Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

Vulnerability and Incident Reporting
product-security@draeger.com

**Dräger Product Security Advisory PSA-21-231-01 Update A**

**CVE-2021-22156 - BadAlloc Vulnerabilities in embedded operating system QNX**

**ICSA-21-119-04 Update C[1]**

**BfArM – "Kritische Schwachstellen in Echtzeitbetriebssystemen verschiedener Hersteller"[2]**

**>> Dräger Medical Devices are not affected by the "BadAlloc"-Series of Vulnerabilities.**

To whom it may concern,

In May, 2021, Dräger became aware of multiple similar Vulnerabilities in several Real-Time Operating Systems. These series of vulnerabilities has since become known under the name "BadAlloc". It is a memory corruption vulnerability, leading to possible Denial of Service or even Remote Code Execution on affected devices[3]. More information can be found in the industry alerts of the US Cybersecurity & Infrastructure Security Agency CISA[1,4], and the US Food and Drug Administration[5].

Of the affected real-time operating systems, Dräger is utilizing WindRiver's VxWorks in some of our devices.

[1] https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04

[2] https://www.bfarm.de/SharedDocs/Risikoinformationen/Medizinprodukte/DE/Schwachstellen_Echtzeitbetriebssysteme.html

[3] https://support.blackberry.com/kb/articleDetail?articleNumber=000082334

[4] https://us-cert.cisa.gov/ncas/alerts/aa21-229a

[5] https://www.fda.gov/drugs/information-industry-drugs/blackberry-qnx-cybersecurity-vulnerabilities-may-affect-drug-manufacturing-equipment

After thorough analysis, supported by the RTOS-vendor WindRiver, Dräger concluded that none of our devices utilizes any of the affected functions in an exploitable way. Thereby, Dräger medical devices are unaffected by the “BadAlloc”-Series of vulnerabilities.

For reporting incidents and potential vulnerabilities in our devices, please refer to https://static.draeger.com/security to contact the Product Security team directly.

Best regards,

Dräger Product Security

**Revisions**

| Version | Date | Change |
|---|---|---|
| **1** | 2021-08-19 | Initial Document |
| **2** | 2021-10-01 | Major Update of the advisory to reflect that Dräger is not affected by any of the BadAlloc security vulnerabilities. |

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