Security Advisory Report

SAR-202405-1

Vulnerability title

Unauthenticated filesystem wipe

Vulnerability description

An attacker who has access to the network where SCHNEIDER Elektronik components are located can cause a denial of service while enumerating the network segment.
SCHNEIDER Elektronik's 700 series uses two ports for communication between controllers and for communication with the programming software. Communication with these ports can occur without any form of authentication. This leads to the fact that malformed or unintended packets can be sent to and be processed by the controller. This results in unintended behavior of the controller that causes a reboot and deletes the file system which contains the program logic.

Vulnerability details

- CVE: CVE-2024-35293
- CVSS v3.1 base score: 6.5
- CVSS v3.1 vector: AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- Vulnerability type: CWE-862

Affected products

Product name	Affected versions	Fixed versions
Series 700	≤ 0.1.17.6	≥ 0.1.17.7

Problem resolution (remediation)

Get the latest version von SCHNEIDER Elektronik series 700 firmware (>= 0.1.17.7) 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.