WinConfig Security Advisory

Software and Firmware for SCADA Cards

A. Eberle GmbH & Co. KG

Document Version 0eb26ca from 2022-10-07

ID: AEBERLE-SA-WC-2022-001
Title: Remote code execution in device firmware
Sharing: TLP:WHITE - disclosure is not limited
Published: 2022-10-07

Products

Product Name	Affected Versions	Fixed Versions
REG-Pcs (TK28-4)	WinConfig > 11.2.5 and ≤ 14.1.0	WinConfig ≥ 14.1.1
REG-PEcs (TK28-6)	WinConfig > 11.2.5 and ≤ 14.1.0	WinConfig ≥ 14.1.1
REG-PEDsv (TK102)	WinConfig > 11.2.5 and ≤ 14.1.0	WinConfig ≥ 14.1.1
PQI-DA with TK28-8	WinConfig > 11.2.5 and ≤ 14.1.0	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

The device firmware of the listed SCADA products contains a security vulnerability that allows remote code execution.

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

The vulnerability allows an unauthenticated attacker to execute arbitrary shell commands on the device with root privileges. It can be abused through the webserver, the SSH service and the serial interface of the devices.

We take care of it.

Solution

Remediation

The vulnerability can be fixed by updating the firmware of the cards to WinConfig 14.1.1 or later.

The PQI-DA with TK28-8 card can be replaced by the PQI-DA smart.

Please ask the support team for the WinConfig 14.1.1 package.

Mitigation

To mitigate attacks through the network without updating, it is possible to deactivate the webserver and the SSH service but saving the settings in advance. After this, an attack is still possible using the local serial interface.

Please note that by deactivating the webserver of the device, it is no longer possible to change the settings or update the firmware via WinConfig. The device can still be recovered by RPL software, together with a serial connection and an unlocked Uboot, but all settings will be reset to defaults.

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

Reported by

A. Eberle thanks Jan Hoff and Daniel Szameitat from E.ON Digital Technology GmbH for pointing us to this issue and further support.