Teracom OOD | Security Advisory

Advisory ID: SEC-2026-001
Publication date: 24.11.2026

1. Description

Two security vulnerabilities affecting the web interface of several Teracom Ethernet controllers have been identified.

The vulnerabilities are related to session management and the handling of stored configuration passwords. Under certain conditions, these issues could allow unauthorized access to the web interface or disclosure of sensitive information.

Both vulnerabilities have been addressed. We have no information indicating that these vulnerabilities have been actively exploited.

2. Affected products and firmware updates

Product	Recommended firmware version
TCW122B-CM	4.07 or later
TCW122B-WD	3.15 or later
TCW122B-RR	3.09 or later
TCW181B-CM	4.05 or later

Users are advised to update their devices to the firmware versions indicated above or later. The latest firmware is available on the corresponding product pages.

3. Network Security Recommendations

These controllers use unencrypted communication protocols, such as HTTP and SNMP v1. Information transmitted over the network, including login credentials and control commands, may be intercepted.

For secure operation, we recommend:

- Connect devices only to trusted networks.
- Never expose devices directly to the Internet.
- Restrict access using firewalls or network segmentation.
- Use a secure VPN for remote access.
- Change the default login credentials.
- Keep authentication enabled and disable unused network services.

These precautions remain important even after installing the latest firmware.