Conseil de Sécurité Produit Xylem

Divulgation de la clé de chiffrement par défaut Sensus wM-Bus

11/20/2024

Vue générale

Xylem a pris connaissance d'une discussion publique décrivant la clé de chiffrement par défaut et la méthode de déchiffrement des messages des compteurs M-Bus sans fil transmis par certains produits Sensus, qui peut permettre de lire certains produits Sensus, mais PAS de les modifier à proximité immédiate, en utilisant un équipement de télécommunication approprié.

Ce conseil a pour but de communiquer aux clients la recommandation de Xylem de modifier la clé de chiffrement des produits concernés pour empêcher la lecture non autorisée des compteurs.

Produits et versions concernés

Ce conseil de sécurité s'applique UNIQUEMENT aux produits énumérés ci-dessous et aux installations UNIQUEMENT dans les pays et marchés suivants.

Il n'est PAS possible de communiquer avec le compteur, de le trafiquer, de le manipuler ou de le modifier sous quelque forme que ce soit.

Cet avertissement de sécurité ne concerne PAS les produits avec radio M-Bus sans fil qui ont été configurés avec des clés de chiffrement spécifiques à un client ou à un individu (utilitaire).

Les produits NON listés ne sont pas affectés. Les produits installés dans des pays NON listés ne sont pas concernés.

Les sites et produits potentiellement affectés sont :

Pays

Chili, Colombie, Tchéquie, Danemark, France et territoires d'outre-mer, Grèce, Italie, Nouvelle-Zélande, Pologne, Slovaquie, Slovénie, Afrique du Sud, Suisse, Ukraine.

Produits

- Compteurs d'eau iPERL, vendus depuis 2014
- 640 compteurs d'eau, vendus depuis 2016
- Compteurs d'eau MeistreamRF, vendus depuis 2016
- Compteurs d'eau MeiTwinRF, vendus depuis 2016
- Unités d'émetteur-récepteur radio PulseRF, vendues entre le 06/2015 et le 03/2018

Détails de vulnérabilité

CWE-1394: utilisation de la clé cryptographique par défaut

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

Un *CWE-1394: utilisation de* la vulnérabilité de la clé cryptographique par défaut qui pourrait permettre à un acteur non autorisé d'accéder à la consommation du compteur et aux données de localisation du compteur.

*Confidentialité – Faible impact

**Intégrité – Aucun impact

***Disponibilité – Aucun impact

Atténuations

Pour atténuer le risque qu'un acteur non autorisé accède aux transmissions de messages des produits concernés par l'utilisation de la clé de chiffrement par défaut exposée, Xylem recommande de prendre l'une ou l'autre des mesures suivantes :

- Changer tous les produits concernés de la clé par défaut à une clé individuelle par compteur .
  -OU -
- Changer tous les produits concernés de la clé par défaut à une clé unique au client.

Des instructions détaillées pour la mise en œuvre de la clé individuelle par compteur sont disponibles en envoyant un e-mail à encryption.keys@xylem.com et en utilisant l'objet « Clé individuelle »

Des instructions détaillées pour la mise en œuvre de la clé unique au client sont disponibles en envoyant un e-mail à encryption.keys@xylem.com et en utilisant l'objet « Clé unique au client »

Coordonnées

Pour plus d'informations sur la mise en œuvre des mesures d'atténuation recommandées, veuillez contacter encryption.keys@xylem.com. Notre équipe sera en mesure de vous fournir des conseils et des outils pour effectuer ce changement.

Pour toute question concernant ce Conseil de Sécurité Produit Xylem, veuillez contacter product.security@xylem.com.

Historique des révisions	
Version	Mises à jour
1,0	Avis publié

Clause de non-responsabilité

Ce document est fourni en l'état et n'implique aucune garantie, y compris les garanties de commercialisation ou d'adéquation à un usage particulier. L'utilisation des informations contenues dans ce document ou des documents liés à partir de ce document se fait à vos propres risques. Xylem se réserve le droit de modifier ou de mettre à jour ce document à tout moment.