

# BEVEILIGINGSBULLETIN

Valleylab™ FT10 en Valleylab™ FX8  
RSSH-kwetsbaarheden elektrochirurgische generator

07-11-2019

Medtronic

## Overzicht van kwetsbaarheden

Medtronic evalueert actief zijn beveiligingspraktijken om risico's te beperken. Dit geldt zowel tijdens ontwikkeling (voor het in de handel brengen) en het gebruik (na het in de handel brengen) van onze producten. Door middel van deze routinemonitoring en -tests heeft Medtronic beveiligingskwetsbaarheden vastgesteld in de software van de Valleylab™ FT10 en Valleylab™ FX8 elektrochirurgische generatoren. Deze producten worden gebruikt in operatiekamers om artsen en verpleegkundigen te helpen tijdens chirurgische procedures. Deze kwetsbaarheden kunnen ervoor zorgen dat een onbevoegde persoon de controle over een elektrochirurgische generator overneemt, ofwel via het netwerk ofwel via fysieke toegang tot het apparaat, en diverse instellingen wijzigt.

**Tot op heden zijn er geen cyberaanvallen, gegevensinbreuken of patiëntletsel met een product van Medtronic gemeld of in verband gebracht met deze kwetsbaarheid.**

### Beperking

Medtronic raadt aan dat artsen en verpleegkundigen deze apparaten blijven gebruiken zoals dat bedoeld is.

Klanten moeten goede cyberhygiënepraktijken aanhouden door deze apparaten alleen op het ziekenhuisnetwerk aan te sluiten wanneer dat nodig is en deze tussentijds uit te schakelen totdat de nieuwe software-update is voltooid.

Medtronic heeft beveiligingsmaatregelen toegevoegd aan een software-update. Met deze maatregelen worden de vastgestelde beveiligingskwetsbaarheden beperkt en wordt het Valleylab™-apparaat beschermd tegen kwaadwillige inbraak. **Voor de FT10-generatoren:** De update is beschikbaar voor bepaalde versies. Klanten dienen contact op te nemen met hun verkoopvertegenwoordiger van Medtronic voor meer informatie. **Voor de FX8-generatoren:** Klanten worden op de hoogte gebracht wanneer de software-update beschikbaar is.

De update wordt aanbevolen voor een verbeterde beveiliging en een optimale gebruikerservaring. Apparaten kunnen verder worden gebruikt totdat de update voltooid is. Klanten met meerdere Valleylab™-generatoren moeten elk systeem afzonderlijk bijwerken.

### Aanvullende bronnen

Met de beschikbare software-update wordt een aparte cyberbeveiligingskwetsbaarheid aangepakt die alleen op de FT10-generator van toepassing is.

Alle klanten dienen contact op te nemen met hun lokale verkoopvertegenwoordiger voor meer informatie. Als u denkt dat er cyberbeveiligingsgerelateerde activiteiten hebben plaatsgevonden op uw apparaat, neemt u contact op met Medtronic via [jen.franssen@medtronic.com](mailto:jen.franssen@medtronic.com).

© 2019 Medtronic. Alle rechten voorbehouden. Medtronic, het Medtronic-logo en Further, Together zijn handelsmerken van Medtronic.

Alle overige merken zijn handelsmerken van een Medtronic-bedrijf. 11/2019 – US191074c