Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference

PSA-26-294-2

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory PSA-26-294-2

PHP2Shell Advisory (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

2026-10-30

2. Overview

On October 21, 2026, the PHP Group released security advisories regarding two critical vulnerabilities in the PHP language interpreter (php-src), together with the fixed releases PHP 8.2.35, 8.3.36, 8.4.27 and 8.5.12 [1][2][3]. The vulnerabilities were assigned the CVE IDs CVE-2026-109618 and CVE-2026-109619 [4][5]. They were reported by Wiz Research, Calif.io and OpenAI and were published under the name “PHP2Shell” [6]. The PHP Group states that updating PHP is the only complete mitigation.

Dräger has assessed its medical devices, such as ventilators, anaesthesia workstations, patient monitors and neonatal care devices, as well as Dräger's medical software products for these vulnerabilities. None of them are affected, because they do not use PHP.

The assessment of all Dräger Service products has been completed. The assessment includes Dräger cloud solutions on my.draeger.com, other internet-connected solutions, as well as remote service tools. None of the products assessed are affected by these vulnerabilities, as they do not use PHP.

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

[1] https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
[2] https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
[3] https://www.php.net/ChangeLog-8.php
[4] https://nvd.nist.gov/vuln/detail/CVE-2026-109618
[5] https://nvd.nist.gov/vuln/detail/CVE-2026-109619
[6] https://www.wiz.io/blog/php2shell-php-rce

3. 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.

4. Change log

Version	Date	Change notes
PSA-26-294-1	2026-10-23	Initial Advisory
PSA-26-294-2	2026-10-30	Updated statement after assessment completion

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.