

PHP2Shell vulnerabilities

Security information from COBS

COBS AB | 27 October 2026

Affected systems, product status and actions for the customer

1 About this information

This information is aimed at customers with systems delivered by COBS and refers to the PHP vulnerabilities that are referred to in the documentation as PHP2Shell: **CVE-2026-109618 and CVE-2026-109619**. The purpose is to describe which systems may be affected and what measures may be needed in the customer's installation.

The information is based on COBS's product documentation and reproduced supplier statements. The assessment only applies to the specified vulnerabilities and is not a general statement about the security of the systems. The installed product, software version and any add-ons need to be checked for each installation. The main document covers affected products. Other product statements and delimitations can be found in Appendix A.

- **COBS CMS:** Affected according to COBS documentation. Update needs to be planned.
- **Zenitel ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE and Exigo:** Specified versions are affected. Please restrict administration access and take product-specific actions as set out below.

Background: According to the security notice, the PHP project made the vulnerabilities public on October 21, 2026. Both are classified as critical with CVSS v4.0 9.2 out of 10 and relate to errors in PHP's memory management. They can enable remote code execution without authentication via an accessible PHP-based web interface, with the web server process permissions. Exploitation, according to the release, is complex and dependent on the configuration of the web server. At the time of this publication, COBS is not aware that any exploitation has taken place in these products.

1.1 Product status and customer actions

1.1.1 COBS CMS

Status: Affected. The COBS CMS needs to be updated to fix the listed vulnerabilities.

Action for customer: Security update to software version **v4.05** CMS III and CMS IV is now available on the COBS Support Portal for download as of 2026-10-27. Older and deprecated CMS systems (I & II) need to be replaced with new CMS IV MkII.

1.1.2 Zenitel

Status: Specified products and versions are affected. Zenitel's Security Notice A100K12410, Revision 1.0, dated October 23, 2026, covers ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE and Exigo (system controllers ICX-500, ICX-510 and ESC1 including AMC-IP). Version limits

and actions are set out below. The update dates in the announcement were planned dates, not confirmations of published updates. Actual availability needs to be confirmed with COBS or Zenitel.

Product family	Affected versions	Action status as per the message
ICX-AlphaCom	All versions up to and including 1.5.3.7	Security update in development; planned for 2026-10-23. Confirm availability. Restrict administration access immediately.
ICX-AlphaCom Core	All versions up to and including 1.5.3.7 on Ubuntu 22.04 LTS	Fixed PHP packages are available as announced via Ubuntu: php8.1 8.1.2-1ubuntu2.28 or later (USN-8948-1). Install the Ubuntu security update as soon as possible.
AlphaCom XE	All versions up to and including 13.2.3.16	Enforce permanent network restrictions. No corrected PHP version is listed as available for this platform.
Exigo	All versions up to and including 1.7.3.7 All versions up to and including 2.0.3.1	Security update for Exigo system controllers under development; planned by 2026-10-26. For ESC1 including AMC-IP, only network restrictions are listed as available action. See below.

Joint actions for affected Zenitel products: Restrict HTTP/HTTPS access to the web-based administration interface to trusted administration networks and administrators' workstations, with firewall rules and separate administration VLANs. Do not expose the interface to the internet or untrusted networks. Use VPN or equivalent authenticated and encrypted connection for remote administration. Control unexpected web interface reboots, configuration changes, and user accounts. Report suspicious activity to Zenitel's product security feature, security@zenitel.com.

1.1.2.1 ICX-AlphaCom

Affected versions: All versions up to and including 1.5.3.7.

Action for customer: Apply the common network restrictions immediately and install Zenitel's security update when available. The message indicates a planned update on October 23, 2026, but does not confirm publication or corrected product version number. Please contact COBS to confirm the available version and update path. The Ubuntu fix in the next section applies to ICX-AlphaCom Core.

1.1.2.2 ICX-AlphaCom Core

Affected versions: All versions up to and including 1.5.3.7 running on Ubuntu 22.04 LTS.

Action for customer: Install Ubuntu security update USN-8948-1 in the virtual machine as soon as possible. Zenitel specifies version 8.1.2-1ubuntu2.28 or later for affected PHP 8.1 packages: libapache2-mod-php8.1, php8.1-cgi, php8.1-cli, and php8.1-fpm. PHP is provided by Ubuntu and is not updated through ICX-AlphaCom Core versions. The customer is responsible for keeping the virtual machine's Ubuntu operating system up to date. Coordinate with the responsible operating organization and also enforce the common network restrictions.

1.1.2.3 AlphaCom XE

Affected versions: All versions up to and including 13.2.3.16.

Action for customer: Permanently apply the common network restrictions. According to

Zenitel's announcement, PHP 5.6.38 is used, for which no corrected version was available at the time of publication. Network restrictions are listed as the only available risk mitigation measure.

Continued handling: Zenitel recommends planning migration from AlphaCom XE to ICX-AlphaCom. Contact COBS for installation-specific planning.

1.1.2.4 Exigo

Affected versions: All versions up to and including 1.7.3.7 and 2.0.3.1 respectively according to Zenitel's product table.

Action for customer: Apply the common network restrictions promptly. For Exigo system controllers, the announcement indicates a security update in development, with planned availability by October 26, 2026. The date is not an acknowledgement of publication; check current availability and the correct update path with COBS or Zenitel.

ESC1 including AMC-IP: These are listed separately using PHP 5.6.38 without an available patched version at the time of publication. For these, network restrictions are specified as the only available measure and they are to be applied permanently. Do not assume that the planned Exigo update will cover these devices without product-specific confirmation.

1.1.2.5 Other Zenitel products

According to Zenitel's Security Notice A100K12410, Revision 1.0, dated October 23, 2026, no Zenitel products other than the product families and system controllers listed in the Zenitel section of the main document are affected. The notice applies only to the two listed PHP vulnerabilities.

Contact and continued management

If you are unsure about which products or versions are included in your installation, contact COBS. Please state the facility, product designation and installed software version so that the correct action can be determined. Updates and network changes should be coordinated with the responsible operating organization and COBS to take into account the installation's function and availability.

COBS AB

Phone: +46 (0)31-33 33 840

E-mail: support@cobs.se

2 Appendix A – Other IP-based products and delimitations

It gathers products that are not affected according to existing documentation as well as information with exceptions or the need for a separate assessment. The information only applies to CVE-2026-109618 and CVE-2026-109619. The fact that a component is not affected does not mean that the entire interconnected system is unaffected.

2.1 COBS Alert4U2 – A-TRAX IP

Status: Not affected. A-TRAX IP transmitters and receivers do not use PHP.

Action for customer: No action is required on these components due to the vulnerabilities listed. If the installation also includes the COBS CMS, the actions in the CMS section apply to that part of the system.

2.2 Moxa NPort

Status: Not affected. Moxa states that none of the company's products are affected by these vulnerabilities.

Action for customer: No action is required on Moxa NPort due to the listed vulnerabilities.

2.3 Modbus-related products

Status: Not affected. states that none of the company's products are affected by these vulnerabilities.

Action for customer: No action is required on Modbus-related devices due to the specified vulnerabilities.

2.4 Funktel Nucleus

Status: Not affected. PHP is not installed by default on the Nucleus platform and is not used by Nucleus.

Action for customer: No action is required for Nucleus in standard design due to these vulnerabilities. The notice does not cover any separately installed PHP software.

2.5 COBS MOBILE

Status: Not affected. These platforms do not use PHP.

Action for customer: No action is required for these platforms due to the vulnerabilities listed.

2.6 COBS CWS DECT

Status: Not affected. Neither DECT systems, including the AMIE administration interface for DECT use PHP.

Action for customer: No action is required for these products due to the listed vulnerabilities. Any connected COBS CMS needs to be assessed separately.

2.7 2N

Status: Not affected. The vendor states that an internal analysis has confirmed that no 2N products are affected by the stated vulnerabilities.

Action for customer: No action is required for 2N's products and solutions due to these vulnerabilities.

2.8 Innovaphone

Status: Not affected, with the exception of legacy v10 App Platform. Innovaphone states that the products do not use PHP, except for the older v10 App Platform which is no longer supported. The announcement that the products are not affected should therefore not be applied to this older platform.

Action for customer: No action is required for the products covered by the PHP non-use notification. v10 App Platform customers should contact COBS for separate assessment and further management.

Provider's services: Innovaphone states that some of its own services were affected and that websites were taken down pending updating. Operational information is referred to status.innovaphone.com.