Xylem Product Security Advisory

Disclosure of Sensus wM-Bus Default Encryption Key

11/20/2024

Overview

Xylem is aware of a public discussion describing the default encryption key, and method to decrypt Wireless M-bus meter messages transmitted by select Sensus products, which may allow select Sensus products to be read, but NOT modified when in close proximity, using appropriate telecommunication equipment.

This advisory is to communicate to customers Xylem's recommendation to change the encryption key on affected products to prevent unauthorized reading of meters.

Affected Products and Versions

This security advisory applies ONLY to the products listed below and installations ONLY in the following countries and markets.

It is NOT possible to communicate with the meter, tamper, manipulate or change in any form the meter's performance.

This security advisory does NOT concern products with Wireless M-Bus radio which have been configured with individual or customer (utility) specific encryption keys.

Products NOT listed are not impacted. Products installed in countries NOT listed are not impacted.

Locations and products potentially affected are:

Countries

Chile, Colombia, Czechia, Denmark, France and overseas territories, Greece, Italy, New Zealand, Poland, Slovakia, Slovenia, South Africa, Switzerland, Ukraine.

Products

- iPERL water meters, sold since 2014
- 640 water meters, sold since 2016
- MeistreamRF water meters, sold since 2016
- MeiTwinRF water meters, sold since 2016
- PulseRF radio transciever units, sold between 06/2015 and 03/2018

Vulnerability Details

CWE-1394: Use of Default Cryptographic Key

CVSS v3.1 Base Score 4.3 | Medium | AV:A/AC:L/PR:N/UI:N/S:U/C:L*/I:N**/A:N***

A *CWE-1394: Use of Default Cryptographic Key* vulnerability exists that could allow an unauthorized actor to access meter consumption and meter location data.

*Confidentiality – Low impact

**Integrity – No impact

***Availability – No impact

Mitigations

To mitigate the risk of an unauthorized actor gaining access to message transmissions of existing affected products via the use of the exposed default encryption key Xylem recommends taking either one of the following actions:

- Change all affected products from the default key to an individual key per meter.
  -OR -
- Change all affected products from the default key to a customer unique key.

Detailed instructions for implementing Individual key per meter can be found by emailing encryption.keys@xylem.com and using the Subject "Individual Key"

Detailed instructions for implementing the customer unique key can be found by emailing encryption.keys@xylem.com and using the Subject "Customer Unique Key"

Contact Information

For additional information regarding how to implement the recommended mitigations, please contact encryption.keys@xylem.com. One of our support team will be able to provide you with guidance and tools to make this change.

For any questions related to this Xylem Product Security Advisory, please contact product.security@xylem.com.

Revision History	
Version	**Updates**
1.0	Published Advisory

Disclaimer

This document is provided on an as-is basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Use of the information in this document or materials linked from this document is at your own risk. Xylem reserves the right to change or update this document at any time.