

■ CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: ICRL-M-8RJ45/4SFP-G-DIN and ICRL-M-16RJ45/4CP-G-DIN / Control RocketLinx® – Multiple Vulnerabilities may allow remote attackers access, program execution and to tap information

Document ID TDOCT-6939_ENG
 Publication date 2020-10-05

Vulnerabilities or CVE Identifier

Identifier	Vulnerability Type	Description
CVE-2020-12502	CWE-352: Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)
CVE-2020-12503	CWE-20: Improper Input Validation	Multiple Authenticated Command Injections
CVE-2020-12504	CWE-912: Hidden Functionality	Active TFTP-Service

Severity

Identifier	Base Score and Vector
CVE-2020-12502	8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
CVE-2020-12503	7.2 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)
CVE-2020-12504	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected products

P+F Control RocketLinx®:

- ICRL-M-8RJ45/4SFP-G-DIN Firmware 1.2.3 and previous
- ICRL-M-16RJ45/4CP-G-DIN Firmware 1.2.3 and previous

Summary

Several critical vulnerabilities within Firmware.

Impact

Pepperl+Fuchs analyzed and identified affected devices.

Remote attackers may exploit multiple vulnerabilities to get access to the device and execute any program and tap information.

Solution

For vulnerability CVE-2020-12502 “Cross-Site Request Forgery (CSRF)” and CVE-2020-12503 “Multiple Authenticated Command Injections”:

An external protective measure is required.

- 1) Traffic from untrusted networks to the device should be blocked by a firewall. Especially traffic targeting the administration webpage.
- 2) Administrator and user access should be protected by a secure password and only be available to a very limited group of people.

For vulnerability CVE-2020-12504 “Active TFTP-Service”:

Step 1) Update following products to the respective Firmware Version:

Product ID	Firmware Version
ICRL-M-8RJ45/4SFP-G-DIN	1.3.1
ICRL-M-16RJ45/4CP-G-DIN	1.3.1

Step 2) Deactivate TFTP-Service

Reported by

T. Weber (SEC Consult Vulnerability Lab)
<https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html>

Coordinated by CERT@VDE

Support

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