SECURITY ADVISORY

Friday, May 14, 2021

05/2021 SpaceCom, Battery Pack SP with WiFi, Data module compactplus - multiple vulnerabilities

Vulnerability Advisory

1 Executive Summary

CVSS v3.1 9.0

ATTENTION: Exploitable remotely/ high skill level to exploit

Vendor: B. Braun Melsungen AG

Equipment: Perfusor® Space, Infusomat® Space, Infusomat® Space P, SpaceCom, Battery Pack SP with WiFi; Perfusor® compactplus, Infusomat® compactplus, Infusomat® P compactplus, Data module compactplus

Vulnerabilities: Insufficient Verification of Data Authenticity, Missing Authentication for Critical Function, Cleartext Transmission of Sensitive Information, Unrestricted Upload of File with Dangerous Type, Improper Input Validation

2 Risk Evaluation

Successful exploitation of these vulnerabilities could allow a sophisticated attacker to compromise the security of the Space or compactplus communication devices, allowing an attacker to escalate privileges, view sensitive information, upload arbitrary files, and perform remote code execution.

Under certain conditions, successful exploitation of these vulnerabilities could allow an attacker to change the configuration of a connected infusion pump Perfusor®, Infusomat®, Infusomat® P from both Space and compactplus family which may alter infusions after a successful attack.

These conditions include all of the following: (i) the pumps are connected to a network, (ii) the attacker has access to this network, (iii) the attacker targets the specific device with this specific attack, (iv) the infusion pump is not delivering a therapy (it is “Turned Off” or in “Standby Mode”).

Change of a running therapy is not possible.

B. Braun has received no reports of exploitation or incidents associated with these vulnerabilities in an actual use environment.

3 Technical Details

3.1 Affected Products

The following versions of B. Braun products are affected:

- SpaceCom, software versions 011L0000L81and earlier
- Battery pack with WiFi, software versions 027L0000L81and earlier
- Data module compactplus, software version I0050A0010

Other devices of B. Braun are **not** affected.

Note: For devices marketed in the United States (software versions ‘U’), a separate advisory is available. Facilities in Canada utilizing “U” versions of software should follow this U.S. Vulnerability Disclosure. Facilities in Canada utilizing non-“U” versions (e.g. L) should follow outside the U.S. Vulnerability Disclosure.

3.2 Vulnerability Overview

3.2.1 CWE-345: Insufficient Verification of Data Authenticity

Insufficient verification of data authority may allow an attacker to upload specific files to the Com devices. Unrecognized files may reset the device to service mode. An upload cannot be done while a therapy is running. Only devices turned off or in standby mode maybe affected.

CVE-2021-33885 has been assigned to this vulnerability. A CVSS v3.1 score of 9.0 has been calculated, the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).

3.2.2 CWE-306: Missing Authentication for Critical Function: Network commands require no authentication

Missing authentication may allow an attacker to upload specific files to the Com devices. Unrecognized files may reset the device to service mode. An upload cannot be done while a therapy is running. A remote change of infusion rates is not possible. Only devices turned off or in standby mode maybe affected.

CVE-2021-33882 has been assigned to this vulnerability. A CVSS v3.1 score of 6.8 has been calculated, the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N).

3.2.3 CWE-319: Cleartext Transmission of Sensitive Information: Network commands are sent in plaintext

Missing encryption may allow an attacker to record data in transmission. An attacker may also send specific network commands to upload files to the Com devices. Unrecognized files may reset the device to service mode. An upload cannot be done while a therapy is running. A remote change of infusion rates is not possible. Only devices turned off or in standby mode maybe affected. These issues do not affect the infusion pump at all.

CVE-2021-33883 has been assigned to this vulnerability. A CVSS v3.1 score of 5.9 has been calculated, the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).

3.2.4 CWE-434: Unrestricted Upload of File with Dangerous Type

By using the vulnerability, an attacker may upload arbitrary files to the system. This may be used to change the communication device behavior including its availability on the network, but not the availability or integrity of the connected pumps.

CVE-2021-33884 has been assigned to this vulnerability. A CVSS v3.1 score of 6.5 has been calculated, the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).

3.2.5 3.2.5 CWE-20: Improper input validation

An improper sanitization of input vulnerability allows a remote unauthenticated attacker to gain user-level command-line access by passing a raw external string straight through to printf statements. The attacker is required to be on the same network as the device.

CVE-2021-33886 has been assigned to this vulnerability. A CVSS v3.1 score of 6.8 has been calculated, the CVSS vector string is (AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).

3.2.6 Relative Path Traversal (CWE-23)

A relative path traversal attack in the B. Braun SpaceCom version L81/U61 and earlier and the Data module compactplus versions A10 and A11 allows attackers with service user privileges to upload arbitrary files. By uploading a specially crafted tar file, an attacker can execute arbitrary commands.

CVE-2020-25150 has been assigned to this vulnerability. A CVSS v3 base score of **7.6** has been assigned; the CVSS vector string is (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L).

3.3 Background

Critical Infrastructure Sectors: Healthcare and Public Health

Countries/Areas Deployed: Worldwide (except USA)

Company Headquarters Location: Germany

3.4 Researcher

McAfee Advanced Threat Research (ATR)

4 Mitigations

B. Braun recommends:

DEVICE RECOMMENDATIONS

Always use the latest updates:

- SpaceStation with SpaceCom2: L81 (011L0000L81) or later
- Battery Pack SP with WiFi:L81 (027L0000L81) or later
- DataModule compactplus: version A11 (I0050A0011) or later

Note: For devices marketed in the United States (software versions ‘U’), a separate advisory is available. Facilities in Canada utilizing “U” versions of software should follow this U.S. Vulnerability Disclosure. Facilities in Canada utilizing non-“U” versions (e.g. L) should follow outside the U.S. Vulnerability Disclosure.

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.

The B. Braun advisory is available at bbraun.com/productsecurity. Please contact your local B. Braun organization to request further help.

Update A:

Software has been released to mitigate the reported vulnerabilities:

- Battery pack SP with WiFi, software 053L00091 (SN 138853 and higher)
- SpaceStation with SpaceCom 2 software versions 011L000083
- DataModule compactplus: version A12 (I0050A0012)

5 Contact information

If you have any additional information regarding the security of our products, please contact your local B. Braun representative or directly productsecurity@bbraun.com.

If you are a B. Braun customer and need support in mitigating the above mentioned vulnerabilities, contact your local B. Braun representative.