B BRAUN

B. Braun Melsungen AG
Division Hospital Care
Safety Officer Medical Devices

34209 Melsungen

Contact: Dr. Stephan Krause

Fon: 05661 71-1339
Fax: 05661 71-1339
Email: stephan.krause@bbraun.com
Internet: http://www.bbraun.de

Date: November 01, 2021

TO WHOM IT MAY CONCERN

To whom it may concern,

this document provides a comprehensive elaboration on the evaluation of potential hazards to patients' health concerning an IT-security issue affecting directly or indirectly SpaceCom, SpaceStation with SpaceCom, Battery Pack SP with WiFi, Infusomat Space, Perfusor Space, Infusomat Space P, Perfusor compactplus, Infusomat compactplus, Infusomat compactplus P and Data module compactplus.

The same issue had been published with different levels of detail at different points in time. All publications refer to the same IT-security issue. The following list is not exhaustive but represents the most relevant publications:

May 2021, (and updated October 2021)	B. Braun	https://www.bbraun.com/en/products-and-therapies/services/b-braun-vulnerability-disclosure-policy/security-advisory/spacecom--battery-pack-sp-with-wifi--data-module-compactplus---m.html
August 2021	McAfee	https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/overmedicated-breaking-the-security-barrier-of-a-globally-deployed-infusion-pump
October 2021	CISA	https://us-cert.cisa.gov/ics/advisories/icsma-21-294-01

1.) Technical Defect

Transfer of configuration data via network with insufficient integrity protection and insufficiently secure authentication is possible. Attackers are able to transfer manipulated data and change functional properties of the pump. Drug libraries, modification data and disposable data could be manipulated. All technical details are provided in a systematic fashion under the B.Braun security advisory https://www.bbraun.com/en/products-and-therapies/services/b-braun-vulnerability-disclosure-policy/security-advisory/spacecom--battery-pack-sp-with-wifi--data-module-compactplus---m.html

2.) Potential clinical consequences

In a worst case, manipulation of disposable data may lead to incorrect calculation of motor speed and altered delivery rates. The rates can lead to under- AND over-infusion. A maximal modulation of rate deviations could not be identified.

3.) Relevant Complaints (Facts)

The above information had been provided by McAfee after detailed security investigation of the addressed devices. However, feedback from the market is unknown. No complaints from the market were registered so far.

4.) Potential Occurrence of Harm

Patient harm resulting from over- and underinfusion can potentially result from no clinical consequences (S1) up to patient's death (S5). As in this case the patient harm is intentionally and maliciously created with criminal motivation, it is assumed that patient harm will be in the range from S4 (serious patient injury) to S5 (death).

5.) Risk estimation

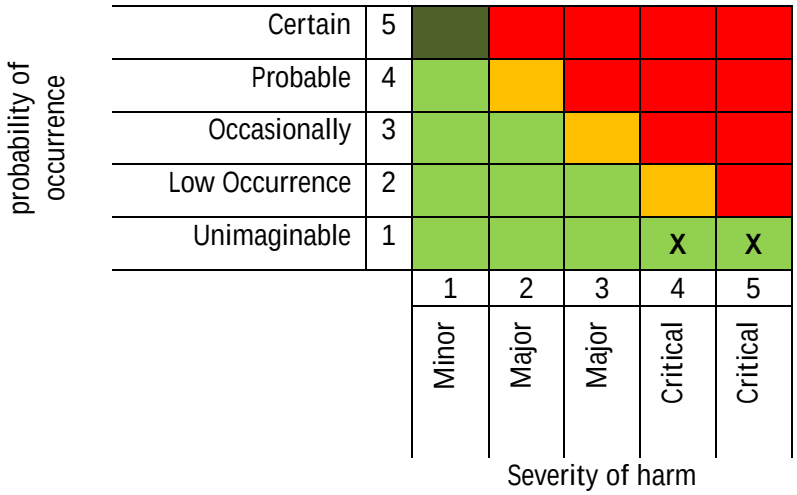
The overall risk is a combination of 1.) likelihood of exploit and 2.) execution of exploit:
(overall risk) = (likelihood of exploit) x (execution of exploit).

Based on the overall CVSS (environmental) score of 9.0 and security risk assessment following FDA Guidance for Industry - Postmarket Management of Cybersecurity in Medical devices (December 28, 2016) an exploitability of 4 in a scale from 1 to 5 is given[1]. This represents the execution of an exploit.
The likelihood of an exploit is affected 1.) by the prior successful intrusion into the hospital network, 2.) by the identification of the vulnerability and 3.) by the identification of attackable pumps. The three factors depend on the network security measures of the hospital, the time and the inside knowledge about the functionality of the pumps and the ability to identify pumps that are currently not running. All three factors are necessary conditions for a successful exploit, that need to be successfully executed at the same attempt of a hack. Most reasonable assumption is that they sum up to a likelihood of an exploit of 1/5000 [(Successful attack of a hospital = 1/10) * (Identification of vulnerability = 1/50) * (Identification of attackable pump = 1/10)]. Given that the information how the attack occurs is now more readily available in the public sphere (see links above) and that some information is presented which may aid malicious actors in reducing the effort necessary to facilitate an attack against a B. Braun device, it is assumed for conservative purposes that the effort is ~50% when compared to the original estimates. Therefore, the overall rate of occurrence is estimated to be 1/2500. In a logarithmic Risk Matrix this factor of 1/2500 reduces the overall rate of occurrence by three steps to an occurrence of O1 in a scale from O1 (<1 ppm/year) to O5 (≥1000 ppm/ year) (see risk graph below).

A central definition relevant to all cybersecurity requirements within the Medical Devices is that 'risk' means the combination of the probability of occurrence of harm and the severity of that harm. Taking into account potential Severities S4 (serious patient injury) and S5 (death) and the likelihood and execution of the exploit (O1), the overall risk is considered a controlled risk.

[1] For a successful exploit, the attacker needs to deliberately choose the specific infusion pump and deliberately change a specific parameter and its checksum

A graphical presentation of the risk estimation is provided below:



red: unacceptable risk
Orange: alert area
green: acceptable risk

Probability of occurrence:

Certain O5	≥1000 ppm/ year
Probable O4	<1000 ppm/ year
Occasionally O3	<100 ppm/ year
Low Occurrence O2	<10 ppm/ year
Unimaginable O1	<1 ppm/ year

The above mentioned facts and estimations were assessed based on the principles of FDA Guidance for Industry - Postmarket Management of Cybersecurity in Medical devices (December 28, 2016) and the risk management standard EN ISO 14971. The risk was found to be in the acceptable area of the risk graph. Actions in the market are not proportionate to the identified risk.

We hope that this adequately explains the situation and the background for our risk assessment. Should there be any open questions please do not hesitate to contact us.

Best regards,

B. Braun Melsungen AG

i.V.

Dr. Stephan Krause
Digital unterschrieben von Dr. Stephan Krause
Datum: 2021.11.03 09:39:58 +01'00'

Dr. Stephan Krause
Safety Officer Medical Devices

i.A.

Dr. Annika Skalik
Digital unterschrieben von Dr. Annika Skalik
Datum: 2021.11.03 12:22:28 +01'00'

Dr. Annika Skalik
Deputy Safety Officer Medical Devices