**B. Braun Medical Ltd.**
3 Naas Road Industrial Park
Dublin 12
e-mail:
productcomplaints.ie@bbraun.com
http://www.bbraun.com

Date:
July 19, 2022

Ref: SECURITY ADVISORY 05/2021

# Urgent FIELD SAFETY NOTICE – IT-SECURITY ADVISORY 05/2021

## SpaceCom

Dear Sir/Madam,

**B. Braun Melsungen AG** has decided to inform affected customers about IT-SECURITY issue 05/2021 referring to the B. Braun device, SpaceCom, via a Field Safety Notice.
This FSN addresses **IT SECURITY responsibles** of affected customers.

**Affected Articles**:

| Article Number | Article Name | Software Version |
|---|---|---|
| 8713142 | SpaceStation with SpaceCom | 011L0000L81and earlier |
| 8713160 | SpaceCom | 011L0000L81and earlier |

**Reason for the Notice**
In April 2021, B. Braun was made aware of potential cybersecurity vulnerabilities in the above mentioned products. The nature of the vulnerabilities including CVE number, CVSS scoring and vector string had already been published in May 2021 on the B.Braun homepage 05/2021 SpaceCom, Battery Pack SP with WiFi, Data module compactplus - multiple vulnerabilities (bbraun.com).

B. Braun has received no reports of exploitation or incidents associated with these vulnerabilities in an actual use environment. No injuries to patients, users, or third parties have been reported to date. However we cannot fully exclude that the vulnerabilities may potentially be exploited with a very low likelihood. Therefore, there is a theoretical risk for occurrence of the death or the temporary or permanent serious deterioration of a patient's state of health.

Under certain conditions, successful exploitation of these vulnerabilities could allow a sophisticated attacker to:

- Compromise the security of the Space communication devices,
- Escalate privileges,
- View sensitive information,
- Upload arbitrary files and perform remote code execution on the communication devices,
- or change the configuration of a connected infusion pump Perfusor®, Infusomat® and Infusomat® P from Space which may alter infusions after a successful attack.

The vulnerabilities can only occur in a small number of devices and under the following conditions:

- devices are connected to a network,
- attacker has access to this network,
- attacker targets the specific device with this specific attack,
- infusion pump is not delivering a therapy (it is "Turned Off" or in "Standby Mode").

**Mitigating Measures**

Mitigating measures are described in the B.Braun IT SECURITY advisory 05/2021 on the B.Braun homepage 05/2021 SpaceCom, Battery Pack SP with WiFi, Data module compactplus - multiple vulnerabilities (bbraun.com) and as an excerpt in Appendix 1 below.

**Actions to be taken**

Our records have shown that your institution has received potentially affected devices.

We kindly ask you to initiate the following activities immediately and with priority:

- Review this Field Safety Notice in its entirety and ensure that the responsible IT SECURITY team in your organisation and other concerned persons are informed about this Field Safety Notice.
- Review and apply the Mitigating Measures in the context of the currently established network security of your institution. If you need help please contact your local B. Braun representative.
- If you are a distributor, please forward this Field Safety Notice to your customer.
- Please confirm receipt of this information at your earliest convenience by completing and signing the attached confirmation slip and returning this to B. Braun using the contact details provided..

*Please return the completed form by **Friday 22nd July 2022**, or sooner if possible.*

The Health Products Regulatory Authority (HPRA) has been informed of this action.

If more information is needed, please contact:

Eamonn Dargan
Healthcare Technology Manager
B. Braun Medical Ltd
Tel: +353 86-2214686
Email: eamonn.dargan@bbraun.com

We appreciate your immediate attention and apologise for any inconvenience caused.

Yours sincerely,

mcguciie Digitally signed by mcguciie Date: 2022.07.19 15:52:49 +01'00'

**Ciarán McGuinness**
**Digital Health & Healthcare Technology Lead**

eganroie Digitally signed by eganroie Date: 2022.07.19 15:22:13 +01'00'

**Roberta Egan**
**Regulatory Affairs Manager**

## Appendix 1 – Mitigating Measures

Mitigating measures are described in the B.Braun IT SECURITY advisory 05/2021 on the B.Braun homepage 05/2021 SpaceCom, Battery Pack SP with WiFi, Data module compactplus - multiple vulnerabilities (bbraun.com) .

NETWORK RECOMMENDATIONS
All facilities utilizing SpaceStation with SpaceCom2, Battery Pack SP with WiFi, and DataModule compactplus should review their IT infrastructure to ensure that a network zone concept has been implemented whereby critical systems, such as infusion pumps, are housed in separate (e.g., by firewalls or VLAN) environments which are not accessible directly from the internet or by unauthorized users.
Wireless networks should be implemented using industry standard encryption and should be equipped with Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS).
Note: In some instances, standard IT security measures (e.g. blocking of ports) may limit the administrative functions of the product, but will not impact the therapy related functions of the device. Where it is necessary to reduce security measures to perform an administrative function, such actions should be temporary in nature, and the recommendations identified above reinstituted immediately upon successful completion of the function.

SOFTWARE
Software has been released to mitigate the reported vulnerabilities:

- Battery Pack SP with WiFi software 027L000092 (below SN 138853)
- Battery Pack SP with WiFi software 053L000092 (SN 138853 and higher)
- SpaceStation with SpaceCom2 software version 011L000092
- DataModule compactplus: version A12 (I0050A0012)