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

07 June 2021
300510053

Security Advisory for ILC1x1 Industrial controllers

Advisory Title

Denial of Service vulnerability triggered by specially crafted IP packets.

Advisory ID

CVE-2021-33541
VDE-2021-019

Vulnerability Description

Phoenix Contact Classic Line industrial controllers are developed and designed for the use in closed industrial networks. The communication protocols and device access do not feature authentication measures. Remote attackers can use specially crafted IP packets to cause a denial of service on the PLC's network communication module (CWE-770).

Affected products

Article no	Article	Affected versions
ILC1x0	All variants	All variants
ILC1x1	All variants	All variants

Impact

A successful attack stops all network communication. To restore the network connectivity the device needs to be restarted. The automation task is not affected.

Classification of Vulnerability

Base Score: 7.5
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Temporary Fix / Mitigation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

Measures to protect network-capable devices with Ethernet connection

Acknowledgement

This vulnerability was discovered by the Industrial Control Security Laboratory of Qi An Xin Technology Group Inc. from China and reported to CERT@VDE.

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.