



Security Advisory for Automation Worx Software Suite and classic line industrial controllers. “Insufficient Read and Write Protection to Logic and Runtime Data”.

Publication Date: 2023-12-12
Last Update: 2023-12-12
Current Version: V1.0

Advisory Title

Classic line industrial controllers provide insufficient read and write protection to logic and runtime data.

Advisory ID

[CVE-2023-46141](#)
[VDE-2023-055](#)

Personally liable partner:
Phoenix Contact Verwaltungs-GmbH
Management office Blomberg
Distr. court Lemgo HRB 10904
Statutory seat Vaduz/Liechtenstein
Comm. reg. FL-0002.700.066-3
GmbH & Co. KG:
Distr. court Lemgo HRA 3746

Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Possel-Dölken, Axel Wachholz

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDE33XXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADE33XXX
IBAN:
DE31 4764 0051 0226 0396 00

Vulnerability Description

Phoenix Contact classic line industrial controllers are developed and designed for the use in closed industrial networks. The controllers don't feature a function to check integrity and authenticity of the application (e.g.: logic files, executable logic, configurations).

Logic files generated by Automation Worx could be manipulated on the engineering station and loaded into the PLC without tamper detection. In addition, the tampering can be done by specially designed attacks in such a way that it remains hidden, and the logic program modifies its own code, making it difficult to determine the impact of a malicious program.

Affected products

Classic line industrial controllers:

Article	Article number	Version
ILC 1x0	All variants	All versions
ILC 1x1	All variants	All versions
ILC 3xx	All variants	All versions
AXC 1050	2700988	All versions
AXC 1050XC	2701295	All versions
AXC 3050	2700989	All versions
RFC 480S	2404577	All versions
RFC 470S	2916794	All versions
RFC 460R	2700784	All versions
RFC 430 ETH	2730190	All versions
RFC 450 ETH	2730200	All versions
PC WORX SRT	2701680	All versions
PC WORX RT BASIC	2700291	All versions
FC 350 PCI ETH	2730844	All versions

Automation Worx Software Suite:

Article	Article number
Automation Worx Software Suite	All variants and versions
PC Worx	All variants and versions
PC Worx Express	All variants and versions
Config+	All variants and versions

Impact

The identified vulnerabilities allow attackers to generate logic files or upload logic with arbitrary malicious code to the classic line industrial controllers once they have access to the engineering station running Automation Worx Software Suite or can communicate with the controllers. Attackers must have network or physical access to the engineering station or controller to exploit this vulnerability.

Classification of Vulnerability

[CVE-2023-46141](#)

Base Score: 9.8

Vector: [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

[CWE-732: Incorrect Permission Assignment for Critical Resource](#)

Temporary Fix / Mitigation

Phoenix Contact classic line controllers are developed and designed for use in closed industrial networks. In this approach, the production plant is protected against attacks, especially from the outside, by a multi-level perimeter, including firewalls, and by dividing the plant into OT zones using firewalls.

This concept is supported by organizational measures in the production facility as part of a security management system. To achieve security here, measures are required at all levels. It must be ensured that logic is always transferred or stored in protected environments.

It applies to both data in transmission and data at rest. Connections between the engineering tools (Automation Worx Software Suite) and the controller must always be in a locally protected environment or, in the case of remote access, protected by VPN.

Project data should not be sent as a file via email or other transmission mechanisms without additional integrity and authenticity checks. Project data should only be stored in protected environments. Customers using Phoenix Contact classic line controllers are recommended to operate the devices as intended in closed networks or protected with a suitable firewall.

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note:

[Application note Security](#)

If a classic line controller can't be used in protected zones, the OT communication protocols should be disabled. Depending on the controller type, this can be done either via CPU services via console or web-based management. Information on which controllers and from which firmware version onwards communication protocols can be deactivated is described in the application note for classic line controllers or in the manual for the respective controller, which is available for download on the Phoenix Contact website.

A summary of measures to protect devices based on classic control technology is provided here:

[Measures to protect devices based on classic control technology](#)

Acknowledgement

This vulnerability was reported by Reid Wightman of Dragos, Inc. Phoenix Contact would like to thank Dragos for the cooperation and detailed communication to prepare this coordinated disclosure.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

History

V1.0 (2023-12-12): Initial publication