Security Advisory

NXP Semiconductor Disclosure

Classification: External
January 20, 2026

Announcement

A disclosure regarding NXP Semiconductors was published January 20, 2026, that identifies a vulnerability for non-diversified and non-locked keys on MIFARE Ultralight® C and MIFARE Ultralight® AES products when not properly configured.

The publication, titled "BREAKMEIFYOUCAN!" Exploiting Keyspace Reduction and Relay Attacks in Ultralight C (MF0ICU2), Ultralight AES (MF0AES), and Common Counterfeits," informs about the possibility to retrieve the 112-bit DES, or 128-bit AES key of the user memory, if not diversified and/or locked.

dormakaba customers are not impacted by this NXP security disclosure and no further action is needed as dormakaba solutions already follow best practices such as:

- **Key diversification**
  dormakaba's implementation, in both legacy *Standard Security* and best practice *Enhanced Security* modes, always uses a unique authentication key per Integrated Circuit (IC).

- **CMAC-based secure messaging**
  For Ultralight AES, dormakaba also employs Cipher-based Message Authentication Code (CMAC)-based secure messaging, which further mitigates this attack vector.

Additional Resources

Email: securitysupport@dormakaba.com
Phone: 1-844-461-2249

Note: The hours of operation for the Security Support hotline are Monday-Friday, 8:30am - 7:00pm ET.