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-2022-003
Title: RBAC vulnerability 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 ≤ 14.1.0	WinConfig ≥ 14.1.1
REG-PEcs (TK28-6)	WinConfig ≤ 14.1.0	WinConfig ≥ 14.1.1
REG-PEDsv (TK102)	WinConfig ≤ 14.1.0	WinConfig ≥ 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 an authenticated attacker to perform actions he does not have the permissions for.

This issue only affects installations that have multiple users via role-based access control (RBAC).

Score

Self determined CVSS v3 Score is 8.8 (high).

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

Impact

The vulnerability allows an authenticated attacker to update the firmware and change the radius server address even though the utilized user account does not contain the required permissions, and this finally

enables to gain full administrative access to the device. It can be abused through the webserver of the device.

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.

This fix changes the behavior of some permissions, called action types in WinConfig. Further information can be found in the application note ”Concept for Role Based Access Control (RBAC)”.

Mitigation

To mitigate attacks through the network without updating, it is possible to deactivate all user accounts with restricted access and only allow administrators, that should have all privileges, to access the device.

As an alternative, it is also possible to block the access to the webserver using a firewall or to deactivate the webserver but saving the settings in advance. For SCADA protocols IEC61850 and IEC60870-5-104 in version WinConfig ≥ 14.1.0 on REG-Pcs, REG-PEcs and REG-PEDsv this can be achieved by deactivating the service Webserver 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.

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.