B. Braun Milano S.p.A.
a Socio Unico

Via V. da Seregno, 14
20161 Milano - Italia
Tel. 02/66.218.1
Fax 02/66.218.312
Email: info.bbitalia@bbraun.com
www.bbraun.it

A CHI DI COMPETENZA

Luogo, Data: Milano, 28/02/2022

In qualità di distributori del fabbricante B. Braun Melsungen AG, con la presente comunicazione siamo ad inviarVi una valutazione del rischio per conto del fabbricante.

Si tratta della valutazione di potenziale rischio per la salute dei pazienti in merito alla sicurezza informatica riguardante in maniera diretta o indiretta i prodotti SpaceCom, SpaceStation con SpaceCom, Battery Pack SP con wi-fi, Infusomat Space, Perfusor Space, Infusomat Space P, Perfusor compactplus, Infusomat compactplus, Infusomat compactplus P e il Data Module compactplus.

La stessa informazione era già stata pubblicata con diversi livelli di dettaglio in diversi momenti. Tutte le pubblicazioni riguardavano lo stesso tema di sicurezza informatica. La seguente tabella non è non esaustiva ma riassume le pubblicazioni più rilevanti in merito:

Maggio 2021 (e relativo aggiornamento di ottobre 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
Agosto 2021	McAfee	https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/overmedicated-breaking-the-security-barrier-of-a-globally-deployed-infusion-pump
Ottobre 2021	CISA	https://www.cisa.gov/uscert/ics/advisories/icsma-21-294-01

1.) **Difetto tecnico**

È possibile che si verifichi il trasferimento dei dati di configurazione tramite rete con protezione di integrità insufficiente e di sicurezza di autenticazione non sufficiente. Gli aggressori sono in grado di trasferire dati manipolati e modificare le proprietà funzionali della pompa. Le librerie di farmaci, i dati di modifica e i dati relatici al monouso potrebbero essere manipolati. Tutti i dettagli tecnici sono forniti in modo sistematico nell'ambito dell'avviso di sicurezza 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

B. Braun Milano S.p.A.
a Socio Unico

Via V. da Seregno, 14
20161 Milano - Italia
Tel. 02/66.218.1
Fax 02/66.218.312
Email: info.bbitalia@bbraun.com
www.bbraun.it

2.) Potenziali conseguenze cliniche

Nel caso peggiore, la manipolazione dei dati relativi al monouso può portare a un calcolo errato della velocità del motore e ad alterazioni della velocità di infusione. Tali alterazioni possono portare a sotto- E sovra-infusione. Non è stato possibile identificare una modulazione massima delle deviazioni.

3.) Reclami pertinenti (fatti)

Le informazioni di cui sopra erano state fornite da McAfee dopo un'indagine di sicurezza dettagliata dei dispositivi coinvolti. Tuttavia, non sono noti feedback dal mercato. Finora non sono stati registrati reclami dal mercato.

4.) Incidenza potenziale del danno

Il danno al paziente derivante da un'infusione eccessiva e insufficiente può potenzialmente andare dall'assenza di conseguenze cliniche (S1) fino alla morte del paziente (S5). Poiché in questo caso il danno al paziente è creato intenzionalmente e malignamente con motivazione criminale, si presume che il danno al paziente sarà compreso tra S4 (lesione grave del paziente) a S5 (morte).

5.) Stima del rischio

Il rischio complessivo è una combinazione di 1.) probabilità di accadimento e 2.) il verificarsi dell'accadimento:
(rischio complessivo) = (probabilità di accadimento) x (il verificarsi dell'accadimento).

Sulla base del punteggio CVSS (ambientale) complessivo di 9,0 e della valutazione del rischio per la sicurezza in base alla Guida FDA per l'industria - Gestione post-vendita della sicurezza informatica nei dispositivi medici (28 dicembre 2016) viene fornito un grado di accadimento di 4 in una scala da 1 a 5[1]. Questo rappresenta il verificarsi dell'accadimento.
La probabilità di un accadimento è influenzata 1.) dalla precedente intrusione riuscita nella rete ospedaliera, 2.) dall'identificazione della vulnerabilità e 3.) dall'identificazione di pompe attaccabili. I tre fattori dipendono dalle misure di sicurezza della rete dell'ospedale, dalla tempistica e dalle conoscenze interne sulla funzionalità delle pompe e dalla capacità di identificare le pompe che attualmente non sono in funzione. Tutti e tre i fattori sono condizioni necessarie per un accadimento di successo, che deve essere eseguito con successo nello stesso tentativo di attacco. L'ipotesi più ragionevole è che venga raggiunta una probabilità di un accadimento di 1/5000 [(Attacco riuscito di un ospedale = 1/10) * (Identificazione della vulnerabilità = 1/50) * (Identificazione della pompa attaccabile = 1/10)].

1 Per un accadimento riuscito, l'aggressore deve scegliere deliberatamente la pompa di infusione specifica e modificare deliberatamente un parametro specifico e il relativo checksum

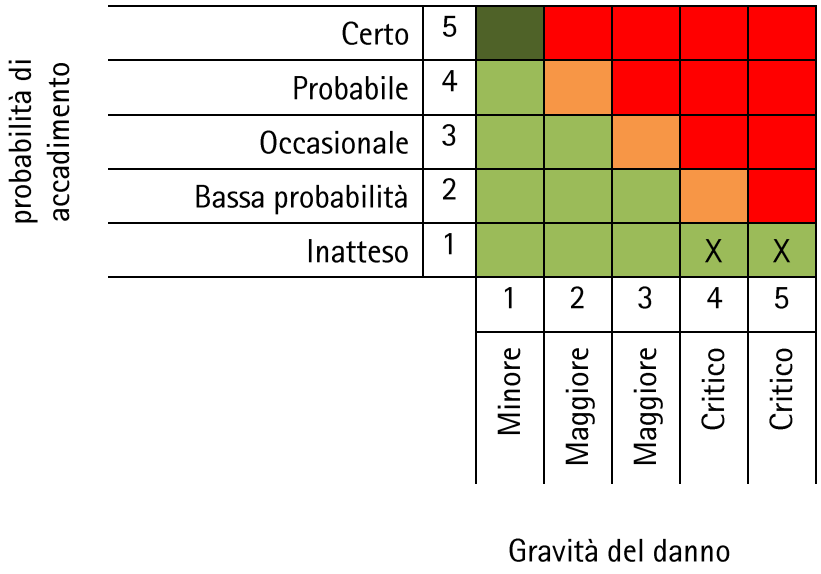
B. Braun Milano S.p.A.
a Socio Unico

Via V. da Seregno, 14
20161 Milano - Italia
Tel. 02/66.218.1
Fax 02/66.218.312
Email: info.bbitalia@bbraun.com
www.bbraun.it

Dato che le informazioni su come si verifica l'attacco sono ora più facilmente e pubblicamente disponibili (vedere i collegamenti sopra) e che vengono presentate alcune informazioni che potrebbero aiutare gli attori malintenzionati a ridurre lo sforzo necessario per facilitare un attacco contro un dispositivo B. Braun, si presume a fini prudenziali che lo sforzo sia del 50% circa rispetto alle stime originali. Pertanto, il tasso complessivo di occorrenza è stimato in 1/2500.

In una matrice di rischio logaritmica, questo fattore di 1/2500 riduce il tasso complessivo di occorrenza di tre gradini al verificarsi di O1 in una scala da O1 (<1 ppm/anno) a O5 (≥1000 ppm/anno) (vedere grafico del rischio qui di seguito).
Una definizione centrale rilevante per tutti i requisiti di sicurezza informatica all'interno dei Dispositivi Medici è che per "rischio" si intende la combinazione della probabilità che si verifichi un danno e la gravità di tale danno. Tenendo conto delle potenziali Gravità S4 (lesioni gravi del paziente) e S5 (morte) e della probabilità e del verificarsi dell'accadimento (O1), il rischio complessivo è considerato un rischio controllato.

Di seguito viene fornita una rappresentazione grafica della stima del rischio:



Rosso: rischio inaccettabile
Arancione: are di allerta
Verde: riaschio accettabile

B. Braun Milano S.p.A.
a Socio Unico

Via V. da Seregno, 14
20161 Milano - Italia
Tel. 02/66.218.1
Fax 02/66.218.312
Email: info.bbitalia@bbraun.com
www.bbraun.it

Probabilità di accadimento:

Certo 05	*≥ 1000 ppm/anno*
Probabile 04	*< 1000 ppm/anno*
Occasionale 03	*< 100 ppm/anno*
Bassa probabilità 01	*< 10 ppm/anno*
Inatteso 01	*< 1 ppm/anno*

I fatti e le stime di cui sopra sono stati valutati sulla base dei principi della FDA Guidance for Industry - Postmarket Management of Cybersecurity in Medical devices (28 dicembre 2016) e della norma di gestione del rischio EN ISO 14971. Il rischio è risultato essere accettabile del grafico di rischio. Le azioni sul mercato non sono proporzionate al rischio identificato.

Ci auguriamo che questo spieghi adeguatamente la situazione e il contesto della nostra valutazione del rischio. In caso di domande aperte, non esitate a contattarci.

Lorenzo Sovera
(Hospital Channel Director)
Tel. +39 0266218302
lorenzo.sovera@bbraun.com

Lidia Perri
(Local Safety Officer)
Tel. +39. 02.662.18.262
Fax: +39.02.662.182.72
lidia.perri@bbraun.com