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

04 August 2021
300510053

Security Advisory Niche Ethernet stack for ILC1x0, ILC1x1 and AXC 1050 Industrial controllers and CHARX control DC

Advisory Title

Niche Ethernet stack vulnerabilities can lead to Denial of Service and Breach of Integrity if triggered by specially crafted IP packets.

Advisory ID

CVE-2020-35683, CVE-2020-35684, CVE-2020-35685,
CVE-2021-31400, CVE-2021-31401, CVE 2021-31227

VDE-2021-032

Vulnerability Description

Third party Niche Ethernet stack has several vulnerabilities announced by the security researcher's community.

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 or a Breach of Integrity of the PLC.

Denial of Service:

CVE-2020-35683: Integer overflow in ICMP packet demultiplexing function (CWE-20)
CVE-2020-35684: Integer overflow in TCP checksum calculation function (CWE-20)
CVE-2021-31400: Infinite loop in TCP urgent data processing function (CWE-248)
CVE-2021-31401: Integer overflow in TCP header processing function (CWE-20)
CVE-2021-31227: Parsing HTTP POST cases heap-buffer overflow (CWE-839)

Breach of Integrity:

CVE-2020-35685: Predictable TCP Initial Sequence Number (ISN) generation can be abused for TCP Connection Hijacking/Spoofing (CWE-330)

Affected products

Article no	Article	Affected versions
2700973, 2700974, 2700975, 2700976, 2701034, 2701141	ILC1x1	All firmware versions
All variants	ILC1x0	All firmware versions
2700988, 2701295	AXC 1050	All firmware versions
1624130	EV-PLCC-AC1-DC1	All firmware versions

Impact

A successful attack to the Niche Ethernet stack can lead to Denial of Service or a Breach of Integrity of the PLC.

Classification of Vulnerability

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

Temporary Fix / Mitigation

Customers using Phoenix Contact Classic Line Controllers are strongly 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:

Measures to protect network-capable devices with Ethernet connection

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.

Phoenix Contact is offering the mGuard product family for network segmentation and protection.

Acknowledgement

This vulnerability was discovered and reported by Forescout Technologies, Inc.
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.