ktauchathuranga / CVE-2025-70994 Public

Code Actions Security and quality Insights

main 1 Branch 0 Tags Go to file Go to file Code

ktauchathuranga cisa bfe9c0b · 3 days ago

| | | |
|---|---|---|
| .github | funds | 2 months ago |
| poc_analyzer | poc updated | 3 weeks ago |
| .gitignore | poc updated | 3 weeks ago |
| LICENSE | Create LICENSE | 2 months ago |
| README.md | cisa | 3 days ago |

README MIT license

# CVE-2025-70994: Weak Authentication in Yadea T5 Electric Bicycle

License MIT CVE 2025-70994 CVSS v3.1 7.3 High

> ⚠ Warning
>
> This repository is published strictly for educational and academic security research purposes. The information and proof-of-concept code provided here are intended to demonstrate a known cryptographic flaw (CWE-1390) to assist vehicle owners and manufacturers in understanding and improving physical security.
>
> The author does not condone, encourage, or support unauthorized access to vehicles or any illegal activities. The proof-of-concept code is strictly a **passive signal analyzer** and contains no transmission or exploitation capabilities. Users are solely responsible for complying with all applicable local, state, and federal laws. Unauthorized interception of RF signals may be illegal in your jurisdiction.

## Executive Summary

A high-risk security vulnerability has been identified in the keyless entry system of the Yadea T5 Electric Bicycle (models manufactured in/after 2024). The system utilizes the EV1527 fixed-code RF protocol over the 433.92 MHz ISM band without implementing rolling codes or cryptographic challenge-response mechanisms.

Because the 20-bit vehicle address is static and decoupled from command authorization, an attacker within proximity can intercept a non-sensitive command (e.g., ringing the vehicle's bell) and mathematically synthesize a high-sensitivity command (e.g., "Start/Ignition"). This allows for complete unauthorized vehicle operation via a replay attack.

| Field | Details |
|---|---|
| **Target Platform** | Yadea T5 Electric Bicycle (manufactured 2024+) |
| **Vulnerability Type** | Weak Authentication (CWE-1390) |
| **Protocol** | EV1527 Fixed-Code (433.92 MHz ASK/OOK) |
| **Impact** | Escalation of Privileges / Unauthorized Vehicle Access |
| **Patch Status** | No global fix available from vendor |
| **Disclosure Status** | Coordinated Public Release (April 23, 2026) in partnership with the U.S. Department of Homeland Security (CISA) and CERT/CC |

| Field | Details |
|---|---|
| **CVSS v3.1 Base Score** | **7.3 (High)** |
| **CVSS v3.1 Vector** | `AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H/E:P/RL:U/RC:C` |

---

## Technical Breakdown

### Protocol Architecture (EV1527)

The system relies on an EV1527-compatible RF encoder. Each transmission consists of a 24-bit data payload transmitted via On-Off Keying (OOK) Pulse Width Modulation.

**Frame Structure:**

1. **Sync Pulse:** ~11.2ms duration (1 high, 31 low periods)
2. **24-bit Payload:**
   - **[Bits 23-4] Address/ID:** A fixed 20-bit identifier unique to the specific remote.
   - **[Bits 3-0] Command:** A 4-bit instruction (e.g., Lock, Unlock, Start, Bell).

### The Authentication Flaw

The core vulnerability stems from the lack of sequential counters (rolling codes). The vehicle's receiver authenticates commands solely by verifying the 20-bit Address.

Because this address never changes, capturing *any* legitimate signal exposes the static key. An attacker can record the signal, extract the 20-bit ID, append the standardized hex code for "Start" ( `0x2` ), and broadcast the synthesized 24-bit frame. The vehicle will accept the forged command as legitimate.

**Standard Command Mappings:**

| Hex | Binary | Function |
|---|---|---|
| `0x1` | 0001 | Bell / Locate |
| `0x2` | 0010 | Start / Ignition |
| `0x4` | 0100 | Unlock |
| `0x8` | 1000 | Lock |

---

## Mitigation & Countermeasures

### For Vehicle Owners

The electronic lock is fundamentally compromised by this protocol flaw. Owners of the Yadea T5 are strongly advised to:

1. Disregard the electronic keyless entry system for security purposes.
2. Utilize heavy-duty physical locking mechanisms (e.g., U-locks, hardened chains) anchored to immovable objects.
3. Utilize the mechanical steering lock.

### For Manufacturers

1. Deprecate the use of EV1527, PT2262, and related fixed-code ICs for security-critical applications.
2. Transition to cryptographic rolling-code implementations (e.g., AES-128, KeeLoq).

---

## Proof of Concept: Signal Analyzer

The provided `poc_analyzer.cpp` is a stripped-down Arduino script designed for the ESP8266 and CC1101 transceiver. It demonstrates the vulnerability by passively listening to the 433.92 MHz band, identifying the EV1527 sync pulse, and decoding the 24-bit frame into plaintext, effectively exposing the static vehicle ID.

**Hardware Requirements:**

- ESP8266 (NodeMCU/Wemos D1)
- CC1101 RF Transceiver Module (SPI Interface)

---

## Disclosure Timeline

A standard 90-day responsible disclosure window was initiated on December 31, 2025. Following a lack of substantive vendor remediation, coordination was established with the U.S. Department of Homeland Security (CISA). The embargo was ultimately extended to April 23, 2026, to allow for a synchronized federal security advisory.

| Date | Event |
|---|---|
| 2025-12-31 | Initial vulnerability disclosure sent to vendor |
| 2026-02-24 | MITRE assigned tracking ID CVE-2025-70994 |
| 2026-03-03 | Formal coordination requested via US CERT/CC (VINCE) |
| 2026-03-31 | U.S. CISA initiates coordination; embargo formally extended for joint federal advisory |
| 2026-04-23 | Coordinated Public Release alongside CISA |

▶ **Click to expand the Full Communication Log**

---

## References

- CISA ICS Advisory: ICSA-26-113-01
- CWE-1390: Weak Authentication
- EV1527 Datasheet
- CVSS v3.1 Calculator
- CVE-2025-70994 on MITRE

---

## Author

**Sponsor this project**

 **ktauchathuranga** Ashen Chathuranga

Sponsor

Learn more about GitHub Sponsors

**Contributors** 1

 **ktauchathuranga** Ashen Chathuranga

**Languages**

- **C++** 100.0%