Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-21-348-2

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-21-348-2

Log4J Advisory

>> Dräger Medical Products (Devices and Software) are not affected by the Log4J Vulnerability

Legal Notice

This Product Security Advisory is based on all our findings that we had at the time of publication. However, the facts of the case are being reviewed on an ongoing basis and it is possible that this may result in changed assessments or that assessments contained in this advisory may turn out to be incorrect. We also reserve the right to change or revoke any recommendations. In addition, differences may result from the circumstances of the individual case on site. This information is naturally not available to us and has not been taken into account. Dräger can therefore accept no responsibility that the information presented here is conclusive or comprehensively correct for you. Therefore, please check carefully to what extent deviations can arise for your individual case. If necessary, you will be informed about new findings through following advisories.

1 Publication Date

2021-12-16

2 Overview

On December 10, 2021, Apache released a security advisory regarding a critical vulnerability in the Log4j Java logging utility[1]. The National Vulnerability Database (NVD) assigned the CVE ID CVE-2021-44228 to the vulnerability[2]. Cybersecurity & Infrastructure Agency (CISA) published an advisory recommending that customers to upgrade to Log4j 2.15.0 or apply recommended mitigations immediately[3].

[1] https://logging.apache.org/log4j/2.x/security.html
[2] https://nvd.nist.gov/vuln/detail/CVE-2021-44228
[3] https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce

None of the Dräger medical products or their accompanying infrastructure utilizes the affected Apache Log4j logging utility. Therefore, Dräger Medical Products (Devices and Software) are not affected by the Log4j vulnerabilities.

This advisory will be updated if there are new findings about Log4j that affect Dräger Medical Products.

The full text of this advisory can be accessed through https://static.draeger.com/security.

Revision History

VERSION	DATE	COMMENTS
1.0	2021-12-14	Initial Advisory
1.1	2021-12-16	Dräger medical devices replaced by Dräger Medical Products (Devices and Software)

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