PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

21 June 2022
300550605

Security advisory for logic without integrity check in classic line industrial controllers

Advisory Title

Products designed for the use in closed industrial networks providing insufficient logic controls allowing attackers to upload logic with arbitrary malicious code.

Advisory ID

CVE-2022-31800
VDE-2022-025

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 uploaded logic.

...

Affected products

Article	Article number
ILC 1x0	All variants
ILC 1x1	All variants
ILC 1x1 GSM/GPRS	2700977
ILC 3xx	All variants
AXC 1050	2700988
AXC 1050 XC	2701295
AXC 3050	2700989
RFC 480S PN 4TX	2404577
RFC 470 PN 3TX	2916600
RFC 470S PN 3TX	2916794
RFC 460R PN 3TX	2700784
RFC 460R PN 3TX-S	1096407
RFC 430 ETH-IB	2730190
RFC 450 ETH-IB	2730200
PC WORX SRT	2701680
PC WORX RT BASIC	2700291
FC 350 PCI ETH	2730844

Impact

An attacker capable of either transmitting manipulated logic or manipulating legitimate logic can execute arbitrary malicious code on the device.

Classification of Vulnerability

CVE-2022-31800
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-345: Insufficient Verification of Data Authenticity

Temporary Fix / Mitigation

Phoenix Contact classic line industrial controllers are developed and designed for the use in closed industrial networks using a defense-in-depth approach focusing on Network segmentation and communication robustness. In such approach, the production plant is protected against attacks, especially from the outside, by a multi-level perimeter, including firewalls as well as dividing the plant into OT zones by using firewalls. This concept is supported by organizational measures in the production plant as part of a security management system. To accomplish security here measures are required at all levels. Ensure that the logic is always transferred or stored in protected environments.

...

This is valid for data in transmission as well as data in rest. Connections between the Engineering Tools and the controller must always be in a locally protected environment or protected by VPN for remote access. Project data should not send as a file via e-mail or other transfer mechanisms without additional integrity and authenticity checks.
Project data should be saved in protected environments only.

Customers using Phoenix Contact classic line controllers are recommended to operate the devices in closed networks or protected with a suitable firewall as intended.

For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note for classic line controllers:

Measures to protect devices based on classic control technology

Remediation

Phoenix Contact classic line controllers are designed and developed for the use in closed industrial networks. The controller doesn’t feature logic integrity and authenticity checks by design. Phoenix Contact therefore strongly recommends using the devices exclusively in closed networks and protected by a suitable firewall.

Acknowledgement

This vulnerability was reported by Forescout.
We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

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