

18 July 2018
300417218/pbsa56

Security Advisory for Phoenix Contact ILC 1x1 ETH

Advisory Title

Operation of the PLC can be slowed down by network flooding

Advisory ID

VDE-2018-012
ICS-VU-333465

Vulnerability Description

The processing program of the IEC 61131 program can be slowed down or stopped completely by creating a large amount of network traffic that needs to be handled by the ILC.

Affected products

Phoenix contact ILC 131, 151, 171, 191 ETH with all firmware versions

Impact

The processing of the network load takes up so much CPU power that the operation of all functions of the device, including the 61131 program, will slow down. This may affect the automation task. Once the network load is removed the ILC will return to normal state.

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

Mitigation

Customers using Phoenix Contact ILC 1x1 are recommended to operate the 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:

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

Acknowledgement

This vulnerability was reported by Matthias Niedermaier (Hochschule Augsburg), Jan-Ole Malchow (Freie Universität Berlin) and Florian Fischer (Hochschule Augsburg)