Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-26-173-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-26-173-1

Dräger Atlan 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

2026-06-22

2. Overview

A set of cybersecurity vulnerabilities was identified in the Atlan anesthesia workstation family (models A300, A300XL, A350, A350XL) through regular penetration testing. The findings relate to network services, authentication, and data transmission. There is no indication these vulnerabilities have been exploited in clinical environments to date. This advisory communicates the potential risks, product impact, and recommended mitigation steps.

3. Affected Products

The following Dräger products part of the Atlan family with version 1.0n are affected by this vulnerability:

- Atlan A300 (8621300)
- Atlan A300XL (8621400)
- Atlan A350 (8621500)
- Atlan A350XL (8621600)

4. How to verify if the product is affected

Identify the Atlan device model and installed software version. Devices with Atlan software version 1.0n are in scope of this advisory. Devices without an ethernet connection cannot be exploited with respect to the vulnerabilities in scope of this advisory.

The issue has been fixed in Atlan software version 2.11.02.

5. Vulnerability Description

This advisory is published with respect to the combined exploitation of several vulnerabilities related to the following weaknesses:

- CWE-1391: Use of Weak Credentials
- CWE-284: Improper Access Control
- CWE-494: Download of Code Without Integrity Check

6. Impact

Atlan devices with Atlan software version 1.0n operating in networked environments can be impacted. A network attacker may gain full access to the device's software and data.

Please note: The only use case to connect Atlan devices to a network is an integration with a Service Connect Gateway (SCG).

7. Severity

CVSS Score: 8.1

Severity: High

Vector: CVSS:3.1/AV:N/AC:H/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

Dräger will contact affected customer sites using Atlan in combination with Service Connect Gateway (SCG) and provide a software update for Atlan, available and approved for the respective country.

Mandatory for networked devices:

- Update to Atlan device software version 2.11.02 or higher.
- Ensure vulnerable devices are disconnected from ethernet networks until they are updated.

All customers:

- Restrict network access to anesthesia workstations.
- Isolate devices on dedicated segments where possible.
- Apply strong physical and network security controls.
- Regularly monitor for unusual device activity.

Please feel free to contact your local Dräger service representative for update scheduling and further instructions, should you be affected and have not been contacted by Dräger directly. Devices running older software in networked scenarios must be updated as part of a Field Quality Improvement Action (FQIA).

9. Credit

N/A

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. Change log

Change notes
2026-06-22: Initial 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.