Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-25-349-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-25-349-1

Zeus IE and Zeus RS C500 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

2025-12-15

2. Overview

A cybersecurity vulnerability has been identified in the Zeus Infinity Empowered (Zeus IE) and Zeus RS C500 anesthesia workstations. An internal assessment penetration test revealed that the devices' USB interfaces could serve as a potential gateway for local attacks, particularly if the device is connected to a network. No reports of patient harm or successful exploitation have been received to date, and the devices' robust design and standard deployment practices reduce overall exposure.

3. Affected Products

- Zeus IE (MK04000)
- Zeus RS C500 (MK04666)

4. How to verify if the product is affected

All Zeus IE and Zeus RS C500 devices, regardless of networking status, are in scope. Devices operating with open USB interfaces, especially those connected to hospital networks or Dräger Service Connect, are at higher risk.

5. Vulnerability Description

If an unauthorized individual attains physical access to the device, the USB interface could potentially be manipulated to compromise software integrity or allow further network-based attacks. This risk is significantly mitigated by strong physical security controls and network segmentation in most customer environments.

6. Impact

If successfully exploited, an attacker could:

- Impair therapy functions.
- Potentially manipulate data processed by the device.
- Potentially use the device as a vector for broader network compromise.

7. Severity

The CVSS 3.1 score for this vulnerability is rated as follow

Base Score:	6.8
Severity:	Medium
Vector:	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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

For Networked Devices:

- Dräger will provide USB locks and re-install the device's base image to ensure software integrity. This intervention is mandatory for networked environments.
- USB interfaces will be locked; unlocking is possible only for approved use with designated keys.

For Non-Networked Devices:

- Upon request, Dräger provides USB locks.

All Customers:

- Follow the operating instructions and restrict physical access to devices.
- Do not connect non-approved hardware to USB, LAN, or DVI ports.
- Monitor system notifications and alarms.
- Close all unused USB interfaces where possible.

USB locks will be provided at no charge and will be accompanied by a supplement to the Instructions for Use

For instructions or to request USB locks, contact your local Dräger representative.

9. Contact Information

If you have any further questions related to the impact of the vulnerabilities, please contact your local Dräger representative. For reporting incidents and potential vulnerabilities in our devices, please refer to https://www.draeger.com/security to contact the Product Security team directly.

10. Revision History

Version	Date	Comments
1.0	2025-12-14	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.