WinConfig Security Advisory

A. Eberle GmbH & Co. KG

ID: AEBERLE-SA-WC-2023-001
Title: DoS Vulnerability in IEC61850 Stack
Sharing: TLP:WHITE
First Published: v1 from 2023-07-14
Last Modified: v1 from 2023-07-14

Products

Product Name	Affected Versions	Fixed Versions
REG-Pcs (TK28-4)	WinConfig ≤ 14.1.1	WinConfig ≥ 14.1.2
REG-PEcs (TK28-6)	WinConfig ≤ 14.1.1	WinConfig ≥ 14.1.2
REG-PEDsv (TK28-6)	WinConfig ≤ 14.1.1	WinConfig ≥ 14.1.2
REG-PE (TK860)	WinConfig ≤ 14.1.1	see remediation
REG-PED (TK885)	WinConfig (all versions)	see remediation

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

Summary

Triangle Microworks informed us about a DoS vulnerability in their IEC61850 stack. Affected are only devices that have the IEC61850 protocol enabled.

Score

Self determined CVSS v3 Score is 5.3 (MEDIUM).

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

Impact

A specially crafted message can result in the IEC61850 functionality to stop working.

This does not affect the functionality of the attached device, like REG-D or REG-DP.

Solution

Remediation

The vulnerability can be fixed by updating the firmware of the cards to WinConfig 14.1.2 or later. This update is only available for the current product generation REG-Pcs (TK28-4), REG-PEcs (TK28-6) and REG-PEDsv (TK102). The previous generation of telecontrol boards REG-PE (TK860) and REG-PED (TK885) can be replaced by the current generation.

Please ask the support team for the WinConfig 14.1.2 package.

Mitigation

To reduce the risk of an attack, the IEC61850 service can be restricted to the network interface that is used for SCADA. WinConfig 14.1.0 or later is required for this.

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