TELEM-GW IEC-104 communication channel DoS

Vulnerable devices
Telem GW6 and GWM devices with unsecure configurations.

Vulnerability description
Vulnerability is based on protocol IEC60870-5-104 implementation and it’s properties. If there is no specified incoming IP connection address, this vulnerability can be used once the attacker is inside the LAN. A new endless IEC-104 connection to a particular IOA causes the communication error for all other existing previously established connections.

Severity of the vulnerability
CVSSv3 Score: 8.2
CVSSv3 vector parameters: (AV:N) / (AC:L) / (PR:N) / (UI:N) / (S:U) / (C:N) / (I:L) / (A:H)

Vulnerability exploiting description
Continuous access to a one or multiple IOAs will cause those addresses not to be available for other existing communication channels thus causing a denial of service condition.

Vulnerability impact
Denial of service disrupting the control of the industrial process.

Corrective actions
In most cases the vulnerability can be resolved by proper configuration:

- Allowing communication only from trusted partners (other’s side IP defined in GWS, fig. 1)
- Using secure VPN channels
- Proper packet filtering (i.e. firewall fig.2) and right interface choice
Appendix

**Figure 1** Other's side IP address definition

**Figure 2** Firewall enabling via GWS