À nos clients utilisateurs des
ventilateurs de Dräger
Infinity Acute Care System – Workstation Critical Care (Evita V500),
Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500)
et Evita V300

Janvier 2022

Consigne importante de sécurité !

Mesure d'amélioration de la cybersécurité

Les produits suivants sont concernés :
Infinity Acute Care System – Workstation Critical Care (Evita V500) avec version logicielle 2.60 et inférieure.
Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500) avec version logicielle 2.60 et inférieure.
Evita V300 avec version logicielle 2.60 et inférieure.

Madame, Monsieur,

Les dispositifs médicaux fonctionnent de plus en plus dans des environnements en réseau. L'échange d'informations entre les dispositifs médicaux, les réseaux hospitaliers et internet permet de développer des solutions qui optimisent le traitement des patients par les prestataires de soins de santé, améliorant ainsi les soins de santé. En même temps, le fonctionnement dans des environnements en réseau augmente le risque de cybermenaces. Une cyberattaque pourrait avoir un impact sur la sécurité et l'efficacité des dispositifs médicaux.

Les ventilateurs de la famille de produits Evita V500/V300 et Babylog VN500 sont utilisés dans de nombreux pays dans le monde entier depuis 2007. Ce sont des ventilateurs fiables et très répandus, avec un total de plus de 124 000 années de fonctionnement. À ce jour, Dräger n'a reçu aucun rapport ni aucune preuve d'un quelconque cas de cyberattaque. Seuls quelques clients utilisent leurs ventilateurs dans un environnement en réseau qui permet l'échange d'informations entre les ventilateurs et la Service Connect Gateway de Dräger. La plupart des appareils sont connectés via une interface série Medibus/Medibus X, qui n'est pas vulnérable aux cyberattaques.

En théorie, les appareils qui ne sont pas connectés à un réseau risquent également d'être exposés à des cybermenaces. Ce type d'attaque nécessiterait toutefois un accès physique direct à l'appareil. Pour

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Allemagne
Adresse postale :
23542 Lübeck, Allemagne
Tél. +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
N° de TVA DE135082211

Coordonnées bancaires :
Commerzbank AG, Lübeck
IBAN : DE95 2304 0022 0014 6795 00 Code SWIFT : COBA DE FF 230
Sparkasse zu Lübeck
IBAN : DE15 2305 0101 0001 0711 17
Code SWIFT : NOLADE21SPL

Siège de la société : Lübeck
Registre du commerce :
Tribunal d'instance Lübeck HRB 7903 HL
Commandité : Drägerwerk Verwaltungs AG
Siège de la société : Lübeck
Registre du commerce :
Tribunal d'instance Lübeck HRB 7395 HL

Président du conseil de surveillance
Pour Drägerwerk AG & Co. KGaA et Drägerwerk Verwaltungs AG :
Stefan Lauer
Direction :
Stefan Dräger (Président)
Rainer Klug
Gert-Hartwig Lescow
Dr Reiner Piske

cela, un cyberattaquant devrait obtenir un accès non autorisé à une unité de soins intensifs et qu'il modifie chaque ventilateur individuellement. Cela pourrait avoir un impact sur la thérapie de ventilation. Les organisations opérationnelles doivent évaluer de manière générale et continue les restrictions d'accès à leur environnement opérationnel.

Les ventilateurs mentionnés ci-dessus utilisent des systèmes d'exploitation spécialement renforcés. Toutefois, l'un des systèmes d'exploitation utilisés ne peut plus être mis à jour et ses vulnérabilités ne peuvent plus être corrigées. Par conséquent, elles ne sont pas préparées contre les cybermenaces dans la même mesure que les appareils plus récents. Cela inclut les cybermenaces effectuées avec un accès physique. Dräger fait donc les recommandations suivantes :

- Suivre les recommandations indiquées dans la notice d'utilisation :
    - Limiter ou contrôler l'accès physique aux ventilateurs mentionnés ci-dessus.
    - Ne pas connecter d'appareils non approuvés aux interfaces USB, LAN et DVI.
    - Être attentif aux notifications, alarmes et alertes.
- Penser à fermer/couvrir toutes les interfaces USB, LAN et DVI inutilisées.

Si vous souhaitez fermer/couvrir les interfaces non utilisées, Dräger propose de fournir gratuitement sur demande des outils pour fermer ou couvrir ces interfaces de données des ventilateurs. Le cas échéant, veuillez contacter votre organisation locale Dräger. Dans le cadre de l'utilisation prévue et autorisée des interfaces, les verrous USB et les couvercles d'interface peuvent être retirés à l'aide de clés ou d'outils appropriés.

Medibus et MedibusX, en tant que protocoles de communication série point à point sans fonctions de réseau, ne sont pas affectés et peuvent donc être utilisés en toute sécurité. Si vous utilisez les appareils mentionnés ci-dessus dans un réseau pour un service distant, veuillez contacter votre organisation locale Dräger.

Veuillez-vous assurer que tous les utilisateurs des appareils mentionnés et les autres personnes concernées de votre établissement sont informés de cette consigne importante de sécurité. Si vous avez fourni les appareils à des tiers, veuillez transmettre une copie du présent courrier. Les autorités compétentes ont été informées de cette action. Nous vous prions de bien vouloir accepter nos excuses pour les désagréments occasionnés, mais nous considérons qu'il s'agit d'une mesure préventive indispensable pour améliorer la sécurité des patients. Nous vous remercions de votre coopération.

Frank Ralfs
Senior Product Manager
Business Area Respiratory Care
Business Unit Therapy
Drägerwerk AG & Co. KGaA

Sonja Hillmer
Director Post Market Surveillance
Quality & Regulatory Affairs
Medical Division
Drägerwerk AG & Co. KGaA