Vulnerability Advisory

1 Executive Summary

- **CVSS v3.1: 9.7**
- **ATTENTION**: Exploitable remotely/ high skill level to exploit
- **Vendor**: B. Braun Medical Inc.
- **Equipment**: Perfusor Space, Infusomat Space, SpaceCom, Battery Pack SP with WiFi
- **Vulnerabilities**: Insufficient Verification of Data Authenticity, Missing Authentication for Critical Function, Cleartext Transmission of Sensitive Information, Unrestricted Upload of File with Dangerous Type

2 Risk Evaluation

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

Under certain conditions identified below, successful exploitation of these vulnerabilities could allow an attacker to change the configuration of connected infusion pumps (e.g. Perfusor® Space, Infusomat® Space) 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 U61 and earlier (United States)
- Battery pack with WiFi, software versions U61 and earlier (United States)
- Other devices of B. Braun are not affected.

Note: For devices marketed outside of the United States, a separate advisory is available.

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 SpaceCom devices. Unrecognized files may set the device in service mode. An upload cannot be done while a therapy is running. Only devices turned off or in standby mode may be affected.

A CVSS v3.1 score of **9.7** has been calculated, the CVSS vector string is CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/CR:H/IR:H/AR:M/MAV:A.

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 SpaceCom 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 may be affected.

A CVSS v3.1 score of **8.2** has been calculated, the CVSS vector string is CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N/CR:H/IR:H/AR:M/MAV:A.

3.2.3 CWE-319: Cleartext Transmission of Sensitive Information

Missing encryption may allow an attacker to record data in transmission. An attacker may also send specific network commands to upload files to the SpaceCom 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 may be affected. These issues do not affect the infusion pump at all.

A CVSS v3.1 score of **7.1** has been calculated, the CVSS vector string is CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/CR:H/IR:H/AR:M/MAV:A.

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.

A CVSS v3.1 score of **5.4** has been calculated, the CVSS vector string is CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/CR:M/IR:M/AR:L/MAV:A.

Background

- **Critical Infrastructure Sectors:** Healthcare and Public Health
- **Countries/Areas Deployed:** USA
- **Company Headquarters Location:** USA

3.3 Researcher

McAfee Advanced Threat Research (ATR)

4 Mitigations and Compensating Controls

B. Braun recommends:

DEVICE RECOMMENDATIONS

- Always use the latest updates:
  - SpaceCom: version U62 or later (United States only)
  - Battery Pack SP with WiFi: version U62 or later (United States only)

NETWORK RECOMMENDATIONS

- All facilities utilizing SpaceCom, and Battery Pack SP with WiFi 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 multi-factor authentication and 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.

A digital version of this advisory can be found at https://www.bbraunusa.com/en/products-and-therapies/infusion-therapy.html#infusion-pumps-accessories-and-services

5 Contact information

If you are a B. Braun customer and need support in mitigating the above-mentioned vulnerabilities, please contact B. Braun Technical Support by calling 800-627-PUMP or by emailing AISTechSupport@bbraunusa.com.

If you have any additional information regarding the security of our products, please forward your concerns to ProductSecurity_NA@bbraunusa.com.