Svetovalec za varnost izdelka Xylem

Razkritje privzetega ključa šifriranja Sensus wM-Bus

11/20/2024

Pregled

Xylem je seznanjen z javno razpravo, ki opisuje privzeti šifrirni ključ in način dešifriranja sporočil merilnika brezžičnega M-busa, ki jih prenašajo izbrani izdelki Sensus, kar lahko omogoči branje izbranih izdelkov Sensus, vendar jih ni mogoče spremeniti, ko so v neposredni bližini, z ustrezno telekomunikacijsko opremo.

S tem svetovanjem lahko strankam sporočite priporočilo družbe Xylem, naj spremenijo šifrirni ključ na zadevnih izdelkih, da preprečijo nepooblaščeno branje merilnikov.

Prizadeti izdelki in različice

To varnostno svetovanje velja SAMO za spodaj navedene izdelke in namestitve SAMO v naslednjih državah in trgih.

Ni mogoče komunicirati z merilnikom, spreminjati, manipulirati ali spreminjati v kakršni koli obliki delovanja merilnika.

To varnostno svetovanje NE zadeva izdelkov z brezžičnim radiem M-Bus, ki so bili konfigurirani s posameznimi ali strankinimi (uporabnimi) šifrirnimi tipkami.

Izdelki, ki niso navedeni, niso prizadeti. Izdelki, nameščeni v državah, ki niso navedene, niso prizadeti.

Mesta in izdelki, ki bi lahko bili prizadeti, so:

Države

Čile, Kolumbija, Češka, Danska, Francija in čezmorska ozemlja, Grčija, Italija, Nova Zelandija, Poljska, Slovaška, Slovenija, Južna Afrika, Švica, Ukrajina.

Izdelki

- Vodomeri iPERL, ki so bili prodani od leta 2014
- 640 vodnih metrov, prodanih od leta 2016
- Vodomeri MeistreamRF, ki se prodajajo od leta 2016
- MeiTwinRF merilniki vode, ki so bili prodani od leta 2016
- Radijske enote PulseRF, prodane med 6. in 3. 2018

Podrobnosti o ranljivosti

CWE-1394: Uporaba privzetega kriptografskega ključa

Ocena osnove CVSS v3.1 4.3 | Srednja | AV:A/AC:L/PR:N/UI:N/S:U/C:L*/I:N**/A:N***

CWE-1394: Obstaja uporaba privzete ranljivosti kriptografskega ključa, ki bi nepooblaščenemu akterju omogočila dostop do podatkov o porabi merilnika in lokaciji merilnika.

*Zaupnost – majhen vpliv

**Integriteta – brez vpliva

***Razpoložljivost – brez vpliva

Zmanjševanje

Za zmanjšanje tveganja, da nepooblaščeni akter pridobi dostop do prenosov sporočil obstoječih prizadetih izdelkov z uporabo izpostavljene privzete šifrirne tipke Xylem priporoča eno od naslednjih dejanj:

- Spremenite vse prizadete izdelke s privzetega ključa na posamezen ključ na meter.
  -ALI -
- Spremenite vse zadevne izdelke iz privzetega ključa v edinstven ključ stranke.

Podrobna navodila za implementacijo posameznega ključa na meter najdete na e-poštnem naslovu encryption.keys@xylem.com in z uporabo predmeta »Posamezni ključ«

Podrobna navodila za izvajanje edinstvenega ključa stranke najdete na e-poštnem naslovu encryption.keys@xylem.com in z uporabo predmeta »enolični ključ stranke«.

Kontaktni podatki

Za dodatne informacije o tem, kako izvajati priporočene blažitve, se obrnite na encryption.keys@xylem.com. Ena od naših podpornih ekip vam bo lahko zagotovila smernice in orodja za izvedbo te spremembe.

Za vsa vprašanja v zvezi s tem svetovalcem za varnost izdelkov Xylem se obrnite na product.security@xylem.com.

Zgodovina revizij	
Različica	**Posodobitve**
1,0	Objavljeno svetovanje

Izjava o omejitvi odgovornosti

Ta dokument je na voljo kot osnova in ne pomeni nobenega jamstva ali garancije, vključno z jamstvi primernosti za prodajo ali primernost za določeno uporabo. Uporaba informacij v tem dokumentu ali gradivih, povezanih s tem dokumentom, je na lastno odgovornost. Xylem si pridržuje pravico, da ta dokument kadar koli spremeni ali posodobi.