Poradenstvo spoločnosti Xylem v oblasti bezpečnosti výrobkov

Zverejnenie Sensus wM-Bus Predvolený šifrovací kľúč

11/20/2024

Prehľad

Spoločnosť Xylem vie o verejnej diskusii opisujúcej predvolený šifrovací kľúč a spôsob dešifrovania správ bezdrôtového merača M-bus prenášaných vybranými produktmi Sensus, čo môže umožniť, aby boli vybrané produkty Sensus prečítané, ale NEUPRAVENÉ, keď sú v tesnej blízkosti, pomocou vhodného telekomunikačného zariadenia.

Táto rada je určená na komunikovanie so zákazníkmi odporúčania spoločnosti Xylem zmeniť šifrovací kľúč na dotknutých výrobkoch, aby sa zabránilo neoprávnenému čítaniu meračov.

Dotknuté produkty a verzie

Toto bezpečnostné poradenstvo sa vzťahuje LEN na produkty uvedené nižšie a inštalácie IBA v nasledujúcich krajinách a trhoch.

Nie je možné komunikovať s glukomerom, manipulovať s ním, manipulovať s ním alebo meniť jeho výkon.

Toto bezpečnostné poradenstvo sa NEVZŤAHUJE na produkty s bezdrôtovým rádiom M-Bus, ktoré boli nakonfigurované s šifrovacími kľúčmi špecifickými pre jednotlivca alebo zákazníka (príslušnosť).

Produkty, ktoré NIE SÚ uvedené v zozname, nie sú ovplyvnené. Produkty nainštalované v krajinách, ktoré NIE sú uvedené v zozname, nie sú ovplyvnené.

Potenciálne ovplyvnené miesta a produkty sú:

Krajiny

Čile, Kolumbia, Česká republika, Dánsko, Francúzsko a zámorské teritóriá, Grécko, Taliansko, Nový Zéland, Poľsko, Slovensko, Slovinsko, Juhoafrická republika, Švajčiarsko, Ukrajina.

Produkty

- Merače vody iPERL, predávané od roku 2014
- 640 metrov vody, predaných od roku 2016
- Merače vody MeistreamRF, predávané od roku 2016
- Merače vody MeiTwinRF, predávané od roku 2016
- Zariadenia PulseRF na rádiový vysielač, predávané od 06/2015 do 03/2018

Podrobnosti o zraniteľnosti

CWE-1394: Použitie predvoleného kryptografického kľúča

CVSS v3.1 Základné skóre 4.3 | Stredné | AV:A/AC:L/PR:N/UI:N/S:U/C:L*/I:N**/A:N***

CWE-1394: Existuje použitie predvolenej zraniteľnosti kryptografickým kľúčom, ktorá by mohla umožniť neoprávnenému aktérovi prístup k spotrebe glukomera a údajom o polohe glukomera.

*Dôvernosť – nízky vplyv

** Bezúhonnosť – bez vplyvu

***Dostupnosť – bez vplyvu

Zmierňujúce opatrenia

Na zmiernenie rizika získania prístupu k prenosom správ existujúcich dotknutých výrobkov neoprávneným aktérom pomocou exponovaného predvoleného šifrovacieho kľúča spoločnosť Xylem odporúča vykonať jednu z nasledujúcich činností:

- Zmeňte všetky dotknuté produkty z predvoleného kľúča na individuálny kľúč na meter.
  -ALEBO -
- Zmeňte všetky dotknuté produkty z predvoleného kľúča na jedinečný kľúč zákazníka.

Podrobné pokyny na implementáciu individuálneho kľúča na meter nájdete e-mailom na adresu encryption.keys@xylem.com a pomocou položky „Individuálny kľúč“ účastníka.

Podrobné pokyny na implementáciu jedinečného kľúča zákazníka nájdete e-mailom na adresu encryption.keys@xylem.com a pomocou predmetu „Jedinečný kľúč zákazníka“

Kontaktné údaje

Ďalšie informácie o tom, ako implementovať odporúčané zmiernenia, získate na adrese encryption.keys@xylem.com. Jeden z našich podporných tímov vám poskytne pokyny a nástroje na vykonanie tejto zmeny.

Ak máte akékoľvek otázky týkajúce sa tohto Poradenstva pre bezpečnosť produktov spoločnosti Xylem, obráťte sa na adresu product.security@xylem.com.

História revízií	
Verzia	**Aktualizácie**
1,0	Publikované poradenstvo

Vylúčenie zodpovednosti

Tento dokument sa poskytuje v aktuálnom stave a neznamená žiadnu záruku ani záruku vrátane záruk obchodovateľnosti alebo vhodnosti na konkrétne použitie. Informácie v tomto dokumente alebo materiály spojené s týmto dokumentom používate na vlastné riziko. Spoločnosť Xylem si vyhradzuje právo kedykoľvek zmeniť alebo aktualizovať tento dokument.