Security Guidelines

Contents

Summary

In this article you can find details about all Teltonika's supported security features also what device has which security implementations and a guide how to use them properly.

Security Guidelines

Below you may find some of the most common security recommendations - these recommendations can and should be applied not only to Teltonika devices, but to all internet-facing appliances. It is always advised to adhere to the following security recommendations whenever device is exposed to the internet in some way.

General Security Guidelines

- **Keep Firmware Updated** - Always ensure that firmware is up to date.
- **Set Strong Passwords** - Use strong, unique passwords for all services (WebUI, SSH, Post/Get). Passwords should include numbers, symbols, uppercase, and lowercase letters. Passwords should be between 15-20 characters long.
- **Install Trusted Packages** - Only install packages from known and trusted sources.
- **Use Secure Configuration Protocols** - Use SSH or HTTPS for device configuration. Avoid using insecure protocols like telnet or HTTP, especially for remote configuration.
- **Disable unused services** - Disable services that are not used, especially those that provide some sort of administrative capabilities (e.g.: WiFi, SMS Utilities, Web CLI).
- **Ensure WiFi Security** - If WiFi is used, ensure it employs the latest encryption standards like WPA3 or WPA2 with AES. Avoid using TKIP.
- **Assign Minimum Necessary Permissions** - Make sure to provide the least amount of required permissions for any additionally created user account.
- **Set SIM Card Limits** - Set SMS and data limits for your SIM card to prevent misuse.

Security Hardening Guidelines

- **Limit Administrative Access** - Avoid exposing administrative services to the internet. If public access is mandatory, set unconventional ports (e.g., 32768-65535) for common services.

- **Secure Exposed Services** - If remote access is necessary, ensure that it is protected by a firewall. If remote access is required for any administrative interface, modify the rule to only accept traffic from known sources (e.g. modify the SSH WAN access rule to only allow connections from a specific source address).
- **Manage WiFi Effectively** - Disable WiFi if it is not needed. Consider reducing wireless transmission power rather than hiding the ESSID.
- **Use Key-Based Authentication** - Make sure to use key-based authentication wherever possible (e.g. accessing device via SSH).
- **Verify Backup Integrity** - Always write down & compare MD5/SHA hashes of backup files and firmware files before uploading them to the device.
- **Use Phone Number Whitelisting** - Create phone number groups for SMS commands to act as a whitelist.
- **Disable Unnecessary Utilities** - Review and disable unnecessary SMS/Call utilities and commands, or disable this functionality completely.

Secure Operation Guidelines

- **Regularly Update Firmware** - Regularly check and apply firmware updates for security patches and improvements.
- **Monitor Access Continuously** - Continuously monitor access to administrative services and restrict as needed. Create and regularly review ”Events Reporting” rules to inform when certain events occur on the device.
- **Update Passwords Periodically** - Regularly update passwords and ensure they adhere to strong password policies.
- **Audit Protocols Regularly** - Regularly audit the protocols used for configuration and management to ensure they remain secure.
- **Review Firewall rules** - Regularly audit and review firewall and traffic rules.
- **Review used services** - Regularly review the services that are being used on the device. Disable services that are not used.
- **Configure Secure VPNs** - Use secure VPN protocols (e.g., IPsec, OpenVPN, WireGuard) for remote access instead of exposing sensitive services directly.
- **Conduct WiFi Audits** - Periodically review WiFi settings and ensure they comply with the latest security requirements.
- **Review SIM Card Usage** - Regularly review SMS and data usage limits and adjust them based on current needs and usage patterns. Disable SMS utilities entirely, if it is not utilized whatsoever.

Please note that regardless of currently running configuration, **we strongly recommend to keep up with the latest firmware version** which generally includes not only overall improvements to the router functionality, but also security patches & vulnerability fixes.

Understandably, every production environment is different and some features may be altered or changed in newer firmware versions – please always make sure to test & verify newer firmware versions **before deploying any such firmware onto devices in production environment**.