit known as a Battery Management System (BMS) to preserve thermal and electrical safety boundaries [cite: 295]. To facilitate convenient local parameter tracking (voltage, temperature, State of Charge), many overseas manufacturers install low-cost integrated or external BLE communication modules [cite: 296].

Figure 1: Architectural Representation of Bluetooth Vulnerability Vectors in EV Smart Battery Management Systems.

The critical security failure stems directly from **Missing Authentication for Critical Functions** [cite: 299]. Hardware sourced from industrial suppliers (including platforms running JBD/Jiabaida-derived architectures) is shipped from factories with the following default parameters [cite: 300, 301]:

- **Absent Pairing Authentication:** No Bluetooth pairing PIN is required, or a universally documented default PIN (e.g., `000000` or `123456`) is deployed [cite: 302].
- **Open Write Permissions:** Unrestricted write permissions are exposed on critical control registers, specifically the software switches governing the battery's MOSFET charge and discharge gates [cite: 303].
- **No Access Whitelisting:** Access Control Lists (ACLs) are completely missing, preventing the system from restricting connections to authorized paired diagnostic hardware [cite: 304].

2.2 Attack Execution Vector Flow

The attack surface requires zero technical proficiency, converting an electronic threat into a vehicle for physical sabotage or localized pranking [cite: 333]. The execution sequence proceeds through four core stages [cite: 336]:

1. **Discovery Phase:** The attacker launches a standard diagnostic application which automatically issues a BLE scan command [cite: 353]. Unsecured battery modules continuously broadcast their availability via open BLE advertising packets [cite: 354].
2. **Connection Phase:** The attacker selects the targeted vehicle from the discovered device registry [cite: 355]. Since no link-layer challenge exists, a stable peer-to-peer connection is established in seconds [cite: 356].
3. **Command Injection:** Within the app's diagnostic interface, the attacker toggles the "Discharge Switch" to OFF [cite: 357, 358]. The application writes an unauthenticated control command directly across the BLE link [cite: 358].
4. **Physical Impact:** The BLE UART bridge module relays this state-change command to the main BMS microcontroller (MCU) [cite: 344, 347, 359]. The BMS opens the discharge circuit, current drops to 0A, and the vehicle suffers an instant mid-ride stall [cite: 348, 349, 360, 361].

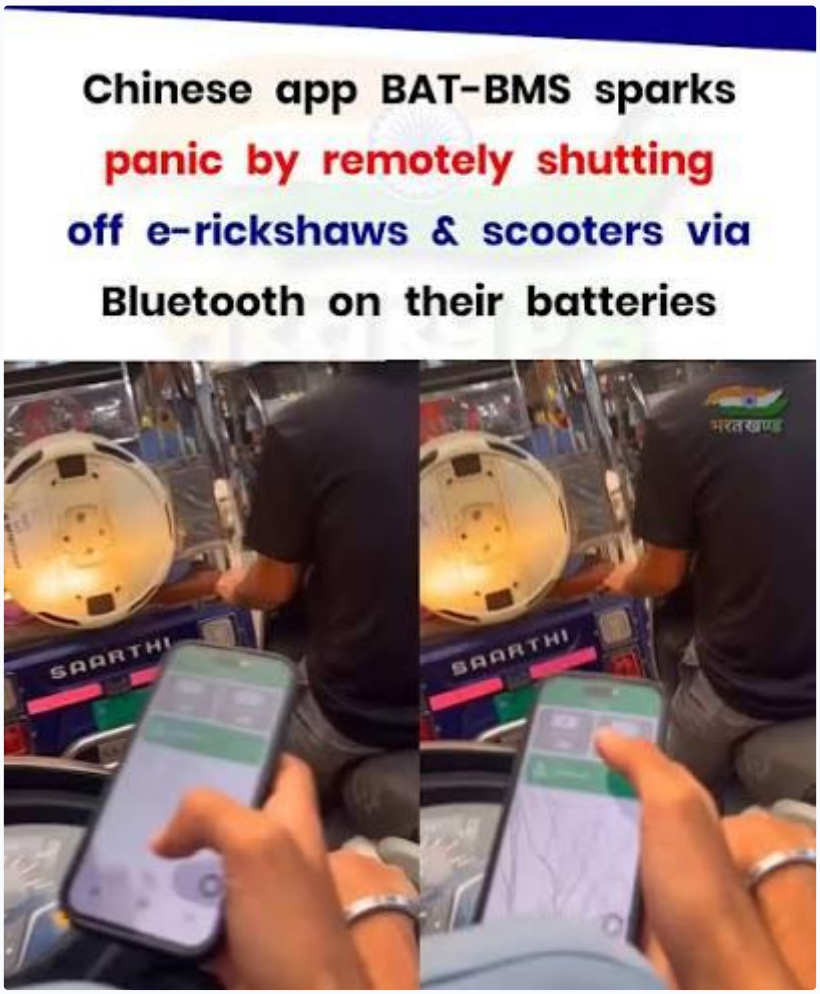

Figure 2: Real-world field reports highlighting moving e-rickshaws disabled via unauthenticated BAT-BMS application commands.

3. Ecosystem Impact & Kinetic Hazards

The massive proliferation of unregulated component assemblies amplifies the operational risk within the Indian market [cite: 364, 365]. This exposure introduces multi-dimensional safety and financial hazards:

- **Severe Kinetic Dangers:** Sudden power dropouts while navigating dense, mixed-speed urban traffic lanes lead to a high probability of rear-end collisions, dangerous vehicle rollbacks on inclines, and loss of control [cite: 370, 371, 372, 374].
- **Economic Destabilization:** Commercial e-rickshaw drivers lose vital operational hours troubleshooting electrical anomalies, endure false repair costs, and face localized extortion rings [cite: 375, 378, 379, 380].
- **Secondary Exploitation Risks:** This vulnerability facilitates secondary criminal operations, including vehicle theft enablement, competitor fleet sabotage, and organized transport infrastructure disruption [cite: 381, 382, 383, 384].

4. Strategic Recommendations & Mitigations

Securing the EV battery footprint demands an immediate, multi-tiered approach combining physical overrides for field operations and cryptographic firmware standards for long-term production [cite: 387].

STAKEHOLDER	ACTION REQUIRED	TIMELINE
Drivers & Fleet Operators	**IMPLEMENT** immediate hardware disconnection of the BLE module or update configurations to replace default PINs [cite: 389, 537].	Immediate (1–2 Days) [cite: 537]
Battery Assemblers	**AUDIT** existing inventory, replace factory default settings, and provide secured firmware upgrades to historical procurement clients [cite: 497, 499, 537].	1–2 Weeks [cite: 537]
BMS Manufacturers	**ENFORCE** mandatory password configurations on first boot and disable public BLE advertising profiles by default [cite: 470, 472, 479, 537].	2–4 Weeks [cite: 537]
Regulatory Agencies	**AMEND** AIS-156 and BIS testing standards to mandate type-approval wireless authentication and encryption audits [cite: 486, 491, 493, 537].	3–6 Months [cite: 537]

4.1 Field Fix: Step-by-Step Hardware Isolation

For vehicles actively targeted where firmware upgrades are unavailable, physical isolation of the BLE radio completely eliminates the attack surface while preserving full cell balancing safety [cite: 389, 390]:

1. **Isolate Power:** Turn OFF the battery's mechanical breaker and disconnect high-voltage terminals [cite: 392]. Allow 5 minutes for capacitor drainage [cite: 392].
2. **Expose Assembly:** Unbolt the protective sheet metal cover plate from the battery pack housing [cite: 396].
3. **Locate Module:** Identify the small independent green secondary circuit card (approx. 3cm x 2cm, marked `JBD B159` or `BLE001`) adjacent to the main silver rectangular BMS unit [cite: 413, 416].
4. **Sever Interconnect:** Disconnect the 4-wire low-voltage UART data line bridging the BLE card to the main controller by pulling the white plastic connector plug straight upward [cite: 419, 420, 426]. Remove the breakout card [cite: 428].
5. **Insulate and Reassemble:** Cover the empty data port terminal with high-quality electrical tape, secure all wiring inside the enclosure templates, rebolt the cover to preserve the IP environmental rating, and power on the vehicle [cite: 434, 439, 440, 441, 442].

5. Affected Supply Chain Components

ASSET TYPE	SUPPLIER / MODEL DETAILS	AFFECTED VERSIONS / STATUS
BMS Platform	JBD / Jiabaida Platforms [cite: 509]	All BLE-enabled variants [cite: 509]
BLE Module Hardware	JBD B159 / BLE001 V1.2 [cite: 509]	All 4-pin UART configurations [cite: 509]
Battery Packs	CAPL (51.2V, 106Ah, 5.4kWh units) [cite: 401, 509]	All factory-default configurations [cite: 509]
Diagnostic Applications	BAT-BMS, XiaoXiangElectric, LOSSIGY [cite: 509]	All accessible mobile versions [cite: 509]