IEC-104 protocol unsanctioned control command injection vulnerability in Telem-GW devices

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 vulnerablity can be used once the attacker is inside the LAN. Sending crafted IEC-104 control commands to the RTU from a rogue node on the network allows unsanctioned control over industrial process.

Severity of the vulnerability

CVSSv3 Score: 9.9

CVSSv3 vector parameters: (AV:N) / (AC:L) / (PR:N) / (UI:N) / (S:C) / (C:H) / (I:H) / (A:L)

Vulnerability exploiting description

The attack starts a new connection to the RTU port 2404/TCP, initiates data transfer with STARTDT command, and delivers arbitrary IEC104 comands to control the industrial devices on the network. To avoid further disruptions, the data connection is stopped via STOPDT and the TCP session is closed by the attacker.

Vulnerability impact

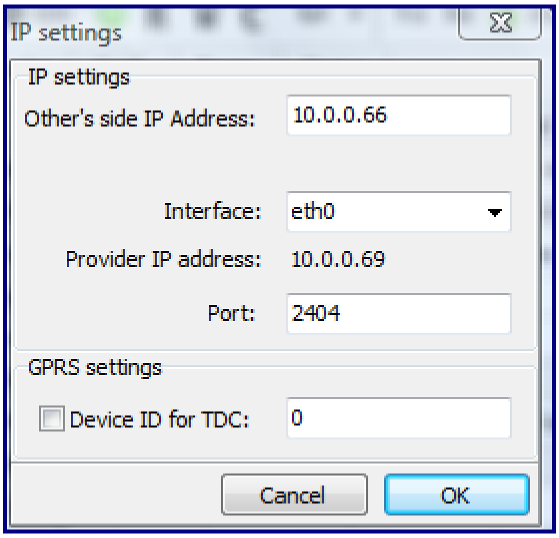
Possible breach of integrity of an industrial process.

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



IP settings

Other's side IP Address: 10.0.0.66

Interface: eth0

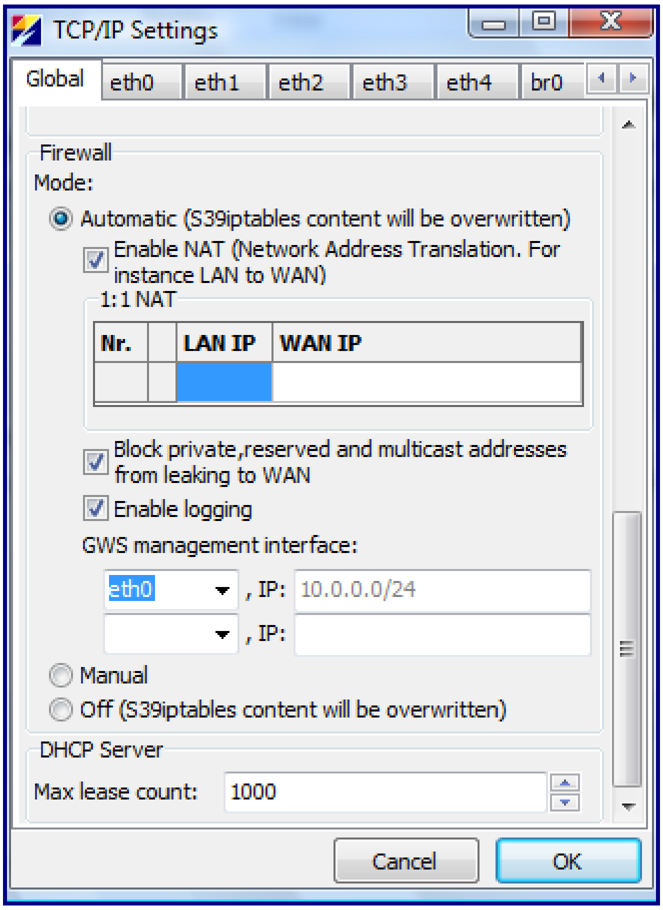
Provider IP address: 10.0.0.69

Port: 2404

GPRS settings

□ Device ID for TDC: 0

Figure 1 Other's side IP address definition



Firewall

Mode:

● Automatic (S39iptables content will be overwritten)

☑ Enable NAT (Network Address Translation. For instance LAN to WAN)

1:1 NAT

Nr.		LAN IP	WAN IP

☑ Block private,reserved and multicast addresses from leaking to WAN

☑ Enable logging

GWS management interface:

eth0 , IP: 10.0.0.0/24

, IP:

○ Manual

○ Off (S39iptables content will be overwritten)

DHCP Server

Max lease count: 1000

Figure 2 Firewall enabling via GWS