

Poradenství společnosti Xylem pro zabezpečení produktů

Zveřejnění výchozího šifrovacího klíče Sensus wM-Bus

11/20/2024

Přehled

Společnost Xylem si je vědoma veřejné diskuse popisující výchozí šifrovací klíč a metodu dešifrování zpráv bezdrátového M-busmetru přenášených vybranými produkty společnosti Sensus, což může umožnit čtení vybraných produktů společnosti Sensus, ale NENÍ v těsné blízkosti upravována pomocí vhodného telekomunikačního zařízení.

Toto upozornění upozorňuje zákazníky, že společnost Xylem doporučuje změnit šifrovací klíč u dotčených výrobků, aby se zabránilo neoprávněnému odečtu měřičů.

Dotčené produkty a verze

Toto bezpečnostní upozornění se vztahuje POUZE na níže uvedené produkty a instalace POUZE v následujících zemích a na následujících trzích.

NENÍ možné komunikovat s přístrojem, manipulovat s ním, manipulovat s ním nebo měnit výkon přístroje.

Toto bezpečnostní upozornění se NEVZTAHUJE na produkty s bezdrátovým rádiovým zařízením M-Bus, které byly nakonfigurovány s šifrovacími klíči specifickými pro jednotlivce nebo zákazníka (užitečné zařízení).

Výrobky, které NEJSOU uvedeny v seznamu, nejsou ovlivněny. Produkty nainstalované v zemích, které NEJSOU uvedeny v seznamu, nejsou ovlivněny.

Mezi potenciálně ovlivněná místa a produkty patří:

Země

Chile, Kolumbie, Česko, Dánsko, Francie a zámořská území, Řecko, Itálie, Nový Zéland, Polsko, Slovensko, Slovinsko, Jihoafrická republika, Švýcarsko, Ukrajina.

Produkty

- Vodoměry iPERL, prodávané od roku 2014
- 640 vodoměrů, prodává se od roku 2016
- Vodoměry MeistreamRF, prodávané od roku 2016
- Měřiče vody MeiTwinRF, prodávané od roku 2016
- Jednotky rádiových snímačů PulseRF, prodávané mezi 6/2015 a 3/2018

Podrobnosti o zranitelnosti

CWE-1394: Použití výchozího kryptografického klíče

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

CWE-1394: Existuje použití výchozí zranitelnosti kryptografického klíče, které by neoprávněnému činiteli umožnilo přístup k údajům o spotřebě měřidla a poloze měřidla.

*Důvěrnost – nízký dopad

**Integrita – žádný dopad

***Dostupnost – žádný dopad

Zmírnění

Aby se snížilo riziko, že neoprávněný aktér získá přístup k přenosu zpráv stávajících dotčených výrobků pomocí odhaleného výchozího šifrovacího klíče, společnost Xylem doporučuje provést jednu z následujících akcí:

- Změňte všechny dotčené výrobky z výchozího na individuální klíč na metr.
-NEBO -
- Změňte všechny dotčené produkty z výchozího klíče na jedinečný klíč zákazníka.

Podrobné pokyny k implementaci individuálního klíče na metr lze nalézt zasláním e-mailu na adresu encryption.keys@xylem.com a použitím předmětu „Individuální klíč“

Podrobné pokyny k implementaci jedinečného klíče zákazníka naleznete zasláním e-mailu na adresu encryption.keys@xylem.com pomocí předmětu „Jedinečný klíč zákazníka“

Kontaktní informace

Další informace o tom, jak zavést doporučená opatření pro zmírnění následků, získáte na adrese encryption.keys@xylem.com. Jeden z našich podpůrných týmů vám poskytne pokyny a nástroje k provedení této změny.

Máte-li jakékoli dotazy týkající se tohoto bezpečnostního upozornění společnosti Xylem, obraťte se na adresu product.security@xylem.com.

Historie revizí	
Verze	Aktualizace
1,0	Publikované poradenství

Prohlášení o odmítnutí záruk

Tento dokument je poskytován tak, jak je, a neznamená žádný druh záruky nebo záruky, včetně záruk prodejnosti nebo vhodnosti pro konkrétní použití. Použití informací v tomto dokumentu nebo materiálech z tohoto dokumentu je na vaše vlastní riziko. Společnost Xylem si vyhrazuje právo tento dokument kdykoli změnit nebo aktualizovat.