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 vulnerablity 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

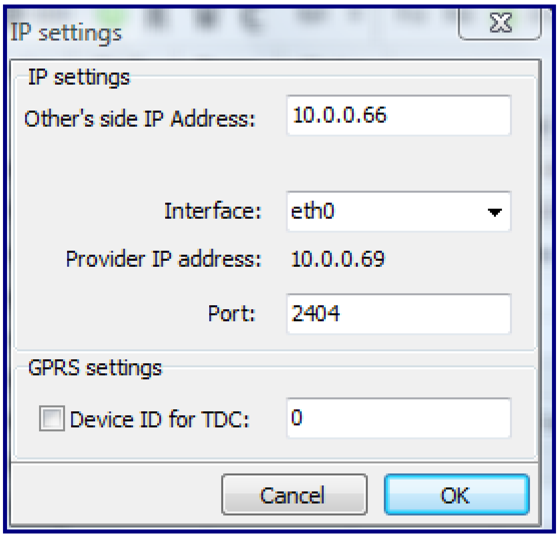
Denial of service disrupting the control of the industrial process.

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



IP settings

Other's side IP Address: 10.0.0.66

Interface: eth0

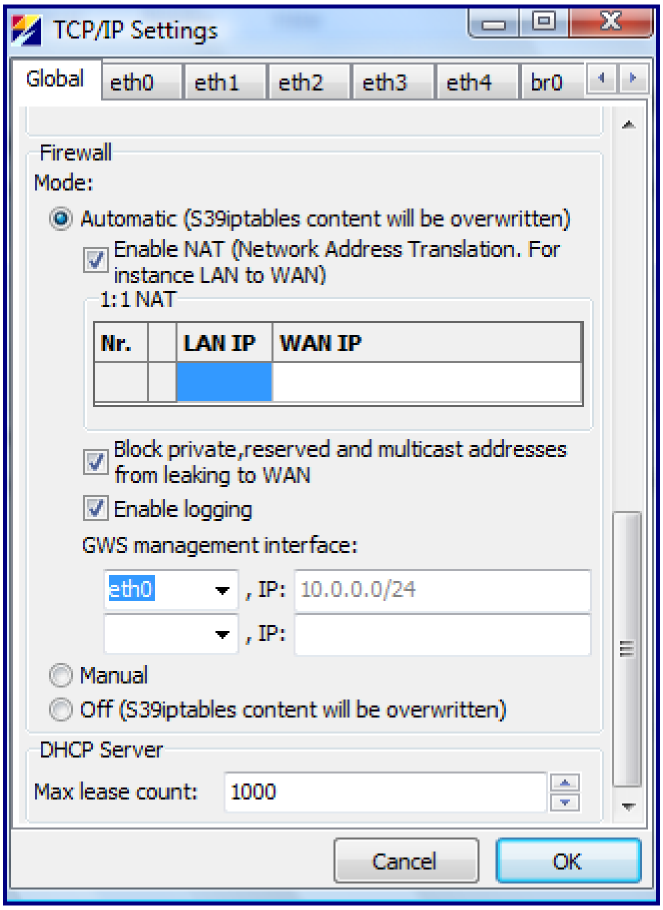
Provider IP address: 10.0.0.69

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