PEPPERL+FUCHS Your automation, our passion.

CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Multiple Ethernet/IP Products – Vulnerability may allow remote attackers to cause a Denial Of Service

Document ID	TDOCT-7104A_ENG
Publication date	2021-02-16
Update of:	
Document ID	TDOCT-7104_ENG
Publication date	2021-02-15
Reason for update	Correction of VDE reference

Vulnerabilities

Identifier	Vulnerability Type	Description
VDE-2021-007, CVE-2021-20987, Hilscher 2019-08-08 “EtherNet/IP stack crash for specific CIP service”	CWE-121: Stack-based Buffer Overflow	A denial of service and memory corruption vulnerability could exist in Hilscher's EtherNet/IP Core V2 that could allow arbitrary code to be injected through the network or make the EtherNet/IP device crash without recovery.

Severity

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

Affected products

Product group PCV/PXV/PGV

Item No.	Item	Version of EtherNet/IP Communication Firmware
293431-100004	PXV100-F200-B25-V1D	1.10.0 and previous
293431-100010	PXV100I-F200-B25-V1D	1.10.0 and previous
284068	PCV100-F200-B25-V1D-6011-6720	1.10.0 and previous
262161	PCV50-F200-B25-V1D	1.10.0 and previous
262162	PCV80-F200-B25-V1D	1.10.0 and previous
262163	PCV100-F200-B25-V1D-6011	1.10.0 and previous

Product group WCS

Item No.	Item	Version of EtherNet/IP Communication Firmware
262006	WCS3B-LS510	1.2.1 and previous
304866	WCS3B-LS510H	1.2.1 and previous
304867	WCS3B-LS510D	1.2.1 and previous
304868	WCS3B-LS510DH	1.2.1 and previous
312680	WCS3B-LS510H-OM	1.2.1 and previous
312681	WCS3B-LS510DH-OM	1.2.1 and previous
312682	WCS3B-LS510D-OM	1.2.1 and previous
312683	WCS3B-LS510-OM	1.2.1 and previous

Summary

Critical vulnerability has been discovered in the utilized component Ethernet IP Stack by Hilscher Gesellschaft für Systemautomation mbH.

The impact of the vulnerability on the affected device is that it can
- denial of service
- remote code execution
- code exposure

For more information see advisory by Hilscher:

https://kb.hilscher.com/pages/viewpage.action?pageId=108969480

Impact

Pepperl+Fuchs analyzed and identified affected devices.
Remote attackers may cause a cause a Denial Of Service of the product.

Solution

An external protective measure is required.

- Minimize network exposure for affected products and ensure that they are not accessible via the Internet.
- Isolate affected products from the corporate network.
- If remote access is required, use secure methods such as virtual private networks (VPNs).

Reported by

Hilscher Gesellschaft für Systemautomation mbH
Coordinated by CERT@VDE

Support

For support please contact your local Pepperl+Fuchs sales representative.