

# VARNOSTNO POROČILO

Ranljivosti RSSH v elektrokirurških generatorjih  
Valleylab™ FT10 in Valleylab™ FX8

07/11/2019

Medtronic

## Povzetek ranljivosti

Družba Medtronic aktivno preverja svoje varnostne postopke za zmanjševanje tveganj med razvojem pred uvedbo na trg in med uporabo po začetku trženja. S tem rutinskim nadzorom ter preskušanjem je družba Medtronic odkrila varnostne ranljivosti v programski opremi elektrokirurških generatorjev Valleylab™ FT10 in Valleylab™ FX8. Ta izdelka se uporabljata v operacijskih dvoranah kot pomoč kirurgom in medicinskim sestram med kirurškimi posegi. Te ranljivosti bi lahko omogočile nepooblaščenemu posamezniku, da bi prevzel nadzor na elektrokirurškem generatorjem, in sicer prek omrežja ali s fizičnim dostopom do naprave, ter spremil različne nastavitve.

**Do danes še ni bil zaznan noben kibernetški napad, niti ni v povezavi s to ranljivostjo prišlo do nobenega škodovanju bolniku, ki bi zajemalo izdelek družbe Medtronic.**

### Ukrepi

Družba Medtronic priporoča, da kirurgi in medicinske sestre še naprej uporabljajo te naprave za njihov ustrezni namen.

Dokler ne bo pripravljena nova posodobitev programske opreme, morajo stranke zagotavljati dobre kibernetške prakse in te naprave povezovati z omrežjem bolnišnice samo takrat, ko je to potrebno, med uporabami pa jih morajo izklopiti.

Družba Medtronic je v posodobitev programske opreme dodala izboljšave varnosti. Te izboljšave bodo zmanjšale odkrite varnostne ranljivosti in zaščitile napravo Valleylab™ pred zlonamernim vdorom. **Za generatorje FT10:** Posodobitev je na voljo za določene različice. Stranke naj se za več informacij obrnejo na prodajnega zastopnika družbe Medtronic. **Za generatorje FX8:** Stranke bodo obveščene, ko bo na voljo posodobitev programske opreme.

Izvedba posodobitve se priporoča za izboljšano varnost in optimalno uporabniško izkušnjo. Naprave se lahko še naprej uporabljajo, dokler ne bo posodobitev pripravljena. Stranke, ki imajo več generatorjev Valleylab™, bodo morale posodobiti vsak sistem posamezno.

### Dodatni viri

Ta posodobitev programske opreme naslavlja ločeno ranljivost, povezano s kibernetško varnostjo, ki vpliva na generator FT10. [povezava do poročila RFID]

Vse stranke naj se za dodatne informacije obrnejo na lokalnega prodajnega zastopnika. Če sumite, da je v vaši napravi prišlo do aktivnosti, povezane s kibernetško varnostjo, pišite družbi Medtronic na e-poštni naslov [rs.assurancequality@medtronic.com](mailto:rs.assurancequality@medtronic.com).