

Avviso sulla sicurezza dei prodotti Xylem

Divulgazione della chiave di crittografia predefinita Sensus wM-Bus

11/20/2024

Panoramica

Xylem è a conoscenza di una discussione pubblica che descrive la chiave di crittografia predefinita e il metodo per decrittografare i messaggi dei contatori Wireless M-bus che vengono trasmessi da prodotti Sensus selezionati. Questo potrebbe consentire la lettura da prossimità di prodotti Sensus selezionati, ma NON la modifica, grazie all'utilizzo di apparecchiature di telecomunicazione appropriate.

Questo avviso ha lo scopo di comunicare ai clienti la raccomandazione da parte di Xylem di modificare la chiave di crittografia sui prodotti interessati per impedire la lettura non autorizzata dei contatori.

Prodotti e versioni interessati

Questo avviso di sicurezza si applica SOLO ai prodotti elencati di seguito e SOLO alle installazioni nei seguenti Paesi e mercati.

NON è possibile comunicare con il contatore, manometterne, manipolarne o modificarne le prestazioni.

Questo avviso di sicurezza NON riguarda i prodotti con radio Wireless M-Bus che sono stati configurati con chiavi di crittografia individuali o specifiche del cliente (utenza).

I prodotti NON elencati non sono interessati. I prodotti installati in paesi NON elencati non sono interessati.

I Paesi e i prodotti potenzialmente interessati sono:

Paesi

Cile, Colombia, Repubblica Ceca, Danimarca, Francia e territori oltreoceano, Grecia, Italia, Nuova Zelanda, Polonia, Slovacchia, Slovenia, Sudafrica, Svizzera, Ucraina.

Prodotti

- Contatori d'acqua iPERL venduti dal 2014
- Contatori d'acqua 640 venduti dal 2016
- Contatori d'acqua MeiStreamRF venduti dal 2016
- Contatori d'acqua MeiTwinRF venduti dal 2016
- Unità ricetrasmittitore radio PulseRF vendute tra giugno 2015 e marzo 2018

Dettagli vulnerabilità

CWE-1394: Utilizzo della chiave di crittografia predefinita

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

Esiste una vulnerabilità che potrebbe consentire a un soggetto non autorizzato di accedere ai dati relativi al consumo e alla posizione del contatore.

*Riservatezza – Basso impatto

**Integrità – Nessun impatto

***Disponibilità – Nessun impatto

Mitigazioni

Per mitigare il rischio che un soggetto non autorizzato acceda ai messaggi trasmessi dai prodotti interessati tramite l'uso della chiave di crittografia, Xylem consiglia di intraprendere una delle seguenti azioni:

- Passare da chiave predefinita a chiave individuale per contatore in tutti i prodotti interessati.
-OR -
- Passare da chiave predefinita a chiave univoca del cliente in tutti i prodotti interessati.

Istruzioni dettagliate per l'implementazione della chiave individuale per contatore sono disponibili inviando un'e-mail all'indirizzo encryption.keys@xylem.com e utilizzando l'oggetto "Individual Key"

Istruzioni dettagliate per l'implementazione della chiave univoca del cliente sono disponibili inviando un'e-mail a encryption.keys@xylem.com e utilizzando l'oggetto "Customer Unique Key"

Contatti

Per ulteriori informazioni su come implementare le mitigazioni consigliate, contattare encryption.keys@xylem.com. Il nostro team di supporto sarà in grado di fornirvi indicazioni e strumenti per apportare questo cambiamento.

Per qualsiasi domanda relativa a questo Avviso sulla sicurezza dei prodotti Xylem, contattare product.security@xylem.com.

Revisioni	
Versione	Aggiornamenti
1,0	Avviso pubblicato

Disclaimer

Il presente documento è fornito così com'è e non implica alcun tipo di garanzia, incluse le garanzie di commerciabilità o idoneità per un uso particolare. L'utilizzo delle informazioni contenute in questo documento o dei materiali collegati a questo documento è a rischio dell'utente. Xylem si riserva il diritto di modificare o aggiornare il presente documento in qualsiasi momento.