PEPPERL+FUCHS Your automation, our passion.

CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: (Update A) Multiple Products / Comtrol RocketLinx® – Multiple Vulnerabilities may allow remote attackers access, program execution and to tap information

Document ID	TDOCT-6954A_ENG
Publication date	2021-02-22
Update of:	
Document ID	TDOCT-6954_ENG
Publication date	2020-10-05
Reason for update	New firmware provided as a solution

Vulnerabilities or CVE Identifier

Identifier	Vulnerability Type	Description
CVE-2020-12500	CWE-285: Improper Authorization	Unauthenticated Device Administration
CVE-2020-12501	CWE-798: Use of Hard-coded Credentials	Undocumented Accounts
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-2020-12500	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2020-12501	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
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 Comtrol RocketLinx®:
ES7510-XT, ES8509-XT, ES8510-XT, ES9528-XTv2,
ES7506, ES7510, ES7528, ES8508, ES8508F, ES8510, ES8510-XTE,
ES9528/ES9528-XT

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

Take the following steps to address vulnerabilities CVE2020-12500, CVE2020-12501, CVE2020-12502, CVE2020-12503 and CVE2020-12504 on the ES7510-XT and ES8510-XT switches:

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

Item	Firmware Version
ES8510	3.1.1
ES7510-XT	2.1.1

Step 2) Deactivate TFTP-Service
Step 3) Deactivate PortVision DX Protocol

For the other affected products, 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.
- Traffic from untrusted networks to the device should be blocked by a firewall. Especially traffic targeting the administration webpage
- If remote access is required, use secure methods such as virtual private networks (VPNs).
- Administrator and user access should be protected by a secure password and only be available to a very limited group of people.

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.