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 unauthenticated protocols in classic line industrial controllers

This vulnerability was originally published by Phoenix Contact 24 June 2019

Advisory Title

Products designed for the use in closed industrial networks providing insufficient authentication for remote communication protocols.

Update A

This updated version contains additional controllers.
In addition, a new application note for classic line controllers had been published to make it easier for our customers to find out the actions how to disable the unauthorized communication ports instead of checking out each controller’s manual.

Advisory ID

CVE-2019-9201
VDE-2019-015

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 authenticate OT communication protocols.

...

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

If the above-mentioned controllers are used in an unprotected open network, an unauthorized attacker can change or download the device code/configuration, start or stop services, update or modify the firmware or shutdown the device.

Classification of Vulnerability

CVE-2019-9201
Base Score: 9.8
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE-306: Missing Authentication for Critical Function

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.

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

If the use of an affected controller in protected zones is not suitable OT communication protocols should be disabled. Either by using the CPU services via console or Web-based Management according to the controller type.
Information's for which controllers and from which firmware version communication protocols can be disabled are described in our application note for classic line controllers or the manual to the respective controller which is available for download at the Phoenix Contact website.

Controller supporting CPU services or WBM for disabling communication protocols:

Article	Article number	From firmware versions
ILC 1x0	All variants	not possible
ILC 1x1	All variants	>= FW 4.42
ILC 1x1 GSM/GPRS	2700977	>= FW 4.42
ILC 3xx	All variants	FW 3.98
AXC 1050	2700988	>= FW 3.01, FW 5.00 (WBM)
AXC 1050 XC	2701295	>= FW 3.01, FW 5.00 (WBM)
AXC 3050	2700989	>= FW 5.60 FW 6.30 (WBM)
RFC 480S PN 4TX	2404577	FW 6.10
RFC 470 PN 3TX	2916600	>= FW 4.20
RFC 470S PN 3TX	2916794	>= FW 4.20
RFC 460R PN 3TX	2700784	>= FW 5.00
RFC 460R PN 3TX-S	1096407	FW 5.30
RFC 430 ETH-IB	2730190	not possible
RFC 450 ETH-IB	2730200	not possible
PC WORX SRT	2701680	not possible
PC WORX RT BASIC	2700291	not possible
FC 350 PCI ETH	2730844	not possible

...

Remediation

Phoenix Contact classic line controllers are designed and developed for the use in closed industrial networks. The control and configuration protocols doesn’t feature authentication mechanisms 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 Sergiu Sechel and re-discovered 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.