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-2022-004
Title: Remote code execution in PC software
Sharing: TLP:WHITE - disclosure is not limited
Published: 2022-10-07

Products

Product Name	Affected Versions	Fixed Versions
WinConfig PC software	WinConfig ≤ 14.1.0	WinConfig ≥ 14.1.1

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 WinConfig PC software contains a security vulnerability that allows an attacker to execute any commands with privileges of the user running WinConfig.

Score

Self determined CVSS v3 Score is 8.4 (high).

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

Impact

The WinConfig PC software opens a local webserver that is bound to localhost. Requests to this webserver can be abused to execute any program on the computer with the privileges of the user running WinConfig. This could be abused by another user on the same machine or by attackers that trigger the human to click on manipulated links to localhost while WinConfig is running.

We take care of it.

Solution

Remediation

The vulnerability can be fixed by updating the PC software to WinConfig 14.1.1 or later. This update is available for the current product generation generation REG-Pcs (TK28-4), REG-PEcs (TK28-6) and REG-PEDsv (TK102). It is also available for the previous generation of telecontrol board REG-PE (TK860) with IEC60870-5-104 or IEC61850.

Please ask the support team for the WinConfig 14.1.1 package.

A. Eberle recommends to ensure that the user running WinConfig has no write permissions in the WinConfig program folder which is possible after an update to WinConfig 14.1.1.

Mitigation

WinConfig is designed to be executed on single-user machines.

To reduce the risk of this vulnerability, we recommend:

- WinConfig should not run on machines where multiple users are logged in at the same time.
- WinConfig should not be executed as administrator.
- Virtual machines can be used to isolate WinConfig.

Reported by

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