

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-2022-002

Title: Device configuration without appropriate authentication 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 \leq 14.1.0	WinConfig \geq 14.1.1
REG-PEcs (TK28-6)	WinConfig \leq 14.1.0	WinConfig \geq 14.1.1
REG-PEDsv (TK102)	WinConfig \leq 14.1.0	WinConfig \geq 14.1.1
REG-PE (TK860)	all WinConfig versions	see remediation
REG-PED (TK885)	all WinConfig 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

The device firmware of the listed SCADA products contains a security vulnerability that allows device configuration without appropriate authentication.

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 change network settings, emergency password and service availability. It can be abused through dedicated UDP packages over the network.

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. 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 14.1.1 package.

Mitigation

To mitigate attacks through the network without updating, it is possible to deactivate the UDP service. For SCADA protocols IEC61850 and IEC60870-5-104 in version WinConfig $\geq 14.1.0$ on REG-Pcs, REG-PEcs and REG-PEDsv this can be achieved by deactivating the service UDP Detect in the network settings and in all other cases by disabling WinConfig management in the network settings.

Please note that by disabling WinConfig management, it is no longer possible to change 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. Another possibility is to re-activate WinConfig management using the local serial connection or SSH.

Blocking traffic to the card on UDP port 1200 is also an option, but in this case the card can no longer be managed over the network using the PC software.

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