Cyber Security Statement

Statement according the Controller c430, c520, c550 and CODESYS Security Advisories 2023-01 .. 10

2023-09-12

CODESYS has published the Security Advisories 2023 - 01 ... 10, which describe various vulnerabilities in the CODESYS Runtime.
The vulnerabilities are as follows:

1. Attacks after successful authentication
2. Access to files through the application program
3. Crafted communication requests
4. Execution of malicious code from the current working directory
5. A bug in the notification Center (Lenze Products are not affected)
6. No restriction on retries of passwords during import
7. Running potentially dangerous scripts
8. WIBU Codemeter (Lenze Products are not affected)

In general, we recommend the following measures

- Use controllers and devices only in a protected environment / PC's to minimize network exposure and ensure thatthey are not accessible from outside
- Use firewalls to protect and separate the control system network from other networks
- Activate and apply user management and password features
- Limit the access to both development and control system by physical means, operating system features, etc.
- Use encrypted communication links
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Protect both development and control system by using up to date virus detecting solutions

Provided that the above measures have been implemented, there is no known increased cybersecurity risk for the c430, c520, c550 if using the Controller Firmware 1.11 (based on CODESYS Runtime 3.5.18.40, released SPS 2023).

- c430,
- c520,
- c550

Reference: SysE-21140