Technology for Life

Dräger Safety AG & Co. KGaA, Revalstraße 1, 23560 Lübeck, Germany

Our reference
PSA-26-296-2

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-26-296-2

PHP Security Vulnerabilities in Dräger Safety Products (Update 1)

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

2026-10-27

2. Overview

On 2026-10-21 the PHP project disclosed two critical vulnerabilities (CVE-2026-109618 and CVE-2026-109619) that can allow unauthenticated remote code execution. These vulnerabilities are not specific to any Dräger product. Dräger has completed its investigation into which products may be affected.

3. Affected Products

The only product made by the Dräger Safety AG & Co. KGaA that is affected is the

Dräger REGARD 7000 OPC UA Server.

When the product is used as intended, the system is not at risk; nevertheless, Dräger is making a software update available and recommends installing it.

A separate advisory (PSA-26-295-2) for that product has been published and is kept up to date. The investigation has been completed; no further affected products were identified.

4. 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://draeger.com/security to contact the Product Security team directly.

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.