# WinConfig Security Advisory

A. Eberle GmbH & Co. KG

**ID**: AEBERLE-SA-WC-2024-001
**Title**: Full device access possible through SSH or serial interface
**Sharing**: TLP:CLEAR
**First Published**: v1 from 2024-11-28
**Last Modified**: v2 from 2024-12-13

## Products

| Product Name | Affected Versions | Fixed Versions |
|---|---|---|
| REG-Pcs (TK28-4) | WinConfig = 14.3.1 | WinConfig ≥ 14.3.2 |
| REG-PEcs (TK28-6) | WinConfig = 14.3.1 | WinConfig ≥ 14.3.2 |
| PQI-DA with TK28-8 | WinConfig = 14.3.1 | WinConfig ≥ 14.3.2 |
| REG-PEDsv (TK102) | WinConfig = 14.3.1 | WinConfig ≥ 14.3.2 |

WinConfig is a software package that contains the firmware of the SCADA cards as well as the PC software for adjusting their settings.

## Summary

We found it is possible to gain full device access locally through the PARAM port. It is also possible remotely via SSH if SSH is enabled.

## Score

Self determined CVSS v3 Score is 9.8 (CRITICAL).

The underlying CVSS Vector is AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

## Impact

An adversary with access to the device-network or to the device's serial interface (PARAM) could gain full device access.

Possible scenarios include:

- exfiltrate or manipulate configuration
- exfiltrate sensitive data
- execute arbitrary code

## Solution

### Remediation

The vulnerability can be fixed by updating the firmware of the cards to WinConfig 14.3.2 or later.

Please ask the support team for the WinConfig 14.3.2 package.

### Mitigation

Remote attacks can be prevented by disabling SSH access completely. Attacks on the local serial port remain possible.

A. Eberle recommends to operate network-capable devices in protected environments like closed networks or networks that are protected with a suitable firewall.