zenitel

Technical Bulletin

Zenitel Security Advisory

To : All Zenitel Offices & Partners

19 Dec 2025

Products Affected: VS-IS/ICX-AlphaCom/Alphacom XE
Firmware status: Fixed in VS-IS v9.3.3.1 and v8.2.3.5 (TCIV)/ ICX-AlphaCom v1.5.3.3/Alphacom XE BSP v32.4.3.12

Summary

Zenitel has addressed a set of security vulnerabilities that were recently identified and assigned Common Vulnerabilities and Exposures (CVE) identifiers.
All identified issues have been resolved in the firmware versions listed below. No further action is required for devices already running these releases.

Resolved Vulnerabilities

CVE ID	Status	Fixed In
CVE-2025-64126	Resolved	VS-IS 9.3.3.0 (8.2.3.4 for TCIV)
CVE-2025-64127	Resolved	VS-IS 9.3.3.0 (8.2.3.4 for TCIV)
CVE-2025-64128	Resolved	VS-IS 9.3.3.0 (8.2.3.4 for TCIV)
CVE-2025-64129	Resolved	VS-IS 9.3.3.0 (8.2.3.4 for TCIV)
CVE-2025-64130	Resolved	VS-IS 9.3.3.0 (8.2.3.4 for TCIV)
CVE-2025-59817	Resolved	VS-IS 9.3.3.0 (8.2.3.4 for TCIV)
CVE-2025-59818	Resolved	VS-IS 9.3.3.0 (8.2.3.4 for TCIV)
CVE-2025-59814	Resolved	ICX-AlphaCom v1.5.3.3
CVE-2025-59815	Resolved	ICX-AlphaCom v1.5.3.3
CVE-2025-59816	Resolved	ICX-AlphaCom v1.5.3.3
CVE-2025-59819	Resolved	AlphaCom XE BSP v32.4.3.12
CVE-2025-64090	Resolved	VS-IS 9.3.3.1 (8.2.3.5 for TCIV)
CVE-2025-64091	Resolved	VS-IS 9.3.3.1 (8.2.3.5 for TCIV)
CVE-2025-64092	Resolved	ICX-AlphaCom v1.5.3.3/ AlphaCom XE to 13.1.3.16 and BSP 32.4.3.12
CVE-2025-64093	Resolved	ICX-AlphaCom v1.5.3.3/ AlphaCom XE to 13.1.3.16 and BSP 32.4.3.12

Note: The CVE IDs above correspond to the public advisories issued through international CERT organizations.

Impact

If unpatched firmware is used, an authenticated user with administrative access to the affected devices may exploit the legacy web interface components. These components have now been removed or refactored, and additional input validation and hardening measures have been implemented. No exploitation in customer installations has been reported to Zenitel.

Mitigation and Customer Actions

To ensure ongoing protection:

- Upgrade all affected devices to the firmware versions listed above or later releases..
- No further mitigation is required once the device has been updated.

Future Hardening Measures

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.

Zenitel Group

Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Zenitel reserves the right to modify designs and alter specifications without notice. ZENITEL PROPRIETARY. This document and its supplementing elements contain Zenitel or third-party information which is proprietary. Any copying is prohibited, if not otherwise explicitly agreed in writing with Zenitel. Any authorized reproduction, in part or in whole, must include this legend. Zenitel – All rights reserved.