Web management console debug message log message XSS injection via WebSocket vulnerability in Telem-GW devices

Vulnerable devices

Telem GW6 and GWM devices with firmware release 2018.04.18-linux_4-01-601cb47 and older.

Vulnerability description

Improper sanitisation of data input over WebSocket allows client-side JavaScript code injection and execution.

Severity of the vulnerability

CVSSv3 Score: 7.4

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

Vulnerability exploiting description

The Martem RTU web management console log message accepts user controlled input via WebSocket WSSend() function and the unsanitsed script will be executed. Information is displayed in the RTU web console debug message tab together with other system debug messages.

Vulnerability impact

Client-side code execution with target user privileges.

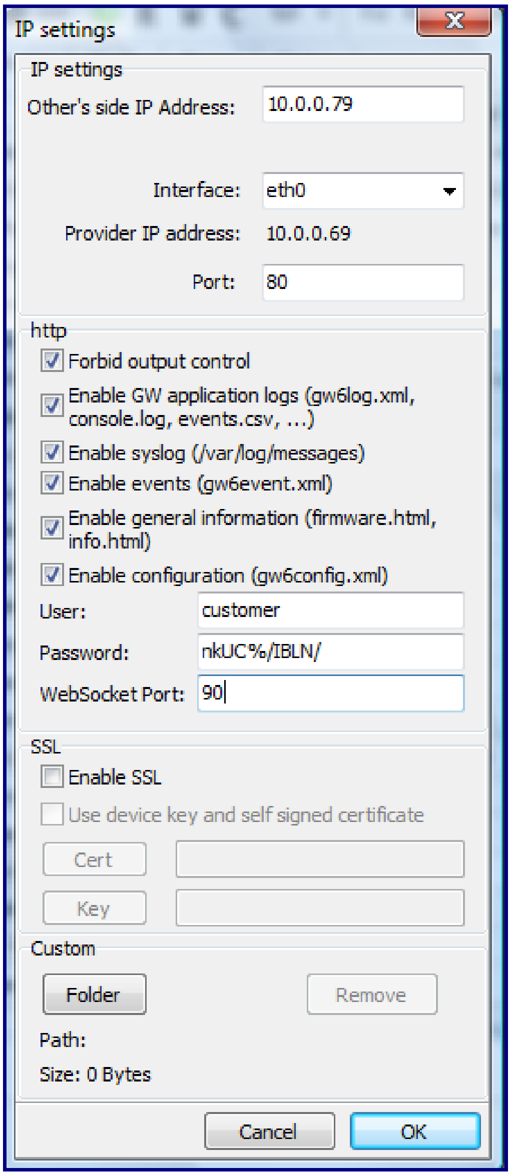
Corrective actions

WebServer should be turned on according to need of the configurator. If the WebServer is not needed anymore, then it should be removed from the configuration.

WebServer access should be protected by strong password to avoid unauthorized access(fig.1). Other side IP should be defined in configuration(fig.1). Use firewall to avoid untrusted connections and to restrict the number of parallel connections to the WebServer.

Fixes are available in firmware release 2.0.72-cb42e64-k4.

Appendix



IP settings

IP settings

Other's side IP Address: 10.0.0.79

Interface: eth0

Provider IP address: 10.0.0.69

Port: 80

http

☑ Forbid output control

☑ Enable GW application logs (gw6log.xml, console.log, events.csv, ...)

☑ Enable syslog (/var/log/messages)

☑ Enable events (gw6event.xml)

☑ Enable general information (firmware.html, info.html)

☑ Enable configuration (gw6config.xml)

User: customer

Password: nkUC%/IBLN/

WebSocket Port: 90

SSL

□ Enable SSL

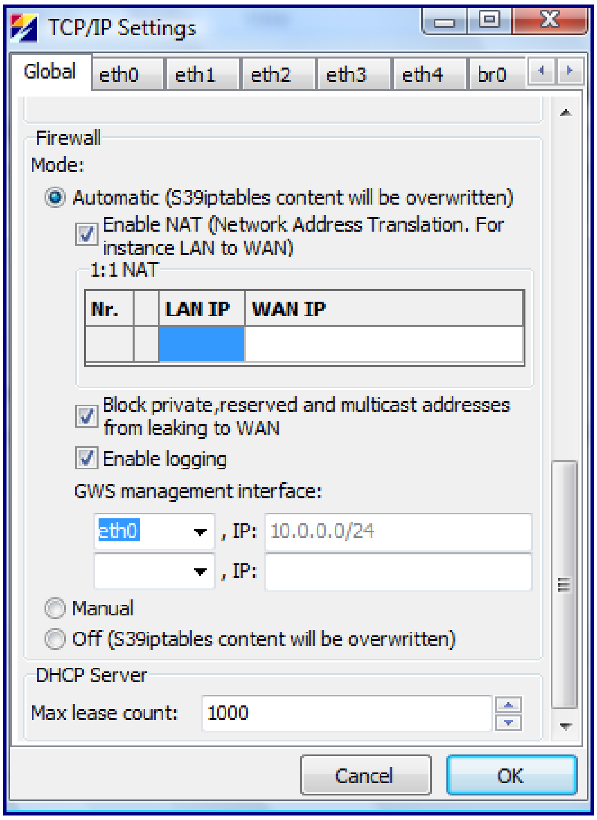
□ Use device key and self signed certificate

Custom

Path:

Size: 0 Bytes

Figure 1 WebServer setup window



TCP/IP Settings

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