CYBER SECURITY NOTIFICATION

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

Document ID	TDOCT-7098_ENG
Publication date	2021-02-15

Vulnerabilities

Identifier	Vulnerability Type	Description
VDE-2021-006, 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

Product group PCV/PXV/PGV

Item No.	Item	Version of Profinet Communication Firmware
285693-100000	PGV100-F200A-B17-V1D	V2.0.0 and previous
285693-100001	PGV150I-F200A-B17-V1D	V2.0.0 and previous
285693-100005	PGV100-F200-B17-V1D-7477	V2.0.0 and previous
293431-100003	PXV100-F200-B17-V1D	V4.2.0 and previous
293431-100020	PXV100-F200-B17-V1D-3636	V4.2.0 and previous
244538	PCV80-F200-B17-V1D	V3.2.3 and previous
247325	PCV100-F200-B17-V1D	V3.2.3 and previous
259676	PCV50-F200-B17-V1D	V3.2.3 and previous
282529	PCV100-F200-B17-V1D-6011-6997	V3.2.3 and previous
264850	PCV100-F200-B17-V1D-6011	V3.2.5 and previous
70103187	PCV100-F200-B17-V1D-6011-8203	V3.2.5 and previous

Product group PXV/PGV B28 Profisafe

Item No.	Item	Version of Profinet Communication Firmware
296169	PXV100A-F200-B28-V1D	V1.0.3 and previous
298410	PXV100A-F200-B28-V1D-6011	V1.0.3 and previous
303881	PGV100A-F200-B28-V1D	V1.0.3 and previous
303883	PGV100A-F200A-B28-V1D	V1.0.3 and previous
70105189	PGV100AQ-F200A-B28-V1D	V2.1.1 and previous
70105231	PGV100AQ-F200-B28-V1D	V2.1.1 and previous
70105248	PXV100AQ-F200-B28-V1D	V2.1.1 and previous
70105249	PXV100AQ-F200-B28-V1D-6011	V2.1.1 and previous

Product group OHV

Item No.	Item	Version of Profinet Communication Firmware
289804-100000	OHV-F230-B17	V1.1.0 and previous

Product group OIT

Item No.	Item	Version of Profinet Communication Firmware
316742	OIT500-F113-B17-CB	V1.3.4 and previous

Product group PHA

Item No.	Item	Version of Profinet Communication Firmware
255662	PHA300-F200-B17-V1D	V3.1.5 and previous
257498	PHA400-F200-B17-V1D	V3.1.5 and previous
258403	PHA300-F200A-B17-V1D	V3.1.5 and previous
265869	PHA300-F200-B17-T-V1D	V3.1.5 and previous
266679	PHA200-F200A-B17-V1D	V3.1.5 and previous
266680	PHA200-F200-B17-V1D	V3.1.5 and previous
270875	PHA400-F200A-B17-V1D	V3.1.5 and previous
283557	PHA300-F200A-B17-T-V1D	V3.1.5 and previous
291103	PHA600-F200A-B17-V1D	V3.1.5 and previous
292686	PHA500-F200-B17-V1D	V3.1.5 and previous
292696	PHA500-F200A-B17-V1D	V3.1.5 and previous
292701	PHA600-F200-B17-V1D	V3.1.5 and previous
293772	PHA150-F200A-B17-V1D	V3.1.5 and previous
295658	PHA200-F200A-B17-T-V1D	V3.1.5 and previous
307562	PHA150-F200-B17-V1D	V3.1.5 and previous
320263	PHA800-F200-B17-V1D	V3.1.5 and previous
323292	PHA400-F200A-B17-T-V1D	V3.1.5 and previous
323438	PHA500-F200A-B17-T-V1D	V3.1.5 and previous
70103352	PHA700-F200-B17-V1D	V3.1.5 and previous

Product group WCS

Item No.	Item	Version of Profinet Communication Firmware
262007	WCS3B-LS610	V3.0.0 and previous
280551	WCS3B-LS610H	V3.0.0 and previous
280552	WCS3B-LS610D	V3.0.0 and previous
280553	WCS3B-LS610DH	V3.0.0 and previous
312676	WCS3B-LS610H-OM	V3.0.0 and previous
312677	WCS3B-LS610DH-OM	V3.0.0 and previous
312678	WCS3B-LS610D-OM	V3.0.0 and previous
312679	WCS3B-LS610-OM	V3.0.0 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 Pepperl+Fuchs sales representative.