

## Xylem-Produktsicherheitshinweis

### Offenlegung des Sensus wM-Bus-Standardverschlüsselungsschlüssels

11/20/2024

#### Überblick

Xylem ist sich einer öffentlichen Diskussion bewusst, in der der Standardverschlüsselungsschlüssel und die Methode zur Entschlüsselung von drahtlosen M-Bus-Messgeräten beschrieben werden, die von ausgewählten Sensus-Produkten übertragen werden. Dadurch können ausgewählte Sensus-Produkte unter Verwendung geeigneter Telekommunikationsgeräte gelesen, aber NICHT geändert werden, wenn sie sich in unmittelbarer Nähe befinden.

Dieser Hinweis soll den Kunden die Empfehlung von Xylem zur Änderung des Verschlüsselungsschlüssels für betroffene Produkte mitteilen, um das unbefugte Lesen von Zählern zu verhindern.

#### Betroffene Produkte und Versionen

Dieser Sicherheitshinweis gilt NUR für die unten aufgeführten Produkte und Installationen in den folgenden Ländern und Märkten.

Es ist NICHT möglich, mit dem Messgerät zu kommunizieren, die Leistung des Messgeräts zu manipulieren, zu manipulieren oder zu ändern.

Dieser Sicherheitshinweis bezieht sich NICHT auf Produkte mit drahtlosem M-Bus-Funk, die mit individuellen oder kundenspezifischen Verschlüsselungsschlüsseln (Dienstprogramm) konfiguriert wurden.

NICHT aufgeführte Produkte sind nicht betroffen. Produkte, die in NICHT aufgeführten Ländern installiert sind, sind nicht betroffen.

Die potenziell betroffenen Standorte und Produkte sind:

#### Länder

Chile, Kolumbien, Tschechien, Dänemark, Frankreich und Überseegebiete, Griechenland, Italien, Neuseeland, Polen, Slowakei, Slowenien, Südafrika, Schweiz, Ukraine.

#### Produkte

- iPERL Wasserzähler, verkauft seit 2014
- 640 Wasserzähler, verkauft seit 2016
- MeistreamRF Wasserzähler, verkauft seit 2016
- MeiTwinRF Wasserzähler, verkauft seit 2016
- PulseRF Funktransziever-Einheiten, verkauft zwischen 06/2015 und 03/2018

## Schwachstellendetails

### CWE-1394: Verwendung des standardmäßigen kryptographischen Schlüssels

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

A *CWE-1394*: Es besteht eine standardmäßige Kryptographieschlüssel-Schwachstelle, die es einem unbefugten Akteur ermöglichen könnte, auf Zählerverbrauch und Zählerstandortdaten zuzugreifen.

\*Vertraulichkeit – Geringe Auswirkungen

\*\*Integrität – Keine Auswirkungen

\*\*\*Verfügbarkeit – Keine Auswirkungen

## Minderung

Um das Risiko zu mindern, dass ein unbefugter Akteur über den veröffentlichten Standardverschlüsselungsschlüssel Zugriff auf Nachrichtenübertragungen von bestehenden betroffenen Produkten erhält, empfiehlt Xylem, eine der folgenden Maßnahmen zu ergreifen:

- Ändern Sie alle betroffenen Produkte von der Standardtaste auf eine einzelne Taste pro Meter.  
-ODER -
- Ändern Sie alle betroffenen Produkte vom Standardschlüssel in einen eindeutigen Kundenschlüssel.

Detaillierte Anweisungen zur Implementierung des individuellen Schlüssels pro Meter erhalten Sie per E-Mail an [encryption.keys@xylem.com](mailto:encryption.keys@xylem.com) und unter Verwendung des Betreffs „Individueller Schlüssel“

Detaillierte Anweisungen zur Implementierung des eindeutigen Kundenschlüssels erhalten Sie per E-Mail an [encryption.keys@xylem.com](mailto:encryption.keys@xylem.com) und über den Betreff „Eindeutiger Kundenschlüssel“.

## Kontaktinformationen

Für weitere Informationen zur Implementierung der empfohlenen Maßnahmen wenden Sie sich bitte an [encryption.keys@xylem.com](mailto:encryption.keys@xylem.com). Einer unserer Support-Teams wird Ihnen Anleitung und Tools zur Verfügung stellen, um diese Änderung vorzunehmen.

Bei Fragen zu diesem Xylem-Produktsicherheitshinweis wenden Sie sich bitte an [product.security@xylem.com](mailto:product.security@xylem.com).

Änderungshistorie	
Version	Updates

## Haftungsausschluss

Dieses Dokument wird im Ist-Zustand zur Verfügung gestellt und beinhaltet keine Garantie oder Gewährleistung, einschließlich der Gewährleistung der Marktgängigkeit oder Eignung für eine bestimmte Verwendung. Die Verwendung der Informationen in diesem Dokument oder der mit diesem Dokument verknüpften Materialien erfolgt auf eigenes Risiko. Xylem behält sich das Recht vor, dieses Dokument jederzeit zu ändern oder zu aktualisieren.