

Aviso de seguridad de productos Xylem

Divulgación de la llave de cifrado predeterminada de Sensus wM-Bus

11/20/2024

Descripción general

Xylem está al tanto que en un foro público se ha divulgado la llave de cifrado predeterminada y el método usado para descifrar los mensajes transmitidos por ciertos productos de Sensus bajo el protocolo Wireless M-Bus (WM-bus). Esto podría permitir que estos productos sean leídos, pero NO modificados, cuando se encuentren cerca a los productos, utilizando el equipo de telecomunicaciones adecuado.

Este aviso tiene como objetivo comunicar a los clientes la recomendación de Xylem de cambiar la llave de cifrado en los productos afectados para evitar la lectura no autorizada de los medidores.

Productos y versiones afectados

Este aviso de seguridad aplica UNICAMENTE a los productos listados a continuación y SOLO a los productos instalados en los siguientes países y mercados.

No es posible comunicarse con el medidor, manipularlo, modificarlo ni alterar su rendimiento de ninguna forma.

Este aviso de seguridad NO afecta a los productos con radio Wireless M-Bus (WM-bus) que se hayan configurado con llaves de cifrado individuales o específicas para cliente (servicios públicos).

Los productos NO listados no se ven afectados. Los productos instalados en países NO listados no se ven afectados.

Las ubicaciones y los productos potencialmente afectados son:

Países

Chile, Colombia, República Checa, Dinamarca, Francia y territorios de ultramar, Grecia, Italia, Nueva Zelanda, Polonia, Eslovaquia, Eslovenia, Sudáfrica, Suiza y Ucrania.

Productos

- Medidores de agua iPERL, vendidos desde 2014
- Medidores de Agua 640, vendidos desde 2016
- Medidores de agua MeistreamRF, vendidos desde 2016
- Medidores de agua MeiTwinRF, vendidos desde 2016
- Unidades transceptoras de radio PulseRF, vendidas entre 06/2015 y 03/2018

Detalles de la vulnerabilidad

CWE-1394: Uso de la llave criptográfica predeterminada

Puntaje base de CVSS v3.1 4,3 | Medio | AV:A/AC:L/PR:N/UI:N/S:U/C:L*/I:N**/A:N***

Existe una vulnerabilidad del *CWE-1394: Uso de la llave criptográfica predeterminada* que podría permitir a un actor no autorizado acceder a los datos de consumo del medidor y a los datos de la ubicación del medidor.

*Confidencialidad: bajo impacto

**Integridad: sin impacto

***Disponibilidad: sin impacto

Mitigaciones

Para mitigar el riesgo de que un actor no autorizado obtenga acceso a las transmisiones de mensajes de los productos afectados existentes mediante el uso de la llave de cifrado predeterminada expuesta, Xylem recomienda tomar una de las siguientes medidas:

- Cambie la llave predeterminada a una llave individual por medidor en todos los productos afectados.
-O -
- Cambie la llave predeterminada a una llave única por cliente en todos los productos afectados.

Puede solicitar instrucciones detalladas para implementar el cambio a llaves individuales por medidor enviando un correo electrónico a encryption.keys@xylem.com con el Asunto "Individual Key"

Puede solicitar instrucciones detalladas para implementar el cambio a llave única del cliente enviando un correo electrónico a encryption.keys@xylem.com con el Asunto "Customer Unique Key"

Información de contacto

Para obtener más información sobre cómo implementar las mitigaciones recomendadas, por favor contacte a encryption.keys@xylem.com. Uno de nuestros miembros del equipo de soporte podrá proporcionarle orientación y herramientas para realizar este cambio.

Para cualquier consulta relacionada con este Aviso de seguridad de productos de Xylem, comuníquese con product.security@xylem.com.

Historial de revisiones	
Versión	Actualizaciones
1,0	Asesoramiento publicado

Descargo de responsabilidad

Este documento se proporciona tal cual, y no implica ningún tipo de garantía, incluyendo las garantías de comerciabilidad o idoneidad para un uso particular. El uso de la información contenida en este documento o de los materiales vinculados a este documento es bajo su propio riesgo. Xylem se reserva el derecho de cambiar o actualizar este documento en cualquier momento.