SA-WSC-20180315-002: Vulnerability in WAGO Service Communication

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 Service Communication.

Impact

Successful exploitation of these vulnerabilities allows a remote attacker to cause a denial of service of the WAGO service communication until a restart of the device.

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
- 750-882
- 750-885
- 750-831
- 750-889

Vulnerability Characterization

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

Improper resource shutdown or release (CWE-404)

The vulnerability affects the availability of the WAGO Service Communication and can be exploited remotely by sending an improper TCP three-way-handshake. WAGO Service Communication is only designated for the initial operation and should be deactivated in while normal operation.

Solution

Update your device to the latest firmware (FW 11 or later). In case this is not feasible, disable the WAGO Service Communication via WBM (Navigation > Port > “WAGO Services”) or limit the access to TCP/IP port 6626 to trusted devices.

Mitigation

- Update your device to the latest firmware.
- Disable the WAGO Service Communication via WBM.
- 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.