CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Multiple VMT Vision System solutions PROFINET Products – Vulnerability may allow remote attackers to cause a Denial Of Service

Document ID	TDOCT-7196_ENG
Publication date	2021-03-29

Vulnerabilities

Identifier	Vulnerability Type	Description
CVE-2021-20986, Hilscher 2020-12-03 “Denial of Service vulnerability in PROFINET IO Device”	CWE-121: Stack-based Buffer Overflow	When handling Read Implicit Request services, depending on the content of the request, the Hilscher PROFINET IO Device V3 protocol stack does not properly limit available resources. This may lead to shortage of resources which in the end may lead to a Denial Of Service.

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

Item No.	Item	Version of Profinet Communication Firmware
209287	PCZUBHIL CIFX 50-RE PCI SL	V3.14.06 and previous
225295	PCZUBHIL CIFX 50-RE PCI ML	V3.14.06 and previous
249961	PCZUBHIL CIFX 50E-RE PCIe +SL	V3.14.06 and previous
254661	PCZUBHIL CIFX 50E-RE PCIE +ML	V3.14.06 and previous

Summary

Critical vulnerability has been discovered in the utilized component PROFINET IO Device by Hilscher Gesellschaft für Systemautomation mbH.

The impact of the vulnerability on the affected device is that it can

- no longer perform acyclic requests
- may drop all established cyclic connections may
- disappear completely from the network

For more information see advisory by Hilscher:
https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device

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 VMT system solution service specialists.