Technical Bulletin

Zenitel Security Advisory

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

2026-10-27

Document No.: A100K12412 • **Revision:** 1.0

Products Affected: Exigo (System Controllers: ICX-500, ICX-510)

Summary

Zenitel has resolved two critical vulnerabilities in PHP, a third-party open-source component used by the web-based management interface of the Exigo System Controllers (ICX-500, ICX-510). The vulnerabilities, CVE-2026-109618 and CVE-2026-109619, were disclosed by the PHP project on 21 October 2026 and could allow an unauthenticated network attacker to execute code on the affected system with the privileges of the web server process. Exigo 1.7.3.8 (1.x release line) and 2.0.3.2 (2.x release line) contain the fixes; all earlier versions are affected. Zenitel is not aware of any exploitation of these vulnerabilities in Zenitel products. Systems already running the fixed versions listed in the table below, or later, require no action. This advisory supersedes, for the Exigo ICX-500 and ICX-510 System Controllers, Zenitel Security Notice A100K12410 of 2026-10-23, which was distributed by e-mail before the fix was available; that notice remains in force for Exigo ESC1 (including AMC-IP) and AlphaCom XE, for which no security update is available. The same vulnerabilities in ICX-AlphaCom are addressed in Zenitel Security Advisory A100K12411.

Affected Products and Fixed Versions

Product family	CVE ID	Affected versions	Fixed in
Exigo (ICX-500, ICX-510)	CVE-2026-109618 CVE-2026-109619	1.x: all versions up to and including 1.7.3.7 2.x: all versions up to and including 2.0.3.1	1.7.3.8 (1.x) 2.0.3.2 (2.x)

Resolved Vulnerabilities

CVE ID	Description	Impact	CVSS	Severity	Fixed in
CVE-2026-109618	Use-after-free in the PHP runtime (versions before 8.2.35) caused by	Remote code execution with the privileges of the web server	9.2 (v4.0)	Critical	1.7.3.8 (1.x) / 2.0.3.2 (2.x)

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.

CVE ID	Description	Impact	CVSS	Severity	Fixed in
	incorrect handling of out-of-memory conditions while a request is being set up, leaving request data partly initialised; reachable through the web-based management interface of the Exigo System Controllers by an unauthenticated network attacker using crafted HTTP requests.	process; loss of confidentiality, integrity and availability of the affected system.			
CVE-2026-109619	Use-after-free in the PHP runtime (versions before 8.2.35): state belonging to a finished request is retained by a PHP worker process after its memory has been released and can be accessed by a later request before re-initialisation; reachable through the web-based management interface of the Exigo System Controllers by an unauthenticated network attacker using crafted HTTP requests.	Remote code execution with the privileges of the web server process; loss of confidentiality, integrity and availability of the affected system.	9.2 (v4.0)	Critical	1.7.3.8 (1.x) / 2.0.3.2 (2.x)

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.

Note: Severity ratings use CVSS v4.0; CVSS v3.1 is used where a v4.0 score is not available (first.org/cvss). The CVSS version is stated with each score. Each CVE ID above links to its authoritative CVE Record at cve.org.

Vulnerability Details

CVE-2026-109618 — Remote code execution via out-of-memory handling in PHP

Description: Use-after-free in the PHP runtime: PHP aborts a request on an out-of-memory condition without accounting for request data that is only partly initialised, and request shutdown may then act on invalid memory state. The condition can be triggered by crafted HTTP requests to the web-based management interface of an Exigo System Controller without authentication and before any application code runs. Affects PHP versions before 8.2.35; Exigo versions up to and including 1.7.3.7 (1.x) and 2.0.3.1 (2.x) ship PHP 8.2.31.

Impact: Unauthenticated remote code execution with the privileges of the web server process (high impact on confidentiality, integrity and availability). The attack is rated as complex by the PHP project and its success depends on the web server configuration and memory limits.

CVSS: 9.2 (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) — score and vector as published by the PHP project for the component vulnerability.

CVE-2026-109619 — Remote code execution via stale request state in PHP

Description: Use-after-free in the PHP runtime: a PHP worker process can retain global state (error, session, object and extension state) that points to memory owned by a request that has already finished; certain operations performed before normal request initialisation read that stale state. Reachable by crafted HTTP requests to the web-based management interface of an Exigo System Controller without authentication; a producing and a consuming request must be handled by the same worker process. Affects PHP versions before 8.2.35; Exigo versions up to and including 1.7.3.7 (1.x) and 2.0.3.1 (2.x) ship PHP 8.2.31.

Impact: Unauthenticated heap use-after-free leading to memory disclosure and remote code execution with the privileges of the web server process (high impact on confidentiality, integrity and availability). The attack is rated as complex by the PHP project; multiple worker processes reduce but do not eliminate the likelihood of success.

CVSS: 9.2 (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) — score and vector as published by the PHP project for the component vulnerability.

Exploitation Status

Zenitel is not aware of any exploitation of these vulnerabilities in Zenitel products as of the publication date of this advisory. The vulnerabilities were disclosed by the PHP project, not reported to Zenitel; at disclosure the PHP project stated that a working exploit existed for at least one common PHP deployment configuration, and exploitation attempts against PHP installations on the internet have been reported publicly. Attacker preconditions for both vulnerabilities: network access (HTTP/HTTPS) to the web-based management interface of an affected product; no credentials and no user interaction are required.

Mitigation and Customer Actions

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.

- Upgrade all Exigo System Controllers to version 1.7.3.8 (1.x release line) or 2.0.3.2 (2.x release line), or a later release.
- Systems that cannot be upgraded immediately: restrict network access to the web-based management interface of the affected product to trusted management networks and administrator workstations (firewall rules, management VLAN), do not expose it to the internet or untrusted networks, and provide any remote administration through a VPN or an equivalent authenticated, encrypted access path.
- If the web-based management interface was reachable from untrusted networks before the upgrade, review the system for unexpected configuration changes or user accounts and contact Zenitel product security if compromise is suspected.

Verifying Update Authenticity

Exigo software update packages are digitally signed, and the signature is verified before installation; a package that fails verification is rejected and is not installed. Obtain software updates only from Zenitel's official distribution channels.

References

- Exigo 1.7.3.8 release notes: https://wiki.zenitel.com/wiki/Exigo_1.7_Release_Notes
- Exigo 2.0.3.2 release notes: https://wiki.zenitel.com/wiki/Exigo_2.0_Release_Notes
- 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
- Zenitel Security Notice A100K12410, critical vulnerabilities in PHP (2026-10-23; distributed by e-mail; superseded for Exigo ICX-500/ICX-510 by this advisory, remains in force for Exigo ESC1 including AMC-IP and AlphaCom XE)
- Zenitel Security Advisory A100K12411 — the same vulnerabilities in ICX-AlphaCom (fixed in 1.5.3.8): https://www.zenitel.com/security/security-advisories

Contact

Questions about this advisory, 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

Zenitel publishes all security advisories at https://www.zenitel.com/security/security-advisories — this page is the authoritative source for the current version of this document.

Future Hardening Measures

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.

Zenitel continues to enhance its secure development practices, proactively scans software prior to release, and takes immediate action when vulnerabilities are identified. Cybersecurity remains a core priority throughout our software lifecycle and product design.

Revision History

Revision	Date	Description
1.0	2026-10-27	Initial publication.

Terms of Use and Distribution

This advisory 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 advisory as new information becomes available. Always obtain the current version from the Zenitel security advisories page.

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.