

## Xylems produktsikkerhedsvejledning

### Videregivelse af Sensus wM-Bus-standardkrypteringsnøgle

11/20/2024

#### Oversigt

Xylem er opmærksom på en offentlig diskussion, der beskriver standardkrypteringsnøglen og metoden til at dekryptere trådløse M-bus-målermeddelelser, der overføres af udvalgte Sensus-produkter, hvilket kan gøre det muligt at læse udvalgte Sensus-produkter, men IKKE ændre dem, når de er tæt på, ved hjælp af passende telekommunikationsudstyr.

Denne rådgivning skal kommunikere til kunderne Xylems anbefaling om at ændre krypteringsnøglen på berørte produkter for at forhindre uautoriseret læsning af målere.

#### Påvirkede produkter og versioner

Denne sikkerhedsrådgivning gælder KUN for de produkter, der er anført nedenfor, og installationer KUN i de følgende lande og markeder.

Det er IKKE muligt at kommunikere med måleren, manipulere, manipulere eller ændre målerens ydelse i nogen form.

Denne sikkerhedsadvisering vedrører IKKE produkter med Wireless M-Bus-radio, som er konfigureret med specifikke krypteringsnøgler til enkeltpersoner eller kunder (brug).

Produkter, der IKKE er anført, påvirkes ikke. Produkter, der er installeret i lande, der IKKE er anført, påvirkes ikke.

Placeringer og produkter, der potentielt kan påvirkes, er:

#### Lande

Chile, Colombia, Tjekkiet, Danmark, Frankrig og oversøiske territorier, Grækenland, Italien, New Zealand, Polen, Slovakiet, Slovenien, Sydafrika, Schweiz, Ukraine.

#### Produkter

- iPERL-vandmålere, solgt siden 2014
- 640 vandmålere, solgt siden 2016
- MeistreamRF-vandmålere, solgt siden 2016
- MeiTwinRF-vandmålere, solgt siden 2016
- PulseRF radiotranscieverenheder, solgt mellem 06/2015 og 03/2018

## Sårbarhedsoplysninger

### CWE-1394: Brug af standard Cryptographic nøgle

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

A *CWE-1394: Brug af standard Cryptographic-nøglesårbarhed*, der kan give en uautoriseret skuespiller adgang til målerforbrug og målerplaceringsdata.

\*Fortrolighed – Lav effekt

\*\*Integritet – Ingen påvirkning

\*\*\*Tilgængelighed – Ingen påvirkning

## Begrænsninger

For at mindske risikoen for, at en uautoriseret aktør får adgang til meddelelsestransmissioner af eksisterende berørte produkter via brugen af den eksponerede standardkrypteringsnøgle, anbefaler Xylem, at der foretages en af følgende handlinger:

- Ændr alle berørte produkter fra standardnøglen til en individuel nøgle pr. måler.  
-OR -
- Ændr alle berørte produkter fra standardnøglen til en unik kundenøgle.

Detaljerede instruktioner til implementering af Individuel nøgle pr. måler kan findes ved at sende en e-mail til [encryption.keys@xylem.com](mailto:encryption.keys@xylem.com) og bruge Emnet "Individuel nøgle"

Detaljerede instruktioner til implementering af kundens unikke nøgle kan findes ved at sende en e-mail til [encryption.keys@xylem.com](mailto:encryption.keys@xylem.com) og bruge Emnet "Kunde unik nøgle"

## Kontaktoplysninger

For yderligere oplysninger om, hvordan de anbefalede afhjælpninger implementeres, bedes du kontakte [encryption.keys@xylem.com](mailto:encryption.keys@xylem.com). Et af vores supportteam vil kunne give dig vejledning og værktøjer til at foretage denne ændring.

Hvis du har spørgsmål vedrørende denne Xylem Product Security Advisory, bedes du kontakte [product.security@xylem.com](mailto:product.security@xylem.com).

Revisionshistorik	
Version	Opdateringer
1,0	Offentliggjort rådgivning

## Ansvarsfraskrivelse

Dette dokument leveres som det er og forefindes og indebærer ikke nogen form for garanti, herunder garantier for salgbarhed eller egnethed til en bestemt brug. Brug af oplysningerne i dette dokument eller materialer, der er linket fra dette dokument, er på egen risiko. Xylem forbeholder sig retten til at ændre eller opdatere dette dokument til enhver tid.