Technology for Life

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

Our reference
PSA-26-295-1

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-26-295-1

REGARD 7000 OPC UA Server 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

2026-10-22

2. Overview

On 2026-10-21 the PHP project published two critical vulnerabilities (CVE-2026-109618 and CVE-2026-109619) that can allow unauthenticated remote code execution. These vulnerabilities do not refer specifically to any Dräger product. Dräger is currently investigating whether the REGARD 7000 OPC UA Server is affected by them. This investigation has not yet been completed.

Irrespective of the outcome, the following applies: as explicitly stated in the security-related information of the instructions for use, “the OPC UA server has not been tested or approved for use in public networks”.

The REGARD 7000 is intended and approved exclusively for use in specially protected network environments. The reported vulnerabilities do not change this assessment.

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

3. Affected Products

Whether the Dräger REGARD 7000 OPC UA Server is affected by the vulnerabilities described below is currently under investigation and has not yet been confirmed.

4. How to verify if the product is affected

A definitive statement on whether the product is affected is not yet possible. This advisory will be updated once the investigation is complete.

5. Vulnerability Description

The following vulnerabilities were published by the PHP project on 2026-10-21 for the PHP runtime. They are not specific to any Dräger product; whether the REGARD 7000 OPC UA Server is affected is under investigation.

CVE-2026-109618 — RCE via OOM corruption

CVE-2026-109619 — RCE via stale global state

6. Impact

Should the product prove to be affected, successful exploitation could, depending on the configuration, allow an attacker to execute arbitrary code in the context of the affected process without prior authentication. Whether and to what extent this applies to the REGARD 7000 OPC UA Server is part of the ongoing investigation.

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.

7. Severity

Upstream (PHP project) classification:
Critical — unauthenticated remote code execution for both vulnerabilities:

CVSS 4.0 Score: 9.2 Critical

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

8. Remediation

The REGARD 7000 OPC UA Server is intended and approved exclusively for use in specially protected network environments. For intended operation within such an adequately protected network environment, Dräger currently sees no acute need for action; from Dräger's point of view, there is nothing to prevent continued operation in adequately protected networks.

Devices that have been improperly connected to a public network must be disconnected from such a network immediately.

Dräger continues to investigate whether the reported vulnerabilities are exploitable at all and will, where appropriate, develop and provide updated software. This advisory will be updated as soon as the assessment changes and/or updated software is made available.

9. Credit

The underlying vulnerabilities were proactively published by the PHP project.

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://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.