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

24 June 2019
300440905/pbsa56

Security Advisory for Industrial Controllers from the ILC1x0, ILC1x1 families, AXC1050 and AXC3050

Advisory Title

Remote configuration using unauthenticated communication protocols.

Advisory ID

CVE-2019-9201
VDE-2019-015

Vulnerability Description

Phoenix Contact Classic Line industrial controllers (ILC1x0 and ILC1x1 product families as well as the AXIOLINE controllers AXC1050 and AXC3050) are developed and designed for the use in closed industrial networks. The communication protocols used for device management and configuration do not feature authentication measures.

Affected products

Article	Article number
ILC1x0	All variants
ILC1x1	All variants
AXC1050	2700988
AXC3050	2700989

Impact

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

...

Classification of Vulnerability

Base Score: 9.8
Vector: CVSS: 3.0:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Temporary Fix / Mitigation

If the use of an affected controller in an unprotected open network cannot be avoided, the affected communication protocols should be disabled by using the CPU services via console. Instructions to CPU services can be found in the manual to the respective device which is available for download at the Phoenix Contact website.

Warning: Disabling the communication protocols will prevent the possibility of remote configuration and monitoring.

For the GSM/GPRS enabled ILC 151 GSM/GPRS (Art. No. 2700977) it is strongly recommended to use Port Filters and a SIM service that provides and implements a VPN (i.e. CDA).

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:

https://www.phoenixcontact.com/assets/downloads_ed/local_pc/web_dwl_technical_info/ah_en_industrial_security_107913_en_01.pdf

Remediation

Phoenix Contact Classic Line Controllers are designed and developed for the use in closed industrial networks. The control and configuration protocols do not 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 discovered by Sergiu Sechel.