

Datum: 15. julij 2022

NUJNO VARNOSTNO OBVESTILO – NASVETI ZA VARNOST IT 05/2021

SpaceCom, Battery Pack SP with WiFi, Data module compactplus

Spoštovani,

Podjetje B. Braun Melsungen AG s tem varnostnim obvestilom obvešča prizadete stranke o varnostni težavi IT, verzija 05/2021, ki se nanaša na naprave B.Braun SpaceCom, Battery Pack SP with WiFi in Data module compactplus.

To varnostno obvestilo se tiče **odgovornosti za IT-varnost** prizadetih strank.

Prizadeti izdelki:

Številka izdelka	Ime izdelka	Različica programske opreme
8713142	SpaceStation with SpaceCom	011L0000L81 in starejše
8713182A	Battery-Pack SP (Li-Ion) incl. pin and WiFi	027L0000L81 in starejše
8713160	SpaceCom	011L0000L81 in starejše
8717160	Data module compactPlus	I0050A0010

Razlog za odpoklic

Aprila 2021 je bilo podjetje B. Braun obveščeno o morebitnih ranljivostih kibernetne varnosti pri zgoraj omenjenih izdelkih. Narava ranljivosti, vključno s številko CVE, točkovanjem CVSS in vektorskim nizom, je že bila objavljena maja 2021 na spletni strani podjetja B.Braun [05/2021 SpaceCom, Battery Pack SP with WiFi, Data module compactplus - multiple vulnerabilities \(bbraun.com\)](https://www.bbraun.com/05/2021_SpaceCom,_Battery_Pack_SP_with_WiFi,_Data_module_compactplus_-_multiple_vulnerabilities).

Podjetje B. Braun v času dejanske uporabe ni prejelo nobenih poročil o zlonamerni rabi ali incidentih, povezanih s temi ranljivostmi. Do danes ni bilo poročil o poškodbah bolnikov, uporabnikov ali tretjih oseb. Vendar pa ne moremo v celoti izključiti možnosti, da bi bile lahko te ranljivosti izkoriščene, kar je sicer malo verjetno. Zato obstaja teoretično tveganje za nastanek smrti ali začasno ali trajno resno poslabšanje bolnikovega zdravstvenega stanja.

Pod določenimi pogoji lahko izkoriščanje teh ranljivosti prefinjenemu napadalcu omogoči, da:

- ogrozi varnost komunikacijskih naprav Space ali compactplus,
- poveča privilegije,
- gleda občutljive informacije,

Stran 2 pisma z dne 15. julij 2022

- nalaga poljubne datoteke in na daljavo upravlja s komunikacijskimi napravami ali
- spremeni konfiguracijo priključene infuzijske črpalke Perfusor®, Infusomat® in Infusomat® P linij Space in compactplus, kar lahko po uspešnem napadu spremeni odmerjanje infuzije.

Ranljivosti se lahko pojavijo le pri majhnem številu naprav in pod naslednjimi pogoji:

- naprave so povezane z omrežjem,
- napadalec ima dostop do tega omrežja,
- napadalec s tem specifičnim napadom cilja na določeno napravo,
- infuzijska črpalka ne izvaja terapije (je izklopljena ali v stanju pripravljenosti).

Omilitveni ukrepi

Omilitveni ukrepi so opisani v dokumentu Nasveti za varnost IT 05/2021 in so objavljeni na spletni strani B.Braun [05/2021 SpaceCom, Battery Pack SP with WiFi, Data module compactplus - multiple vulnerabilities \(bbraun.com\)](https://www.bbraun.com/05/2021_SpaceCom_Battery_Pack_SP_with_WiFi_Data_module_compactplus_multiple_vulnerabilities) ter kot izvleček v Dodatku 1 spodaj.

Ukrepi, ki jih je treba izvesti

Naše evidence kažejo, da je vaša ustanova prejela potencialno prizadete naprave.

Prosimo vas, da takoj in prednostno začnete z naslednjimi ukrepi:

- V celoti preberite to varnostno obvestilo in zagotovite, da so odgovorna ekipa za varnost IT v vaši ustanovi in druge zadevne osebe obveščene o tem varnostnem obvestilu.
- Preglejte in izvedite omilitvene ukrepe glede trenutno vzpostavljene varnosti omrežja vaše ustanove. Če potrebujete pomoč, se obrnite na lokalnega predstavnika podjetja B. Braun.
- Če ste distributer, posredujte to varnostno obvestilo svoji stranki.
- Prosimo, da čim prej potrdite prejem teh informacij. Izpolnite priloženo potrdilo in ga pošljite podjetju B. Braun prek navedenih kontaktnih podatkov.

Če potrebujete več informacij, se obrnite na:

e-mail: edvard.skof@medis.com

Tel. št.: +386 41 332 030

Za morebitne nevednosti se iskreno opravičujemo in se vam vnaprej zahvaljujemo za hitro ukrepanje.

S spoštovanjem,

Vodja kontrole kakovosti
Andreja Oblak

Dodatek 1 – Omilitveni ukrepi

Omilitveni ukrepi so opisani v dokumentu Nasveti za varnost IT 05/2021 in so objavljeni na spletni strani B.Braun [05/2021 SpaceCom, Battery Pack SP with WiFi, Data module compactplus - multiple vulnerabilities \(bbraun.com\)](https://www.bbraun.com/05/2021_SpaceCom_Battery_Pack_SP_with_WiFi_Data_module_compactplus_-_multiple_vulnerabilities).

PRIPOROČILA ZA OMREŽJE

Vse ustanove, ki uporabljajo izdelke SpaceStation s SpaceCom2, Battery Pack SP with WiFi in DataModule compactplus, morajo pregledati svojo infrastrukturo IT in zagotoviti, da je bil implementiran koncept omrežnih con, pri katerem so kritični sistemi, kot so infuzijske črpalke, nameščeni v ločenih okoljih (npr. varovani s požarnimi zidovi ali z VLAN-om), ki niso dostopni neposredno s spleta ali s strani nepooblaščenih uporabnikov.

Brezžična omrežja je treba implementirati tako, da uporabite šifriranje po industrijskem standardu in ga opremito s sistemi za odkrivanje vdorov (»Intrusion Detection Systems«, IDS) in/ali sistemi za preprečevanje vdorov (»Intrusion Prevention Systems«, IPS).

Opomba: v nekaterih primerih lahko standardni varnostni ukrepi IT (npr. blokiranje vhodov) omejijo administrativne funkcije izdelka, vendar ne bodo vplivali na funkcije naprave, ki so povezane s terapijo. Kadar je za opravljanje administrativne funkcije treba zmanjšati varnostne ukrepe, morajo biti takšna dejanja začasne narave, zgoraj opredeljena priporočila pa se ponovno uvedejo takoj po uspešnem zaključku tega dejanja.

PROGRAMSKA OPREMA

Izdana je bila programska oprema za ublažitev prijavljenih pomanjkljivosti:

- Battery Pack SP with WiFi software 027L000092 (starejše od SN 138853)
- Battery Pack SP with WiFi software 053L000092 (SN 138853 in novejše)
- SpaceStation with SpaceCom2 software, različica 011L000092
- DataModule compactplus: različica A12 (I0050A0012)