SA-CDS-20180315-003: Vulnerability in the WAGO Ethernet TCP/IP driver

Publication Date: 2018-03-15
Last Update: 2018-03-15
Version: V1.0
Severity: Moderate

Description

Independent researcher reported a vulnerability to the NCCIC ICS which can affect the availability of the WAGO Ethernet TCP/IP driver and serial communication.

Impact

Successful exploitation of this vulnerability allows a remote attacker to cause a denial of service of the WAGO Ethernet TCP/IP driver and serial communication. The device can be still used with same functionality via 3S TCP/IP level 2 driver and WAGO Service Communication over TCP/IP.

Affected Products

To our current knowledge following products with firmware version 10 and prior are affected by these vulnerabilities:

- 750-880
- 750-881
- 750-852
- 750-829
- 750-831
- 750-889
- 750-882
- 750-885

Vulnerability Characterization

This advisory is based upon the report of the NCCIC ICS.

Improper resource shutdown or release (CWE-404)

The vulnerability can be exploited remotely by sending special crafted packets to the TCP/IP port 2455 which results in a denial-of-service condition of the communication via WAGO Ethernet TCP/IP driver and serial communication until a restart of the device.

Solution

Update your device to the latest firmware (FW 11 or later). In case this is not feasible, disable the CODESYS communication via WBM (Navigation > Port > “CoDeSys”) or Ethernet Settings Tool (Protocol > “PLC (Port 2455)”, or limit the access to the TCP/IP port 2455 to trusted devices.

Mitigation

- Update your device to the latest firmware.
- Disable the CODESYS communication via WBM or via Ethernet Settings Tool.
- Restrict network access to the device.
- Do not directly connect the device to the internet.
- Restrict the number of users, with access to the device, to a minimum.
- Change the default passwords of devices.
- Do not install software from untrusted sources.

Additional Resources

None

Reported

This vulnerability was originally reported by Younes Dragoni of Nozomi Networks to NCCIC ICS.

Disclaimer

The security instructions given here have exclusively technical-informatory character; contractual stipulations remain unaffected.

http://global.wago.com/en/wago/impressum/software-user-agreement/index.jsp

For updates please visit https://www.wago.com/de/automatisierungstechnik/security regularly, in case of any questions please contact your local sales representative or send your question by email to security@wago.com.