B|BRAUN

B. Braun Melsungen AG
Division Hospital Care
Complaint Management

34209 Melsungen

Contact: Dr. Stephan Krause

Our Reference SECURITY ADVISORY 05/2021
Fon: +49 5661 71-1339
Fax: +49 5661 71-
Email: stephan.krause@bbraun.com
Internet: http://www.bbraun.com

Date: Jul 15, 2022

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

SpaceCom, Battery Pack SP with WiFi, Data module compactplus

The B. Braun Melsungen AG has decided to inform affected customers about IT-SECURITY issue 05/2021 referring to the B.Braun devices SpaceCom, Battery Pack SP with WiFi and Data module compactplus 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
8713182A	Battery-Pack SP (Li-Ion) incl. pin and WiFi	027L0000L81and earlier
8713160	SpaceCom	011L0000L81and earlier
8717160	Data module compactPlus	I0050A0010

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 up 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 or compactplus 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 both Space and compactplus family 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 organization 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. Please complete the attached confirmation slip and return this to B. Braun using the contact details provided.

If more information is needed, please contact

Local contact 1	Local contact 2
Name	
Title	
Email	
telephone	

B|BRAUN

Kindly accept our apologies for any inconveniences caused and thank you in advance for your cooperation to resolve this matter quickly.

Yours sincerely,

B|BRAUN

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)