PEPPERL+FUCHS

Your automation, our passion.

CYBER SECURITY NOTIFICATION

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

Document ID	TDOCT-7083_ENG
Publication date	2021-02-15

Vulnerabilities

Identifier	Vulnerability Type	Description
CVE-2020-25159 ICSA-20-324-03 VDE-2020-050	CWE-787: Out-of-bounds Write	Adaptor Source Code is vulnerable to a stack-based buffer overflow, which may allow an attacker to send a specially crafted packet that may result in a denial-of-service condition or code execution

Severity

Identifier	Base Score and Vector
CVE-2020-25159	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected products

• IC-KP2-2HB17-2V1D	Firmware Version 18-31440H and previous
• IC-KP2-1HB17-2V1D	Firmware Version 18-31766H and previous
• IC-KP-B17-AIDA1	Firmware Version 18-31785F and previous

Summary

Critical vulnerability has been discovered in the utilized component 499ES EtherNet/IP Stack by Real Time Automation (RTA).

Impact

Pepperl+Fuchs analyzed and identified affected devices.
Remote attackers may exploit the vulnerability sending specially crafted packages that may result in a denial-of-service condition or code execution.

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

Sharon Brizinov of Claroty reported this vulnerability to CISA.
Coordinated by CERT@VDE

Support

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