مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Zenitel TCIV-3+

Tracking #:432318083

Date:28-11-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in Zenitel TCIV-3+ devices. These vulnerabilities could allow attackers to execute arbitrary code or disrupt device functionality

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified in Zenitel TCIV-3+ devices, including OS Command Injection, Out-of-Bounds Write, and Cross-Site Scripting. These issues are remotely exploitable with low attack complexity. Successful exploitation could allow attackers to execute arbitrary code or disrupt device functionality.

Vulnerability Details

- **CVE-2025-64126 — CVSS v4: 10.0 (Critical)**
  - An input-handling flaw allows user-supplied parameters to be processed without proper validation, enabling remote command execution.
- **CVE-2025-64127 — CVSS v4: 10.0 (Critical)**
  - Improper sanitization of user-provided data allows malicious input to be incorporated into system commands.
- **CVE-2025-64128 — CVSS v4: 10.0 (Critical)**
  - Incomplete validation of input formatting may allow attackers to craft specially formed requests that result in command injection.
- **CVE-2025-64130 — CVSS v4: 9.3 (Critical)**
  - A reflected input-processing flaw could allow specially crafted requests to trigger unauthorized script execution in the user's browser.
- **CVE-2025-64129 — CVSS v4: 7.0 (High)**
  - A memory handling error may allow a remote attacker to write data out of bounds, causing unexpected device behavior or crashes.

Impact:

Exploitation of these vulnerabilities may allow attackers to execute unauthorized actions, including remote code execution or causing the device to become unavailable, leading to service disruption.

Affected Versions

- TCIV-3+: versions prior to 9.3.3.0

Fixed Versions

- TCIV-3+ Version 9.3.3.0 and later.

RECOMMENDATIONS:

- Apply the latest available software updates or patches.
- Limit network exposure of affected devices and avoid direct internet access.
- Implement network segmentation and use firewalls to protect critical systems.
- Use secure remote access methods where required.
- Regularly review device configurations and perform security assessments.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.cisa.gov/news-events/ics-advisories/icsa-25-329-03