CVE-2026-112345: Insecure Cryptographic Key-Sharing Protocol in TTLock Bluetooth Pairing

Published 23 octobre 2026 CVSS 8.6 TTLock TTLock

< 9.8.260718

Executive summary

The TTLock Bluetooth pairing protocol uses a hardcoded static AES key (defaultKey) to encrypt the transmission of the session key (aesKeyStr), allowing an attacker within Bluetooth range to recover it and forge legitimate requests to the lock.

Description

TTLock's proprietary Bluetooth protocol uses, during pairing, a static AES key (defaultKey) hardcoded in the app and the firmware to protect the exchange of the session key (aesKeyStr):

Attack vectors

- **Network access:** Adjacent (Bluetooth)
- **Authentication required:** None
- **User interaction:** None

Vulnerability Details

defaultKey is identical across the entire device fleet and recoverable through reverse engineering of the app or firmware. An attacker passively capturing the pairing exchange can decrypt the lock's response with defaultKey and obtain aesKeyString plaintext. This key is **permanent**: it is never rotated for the lifetime of the pairing, making the compromise persistent.

Proof of Concept (PoC)

- Extract defaultKey via static reverse engineering of the app/firmware.
- Passively capture the two BLE frames of the pairing exchange.
- Decrypt the response with defaultKey → obtain aesKeyStr.
- Forge BLE requests encrypted with aesKeyStr (unlocking, adding fingerprint, adding access code).

Risk and Impact

- Unauthorized physical access (unlocking).
- Unauthorized creation of access credentials.
- Full and persistent administrative takeover.
- Structural flaw exploitable against any device of the same model.

Author

- Yassine Damiri

© 2023 Yassine Damiri. All Rights Reserved.
