Technical Bulletin

Zenitel Security Notice

TLP:CLEAR — unlimited distribution. Recipients may share this notice without restriction (FIRST TLP 2.0). No additional sharing restrictions apply.

2026-10-28

Document No.: A100K12410 • **Revision:** 1.1

Products Affected: ICX-AlphaCom; ICX-AlphaCom Core; AlphaCom XE, Exigo (System Controllers: ICX-500, ICX-510, ESC1 including AMC-IP).

Note! No other Zenitel products are impacted.

Fix status: ICX-AlphaCom: fixed in 1.5.3.8 — see Zenitel Security Advisory A100K12411. Exigo ICX-500 and ICX-510: fixed in 1.7.3.8 (1.x release line) and 2.0.3.2 (2.x release line) — see Zenitel Security Advisory A100K12412. ICX-AlphaCom Core: PHP is provided by Ubuntu 22.04 LTS, not by Zenitel — fixed Ubuntu packages are available (USN-8948-1); apply the Ubuntu security update now. AlphaCom XE and Exigo ESC1 including AMC-IP: mitigating action defined; no security update available.

Summary

On 21 October 2026 the PHP project disclosed two critical vulnerabilities in the PHP runtime (CVE-2026-109618 and CVE-2026-109619) that may allow an unauthenticated network attacker to execute code on a system that serves PHP web requests. ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE and Exigo System Controllers use PHP in their web-based management interface and are affected; see the table below for the affected versions and fix status. Zenitel is not aware of any exploitation of these vulnerabilities in Zenitel products; both vulnerabilities were, however, added to the CISA Known Exploited Vulnerabilities catalogue on 26 October 2026, confirming active exploitation of PHP installations in the wild. Security updates are now available: ICX-AlphaCom 1.5.3.8 (Zenitel Security Advisory A100K12411) and, for the Exigo ICX-500 and ICX-510 System Controllers, Exigo 1.7.3.8 and 2.0.3.2 (Zenitel Security Advisory A100K12412). ICX-AlphaCom Core runs on Ubuntu 22.04 LTS and uses the PHP packages provided by Ubuntu: Canonical has released fixed packages, and Zenitel urges users to apply the Ubuntu security update immediately. For AlphaCom XE and Exigo ESC1 including AMC-IP, no security update is available; Zenitel has defined mitigating action. Users of all affected products should install the applicable security update or apply the risk mitigations below.

Affected Products

Product family	Affected versions	Fix status
ICX-AlphaCom	All versions up to and including 1.5.3.7	Fixed in 1.5.3.8 — see Zenitel Security Advisory A100K12411

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

Product family	Affected versions	Fix status
ICX-AlphaCom Core	All versions up to and including 1.5.3.7, running on Ubuntu 22.04 LTS	Fixed PHP packages available from Ubuntu (php8.1 8.1.2-1ubuntu2.28, USN-8948-1) — apply the Ubuntu security update
AlphaCom XE	All versions up to and including 13.2.3.16	Apply mitigations
Exigo (ICX-500, ICX-510)	1.x: all versions up to and including 1.7.3.7 2.x: all versions up to and including 2.0.3.1	Fixed in 1.7.3.8 (1.x) / 2.0.3.2 (2.x) — see Zenitel Security Advisory A100K12412
Exigo ESC1 (including AMC-IP)	All versions up to and including 13.0.3.17	Apply mitigations

Nature of the Issue

The vulnerabilities are in the PHP runtime itself, an open-source component used by the web-based management interface of ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE and Exigo System Controllers; they are not in code written by Zenitel. Both were published by the PHP project on 21 October 2026 and are rated Critical (CVSS v4.0 base score 9.2 each; both are use-after-free memory-safety flaws). According to the PHP project, all PHP versions from PHP 5 onward are affected; fixes are available only in PHP 8.2.35, 8.3.36, 8.4.27 and 8.5.12 (with source-level backports for 7.4, 8.0 and 8.1). ICX-AlphaCom and Exigo System Controllers ship PHP 8.2.31. ICX-AlphaCom Core runs inside a virtual machine on Ubuntu 22.04 LTS and uses the PHP 8.1 packages provided by Ubuntu, not PHP shipped by Zenitel; Canonical has released fixed packages (php8.1 8.1.2-1ubuntu2.28). AlphaCom XE and Exigo ESC1 including AMC-IP ship PHP 5.6.38, for which no fixed version exists at the time of writing.

- CVE-2026-109618 — incorrect handling of out-of-memory conditions while a request is being set up can leave request data partly initialised; the subsequent clean-up may then act on invalid memory state.
- CVE-2026-109619 — state belonging to a finished request can be retained by a PHP worker process after its memory has been released, and accessed by a later request before it is re-initialised.

Both vulnerabilities can be triggered by specially crafted HTTP requests to the PHP-based web interface without authentication and before any application code runs. Successful exploitation results in code execution with the privileges of the web server process. The PHP project rates the attack as complex and dependent on the web server configuration (CVSS attack complexity High, attack requirements Present); Zenitel is analysing which of the published conditions apply to the ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE and Exigo System Controllers configurations. No further technical detail is provided in this notice.

Exploitation Status

Zenitel is not aware of any exploitation of these vulnerabilities in Zenitel products as of the publication date of this notice. Exploitation of PHP installations in general is, however, confirmed: on 26 October 2026 the U.S. Cybersecurity and Infrastructure Security Agency (CISA) added both CVE-2026-109618 and CVE-2026-

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

109619 to its Known Exploited Vulnerabilities (KEV) catalogue on the basis of evidence of active exploitation, and security researchers have reported successful exploitation of unpatched, internet-exposed PHP installations (predominantly CVE-2026-109618 on Apache mod_php deployments), with large-scale exploitation attempts observed worldwide. An attacker needs network access (HTTP/HTTPS) to the web-based management interface of an affected product; no credentials and no user interaction are required. Zenitel will update this section if the status changes.

Risk Mitigation and Recommended User Actions

- Restrict network access to the ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE and Exigo System Controllers web-based management interface to trusted management networks and administrator workstations (firewall rules, management VLAN). Do not expose the web-based management interface to the internet or to untrusted networks.
- Where remote administration is required, provide it through a VPN or an equivalent authenticated, encrypted access path rather than by direct exposure of the web-based management interface.
- Review ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE and Exigo System Controllers systems for signs of unexpected activity — unexplained restarts of the web-based management interface, unexpected configuration changes or user accounts — and report anything suspicious to Zenitel product security (see Contact).
- ICX-AlphaCom: upgrade to version 1.5.3.8 or a later release (Zenitel Security Advisory A100K12411).
- ICX-AlphaCom Core: apply the Ubuntu 22.04 LTS security update for PHP (USN-8948-1 — libapache2-mod-php8.1, php8.1-cgi, php8.1-cli and php8.1-fpm version 8.1.2-1ubuntu2.28 or later) on the virtual machine as soon as possible; a standard system update installs it. Keeping the Ubuntu operating system of the ICX-AlphaCom Core virtual machine updated is the user's responsibility, and PHP is not updated by ICX-AlphaCom Core releases.
- Exigo ICX-500 and ICX-510 System Controllers: upgrade to Exigo 1.7.3.8 (1.x release line) or 2.0.3.2 (2.x release line), or a later release (Zenitel Security Advisory A100K12412).
- AlphaCom XE and Exigo ESC1 including AMC-IP: the network restrictions above are the only available mitigation and should be applied permanently. Zenitel recommends planning migration of AlphaCom XE installations to ICX-AlphaCom; contact your Zenitel partner or Zenitel Customer Support for migration options.

Zenitel's Actions and Fix Status

Zenitel has confirmed that ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE and Exigo System Controllers include affected PHP versions and has treated this issue with the highest priority. For ICX-AlphaCom and the Exigo ICX-500 and ICX-510 System Controllers, Zenitel has:

- Released ICX-AlphaCom 1.5.3.8, which upgrades PHP to a fixed release, and published Zenitel Security Advisory A100K12411 (2026-10-23).
- Released Exigo 1.7.3.8 (1.x release line) and 2.0.3.2 (2.x release line), which upgrade PHP to a fixed release, and published Zenitel Security Advisory A100K12412 (2026-10-27).

The security advisories are published at https://www.zenitel.com/security/security-advisories (see References). For ICX-AlphaCom Core, PHP is part of the Ubuntu 22.04 LTS operating system of the virtual machine and is not shipped or updated by Zenitel; the fix is delivered by Canonical through the Ubuntu security update (USN-8948-1), which users apply themselves. For AlphaCom XE and Exigo ESC1 including

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

AMC-IP, the fixed PHP releases published by the PHP project do not cover the PHP version they use. Zenitel is assessing whether any additional configuration guidance can be provided for AlphaCom XE and Exigo ESC1 including AMC-IP, and will include it in the next update of this notice.

Next Update

Zenitel will update this notice if material new information becomes available — in particular if exploitation in Zenitel products becomes known, or if additional guidance for AlphaCom XE and Exigo ESC1 including AMC-IP becomes available.

References

- PHP project security advisory GHSA-w8hw-w9fx-j79w (CVE-2026-109618): https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
- PHP project security advisory GHSA-6wmf-4rv5-p3rp (CVE-2026-109619): https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
- CERT-EU Security Advisory 2026-018, Critical Vulnerabilities in PHP: https://cert.europa.eu/publications/security-advisories/2026-018
- Ubuntu Security Notice USN-8948-1, PHP vulnerabilities (fixed packages for Ubuntu 22.04 LTS): https://ubuntu.com/security/notices/USN-8948-1
- Ubuntu php8.1 package 8.1.2-1ubuntu2.28 (Launchpad): https://launchpad.net/ubuntu/+source/php8.1/8.1.2-1ubuntu2.28
- CISA Known Exploited Vulnerabilities catalogue (CVE-2026-109618 and CVE-2026-109619 added 2026-10-26): https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Zenitel Security Advisory A100K12411 — ICX-AlphaCom, fixed in 1.5.3.8: https://zenitel.com/sites/default/files/2026-10/A100K12411-Zenitel-Security-Advisory.pdf
- Zenitel Security Advisory A100K12412 — Exigo ICX-500 and ICX-510 System Controllers, fixed in 1.7.3.8 / 2.0.3.2: https://www.zenitel.com/sites/default/files/2026-10/A100K12412-Zenitel-Security-Advisory.pdf

Contact

Questions about this notice, or new vulnerability reports, can be directed to Zenitel product security: security@zenitel.com. Our coordinated vulnerability disclosure policy is published at https://www.zenitel.com/security/vulnerability-disclosure (see also https://www.zenitel.com/.well-known/security.txt). Customers may also contact Zenitel Customer Support through their usual channel.

Stay Informed

This notice is distributed by e-mail and is also published in the Zenitel library at https://zenitel.com/library. The security advisories for the released updates (A100K12411, A100K12412) are published at https://www.zenitel.com/security/security-advisories.

Revision History

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

Revision	Date	Description
1.0	2026-10-23	Initial publication.
1.1	2026-10-28	Security updates released: ICX-AlphaCom 1.5.3.8 (Zenitel Security Advisory A100K12411) and Exigo 1.7.3.8 / 2.0.3.2 for the ICX-500 and ICX-510 System Controllers (Zenitel Security Advisory A100K12412); fix status, user actions and Zenitel's actions updated accordingly. Exigo ESC1 (including AMC-IP) listed separately in the Affected Products table. CISA KEV listing of both CVEs (2026-10-26) added to Summary and Exploitation Status. Advisory references added.

Terms of Use and Distribution

This notice is marked TLP:CLEAR (FIRST Traffic Light Protocol, version 2.0): recipients may distribute it without restriction, subject to standard copyright rules. It is provided “as is”, without warranty of any kind; Zenitel assumes no responsibility for errors in this publication or for damages arising from the information herein, and may revise this notice as new information becomes available. Updated versions of this notice are distributed through the same e-mail channels.

Zenitel Group

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided “as is” without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.