Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-21-173-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-21-173-1

Dräger Clinical Assistance Package (CAP1) Security Vulnerabilities

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

2021-06-22

2 Overview

A security vulnerability was identified in the gSOAP library used by CAP1 devices. The vulnerability could allow a remote attacker to carry out a denial of service attack or possibly even to execute arbitrary code on the device.

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

3 Affected Products

The following Dräger products part of the CAP1 are affected by this vulnerability:

- Dräger CC300 Version 1.1.1
- Dräger IACS VG7.1/VG7.1.1
- Infinity Gateway VF9.0

4 How to verify if the product is affected

Dräger IACS and Infinity Gateway: Open the information screen on the device to review the software version. The software version is also displayed on the screen during device startup.

5 Vulnerability Description

Integer Overflow or Wraparound (CWE-190)
CVE-2020-13576

gSOAP contains an integer overflow condition in the WS-Addressing plugin's functionality. The issue is triggered as certain input is not properly validated. With a specially crafted SOAP HTTP request, a remote attacker can cause a buffer overflow, resulting in a denial of service or potentially allowing the execution of arbitrary code.

6 Impact

By sending a specially crafted SOAP HTTP request, a remote attacker can exploit this vulnerability which could cause the system to crash or execute malicious code on the system.

7 Severity

CVSS 3.1 Score

Base Score:	9.8
Severity:	High
Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

8 Remediation

The vulnerability is negligible since it will not result in an unacceptable risk to health for patients, users or bystanders. No action is required. In the course of a product improvement this vulnerability may be fixed in a future product release.

9 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.

10 Revision History

VERSION	DATE	COMMENTS
1.0	2021-06-22	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