Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-26-180-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-26-180-1

Dräger Service Interface (DSI) Security Vulnerability

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

2026-06-29

2. Overview

A security vulnerability was identified in the Dräger Service Interface (DSI). The vulnerability could allow an attacker to spawn subprocesses from the DSI and execute arbitrary code via a specially forged link to the DSI server. All DSI versions prior to 1.56.3 are affected.

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

3. Affected Products

- Dräger Service Interface (DSI) all versions prior to 1.56.3

4. How to verify if the product is affected

The DSI version number can be found using one of the following methods:

- Right-click the DSI icon in the taskbar, open the connections window and check the version in the the bottom right corner.
- Open the ServiceConnect Desktop application page and review the listed DSI version.

If the installed version is lower than 1.56.3, the system is affected.

5. Vulnerability Description

CWE-20: Improper Input Validation

The Dräger Service Interface (DSI) server does not adequately validate request data provided by a browser. An attacker can craft a specially forged link and embed it in a webpage that, when processed by the DSI server, causes it to spawn subprocesses and execute arbitrary code in the context of the DSI application. No prior authentication or elevated privileges are needed by the attacker.

No CVE number has been assigned to this vulnerability.

6. Impact

Successful exploitation allows an attacker to execute arbitrary code with the privileges of the DSI process on the service technician's workstation. This could lead to full compromise of the workstation, unauthorized access to sensitive service data, and potential interference with Dräger devices connected during an active service session.

7. Severity

CVSS Score: 8.8

Severity: High

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/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

Update the Dräger Service Interface (DSI) to version 1.56.3 or later. The update is available via the ServiceConnect Desktop locally. If ServiceConnect Desktop is unavailable use ServiceConnect Desktop. Please contact your Dräger service representative for assistance locating and installing the update.

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
2026-06-17: 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.