Martem TELEM-GW devices configuration update process abuse allowing configuration modification, command execution and privilege escalation vulnerability

Vulnerable devices

Telem GW6 and GWM devices with firmware release before 2.0.87-4018403-k4.

Vulnerability description

Possibility of using unprivileged default credentials to connect to the RTU and modify/upload a new system configuration or take the full control over the RTU.

Severity of the vulnerability

CVSSv3 Score: 8.8

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

Vulnerability exploiting description

As the Martem gws.exe is available over the Internet with the default password in it, there is possibility to connect to the device using default credentials. Additionally the configuration utility produces action log, where all PuTTY commands with the RTU credentials are visible in plain text. There are vulnerabilities in the way how the RTU configuration is being accessed, uploaded, verified and committed. Weak system permissions allow the limited user to download existing and upload new modified configuration by the attacker. There are no proper security checks and verification to confirm the validity and integrity of the new configuration file.

Vulnerability impact

Full system control over RTU and the related industrial process.

Corrective actions

To mitigate this vulnerability the default passwords should always be changed (fig.1) to reasonably strong ones. On using the default password the insistent warning has added to GWS software. The RTU credentials are removed from the GWS action log.
Firewall (fig.2) rules should be implemented to limit unsanctioned SSH access for IPv4 and IPv6. Authorization with SSH public key should be used.
The GWS.exe should be up to date.
Update to new firmware to get configuration tests before applying new configuration, filesystem permission fixes, signed firmware checks. Fixes are available in firmware release 2.0.87-4018403-k4. Refer to chapter 8 “Security considerations” of Telem-GWS User Manual.

Appendix

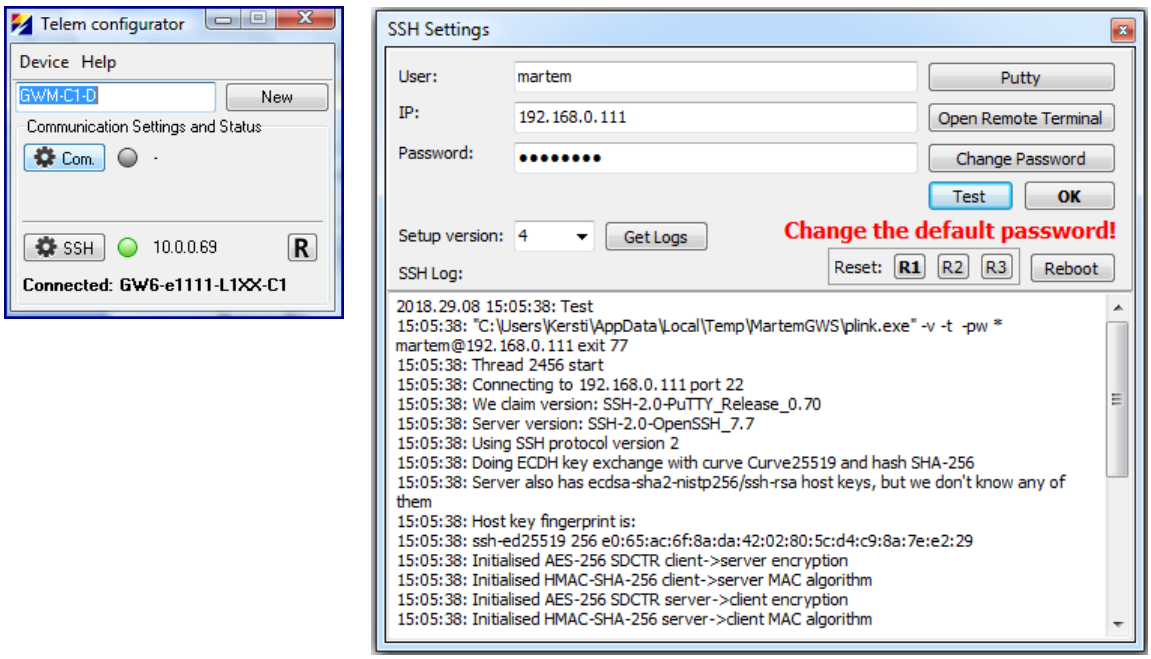

Figure 1 Press „SSH“ and then „Change password“ button in GWS.exe to change default password. The device must be connected.

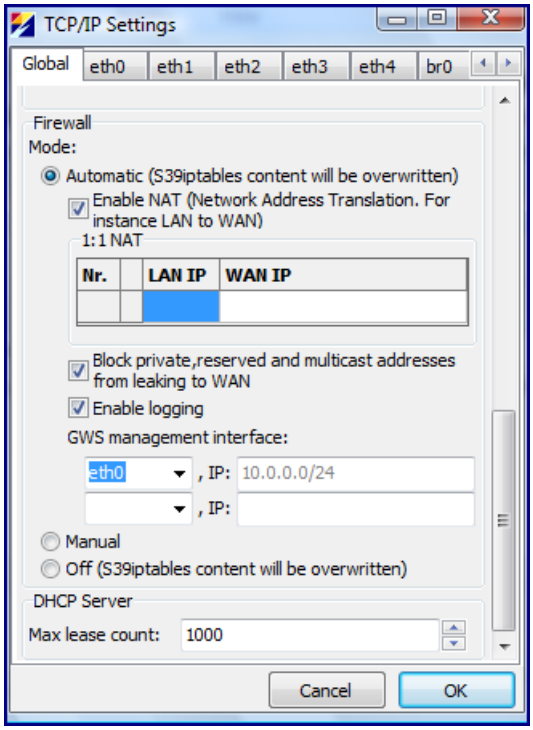

Figure 2 Firewall enabling via GWS. GWS management interface for restricting unsanctioned SSH connections.