Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-25-196-2

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-25-196-2

Intensive Care Manager (ICM) 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

2025-08-05

2. Overview

A security vulnerability was identified in the ICMHelper service running on the system of an ICM installation. This issue can only be taken advantage of by someone who already has access to the system. It could potentially let an attacker increase their privileges and run unauthorized commands on the system.

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

3. Affected Products

ICM installations with the affected ICMHelper version of 1.4.0.1 or older are affected.

4. How to verify if the product is affected

To verify if the product is affected, check the file version of the ICMHelperSvc.exe. The ICMHelper's default installation location is
"C:\Program Files (x86)\Draeger\ICMHelperSvc\ICMHelperSvc.exe".
Version 2.0.1.0 is the fixed version. All older executable versions are affected.

5. Vulnerability Description

The ICMHelperSvc service used to deploy and run ICM contains a vulnerability for a local privilege escalation.
The vulnerability CVE-2025-41698 allows an attacker to gain full access to application, sensitive information, client system and server. This requires successful exploitation of CVE-2025-2810.

6. Impact

The following is considered impact if a system is compromised through this vulnerability:

- Full Access To Application
- Full Access To Client System
- Full Access To Sensitive Information
- Full Access To Server

7. Severity

The CVSS 3.1 score for the vulnerability CVE-2025-41698 is rated as follows

Base Score: 7.8
Severity: High
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

The CVSS 3.1 score for the vulnerability registered as CVE-2025-2810 is rated as

Base Score: 5.5
Severity: Medium
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

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. Remediation

The issue has been fixed in ICMHelper version 2.0.1.0. Dräger Service will reach out to customers to schedule a date for the software update at no cost.

9. Credit

The vulnerability was discovered and reported by CODE WHITE GmbH. Thank you for helping us improving the cybersecurity of our products!

10. 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.

11. Revision History

Version	Date	Comments
1.0	2025-07-15	Initial Advisory
2.0	2025-08-05	Additional vulnerability details

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.