Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-22-040-1

Vulnerability and Incident Reporting
product-security@draeger.com

Important Safety Notice!

Infinity Acute Care System - Workstation Critical Care (Evita V500),
Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500) and
Evita V300

1 Publication Date

2022-02-10

2 Description

Medical devices are increasingly operated in networked environments. The exchange of information among medical devices, hospital networks and the internet allow solutions that improve the treatment of patients by healthcare providers and can make health care better. At the same time, the operation in networked environments increases the risk of potential cybersecurity threats. A cybersecurity attack could impact the safety and effectiveness of medical devices.

The ventilators of the product family Evita V500/V300 and Babylog VN500 have been in use in many countries worldwide since 2007. They are highly accepted, reliable ventilators with a total of more than 124,000 years of operation. To date, Draeger has not received any report or evidence of any case of a cyberattack.

The abovementioned ventilators use specially hardened operating systems. However, one of the used operating systems cannot be updated any longer, and its vulnerabilities cannot be fixed anymore. Therefore, they are not prepared against potential cyber security threats to the same extent as newer devices. This includes those carried out with physical access. Draeger therefore recommends the following:

- Follow the recommendations in the instructions for use:
    - Limit or control physical access to the abovementioned ventilators.
    - Do not connect any non-approved devices to the USB, LAN and DVI interfaces.
    - Be attentive to notifications, alarms and alerts
- Consider closing/covering all unused USB, LAN and DVI interfaces

For customers who decide to close/cover unused USB, LAN and DVI interfaces, Dräger offers to provide tools upon request to cover or close these ventilation data interfaces. If applicable, customers can contact their local Dräger organization.

3 Affected Products

The following Dräger products are affected:

- Infinity Acute Care System - Workstation Critical Care (Evita V500) with SW2.60 and lower
- Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500) with SW2.60 and lower
- Evita V300 with SW2.60 and lower

4 Contact Information

If you have any further questions related to the impact of the vulnerabilities, please contact your designated regional marketing manager. For reporting incidents and potential vulnerabilities in our devices, please refer to https://static.draeger.com/security to contact the Product Security team directly.

5 Revision History

VERSION	DATE	COMMENTS
1.0	2022-02-10	Initial Advisory

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner