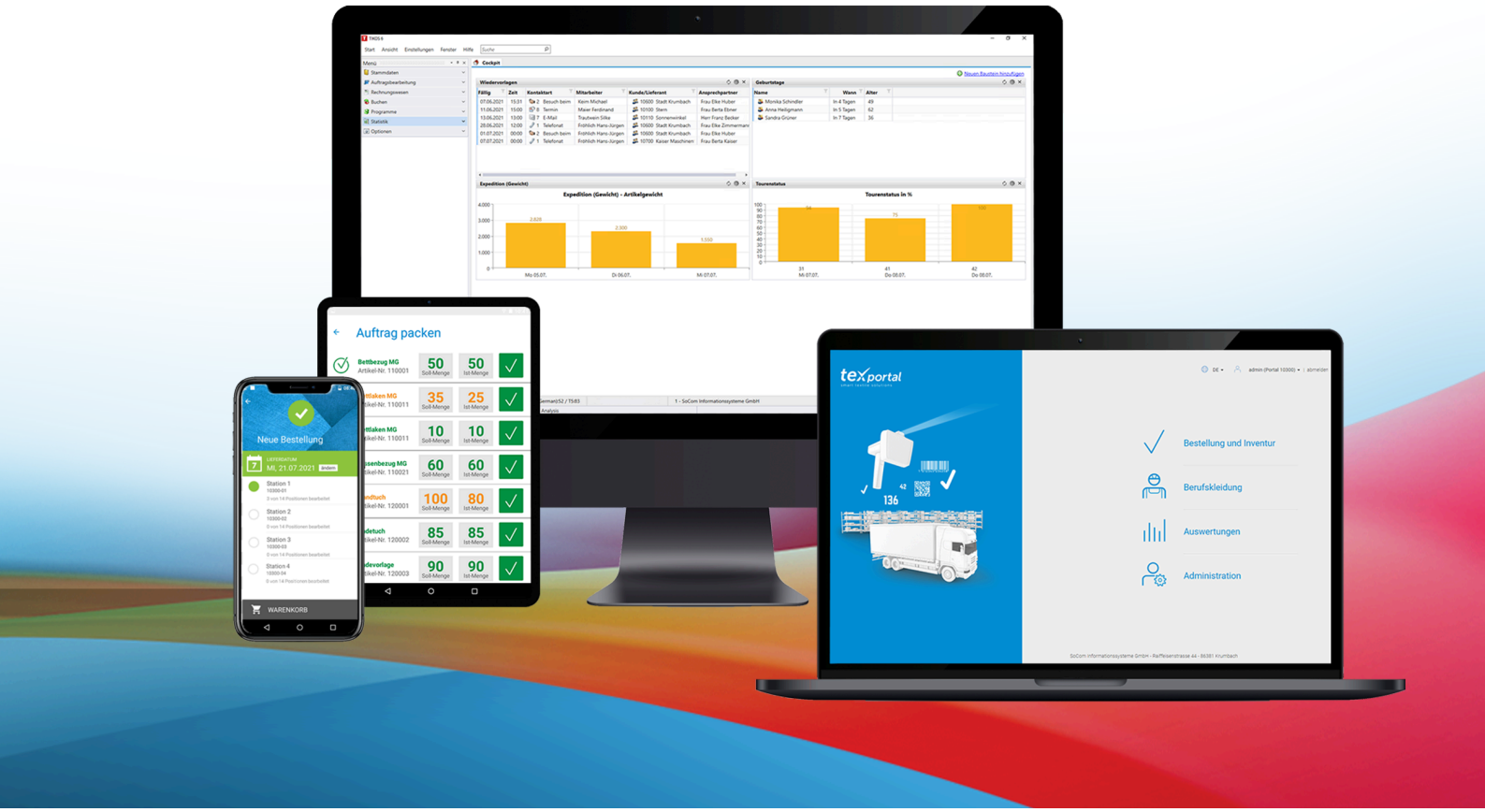
WEB & APP
ONLINE & MOBILE SOLUTIONS

Security advisory SOCOM-2026-002



Copyright © SoCom Informationssysteme GmbH 2026, All rights reserved
security@socom.de | socom.de/security

socom.de

SoCom SECURITY ADVISORY

Critical PHP vulnerabilities (“PHP2Shell”) affect texPortal and texApps

Severity	Critical, CVSS v4.0: 9.2
CVE	CVE-2026-109618, CVE-2026-109619
Published	2026-11-05
Last updated	2026-11-05

Affected product

texPortal, all releases, and with it the server side of the texApps texRoute, texOrder, texEasyPick, texScan and texUniScan. The texRepair app is not affected.

- texPortal 2024.1 and later (Docker): The PHP runtime is part of the Docker image we ship, PHP 8.3 up to release 2025.2, PHP 8.4 from release 2026.1.
- texPortal before 2024.1: The PHP runtime is provided by the operator of the server.

Fixed in

texPortal	PHP in image	Fixed from
2024.1	8.3.36	texPortal image, builds from 2026-10-22
2025.1	8.3.36	texPortal image, builds from 2026-10-22
2025.2	8.3.36	PHP image `php:8.3-2025.2`, made available on 2026-10-22
2026.1	8.4.27	PHP image `php:8.4`, made available on 2026-10-22
2026.2	8.4.27	PHP image `php:8.4-2026.2`, made available on 2026-10-22

For installations before 2024.1 the fix comes from the PHP project: PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35, plus backported fixes for PHP 7.4, 8.0 and 8.1. There is no fix for PHP 7.3 and older.

Description

On 21 October 2026 the PHP project fixed two vulnerabilities in the PHP runtime. They affect all PHP versions and every installation that processes web requests. They are triggered while a request is processed, before any application code runs, and require no authentication.

texPortal is a PHP application. The vulnerabilities are not in texPortal’s code but in the runtime it runs on.

Impact

An unauthenticated attacker can execute code on the server over the internet, with the privileges of the PHP process. This exposes the portal’s data and, depending on the network layout, other systems.

Remediation

Copyright © SoCom Informationssysteme GmbH 2026, All rights reserved

WEB ONLINE SOLUTIONS

texPortal 2024.1 and later (Docker)

Apply the corrected image; no change of texPortal release is required. Portals hosted by us have already been updated. For installations on your own server, our support or your IT service provider applies it with the update command of the setup script.

texPortal before 2024.1 (without Docker)

Update PHP on your server to one of the fixed versions above and restart the web server or PHP-FPM. If PHP comes from your Linux distribution's package manager, its security advisory applies. texPortal itself does not need to be updated.

Note: With PHP 7.3 or older this is not possible. Disconnect the server from the internet and move to a current texPortal release with us.

How to verify that the fix is in place

- Docker: In the texPortal folder, `docker compose exec texportal php -v` reports 8.3.36 or 8.4.27 or later.
- Without Docker: `php -v` reports one of the fixed versions, or your distribution confirms the fixed package version.

Workaround

None that is reliable. The settings published by the PHP project reduce the attack surface without closing it and can restrict portal functions. Until the fix is applied, only disconnecting the server from the internet protects it. Please contact us before changing settings.

Credit

Published by the PHP project on 21 October 2026. Third parties report exploitation. We are not aware of any exploitation at our installations.

Timeline

Date	Step
2026-10-21	Fixes published by the PHP project
2026-10-21	Update of the servers we host without Docker started
2026-10-22	Affected customers informed, notification to BSI (CERT-Bund)
2026-10-22	Corrected Docker images made available
2026-10-22	Portals hosted by us updated
2026-11-05	This advisory published

Contact

To report a vulnerability in our products: security@socom.de. Our policy for handling such reports: socom.de/security.

Copyright © SoCom Informationssysteme GmbH 2026, All rights reserved

WEB ONLINE SOLUTIONS