Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-24-110-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-24-110-1

Dräger Core and Dräger M540 Converter Service vulnerable to specially crafted, unencrypted SDC messages

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

2024-04-22

2. Overview

Dräger proactively tests their products for vulnerabilities to strengthen their cyber resilience, not only during developement but also during a product's life cycle based on concurrent knowledge. During these activies Dräger found an unpublished, unknown vulnerability in gSOAP 2.8.131.

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

3. Affected Products

The following Dräger products are affected by this vulnerability:

- Core, version 1.0.5
- M540 Converter Service, version 1.0.9

4. Vulnerability Description

The vulnerability occurs when a specially crafted, unencrypted SDC message is received and processed during the discovery process. An attacker requires access to the hospital network and must be able to send data packets over it.

5. Impact

In the event of successful exploitation, the affected process will generate a high CPU load and further SDC messages will no longer be processed. An abuse of the vulnerability will become immediately apparent to users by the fact that vital parameters on the Core software application are no longer visualised. A restart of the service or the entire computer would remedy this condition.

6. Severity

Patient endangerment can be ruled out, as users can continue to retrieve the desired information from the primary monitor. It is ruled out that incorrect or outdated data will be displayed on the Core software application. The vulnerability cannot be exploited to make persistent changes on a computer. Other processes on a computer are only affected insofar as fewer CPU resources are available because a CPU core is under full load.

The computed CVSS 3.1 Scores are as follows

Base Score:	7.5
Severity:	High
Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

7. 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 will be fixed in the next product release.

Use of this document / contents is forbidden without express authority. All rights reserved. Refer to protection notice ISO 16016.
Printed copies are uncontrolled and for reference purposes only.

8. 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.

9. Revision History

Version	Date	Comments
1.0	2024-04-19	Initial Advisory

Use of this document / contents is forbidden without express authority. All rights reserved. Refer to protection notice ISO 16016.
Printed copies are uncontrolled and for reference purposes only.