SCHAKO Group

Security Advisory Report

SAR-202405-2

Vulnerability title

Unauthenticated file download

Vulnerability description

SCHNEIDER Elektronik's 700 series components allow to download traffic captures without authentication. This capture may contain the credentials of administrative user.
Via the web interface, an unauthenticated user can start a traffic capture and may capture the login of an administrative user therefore user interaction is required. The web interfaces allow only login via HTTP and the credentials are transferred in plain text.

Vulnerability details

- CVE: CVE-2024-35294
- CVSS v3.1 base score: 6.5
- CVSS v3.1 vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
- Vulnerability type: CWE-862

Affected products

Product name	Affected versions	Fixed versions
Series 700	≤ 0.1.17.8	≥ 0.1.17.9

Problem resolution (remediation)

Get the latest version von SCHNEIDER Elektronik series 700 firmware (>= 0.1.17.9) and update all affected units.

Acknowledgement

We would like to thank Felix Eberstaller and David Schauer from Limes Security GmbH for bringing this vulnerability to our attention.