

Release Note for Vigor2962

Firmware Version:	4.3.2.1
Release Type:	Normal
Applied Models:	Vigor2962, Vigor2962P

Read First

Due to the WebGUI security issue (fixed in 3.9.6.3), we recommend **changing the passwords** for admin login and password/PSKs for VPN profiles after upgrading the latest firmware from 3.9.6.2 or earlier.

New Features

- Support daylight saving time enabled automatically.
- Support the "Session-Based" and "IP-Based" modes options for Routing >> Route Policy.

Improvement

- Improved: Support up to 31 characters for "IP Bind Mac" comment.
- Corrected: An issue with the buffer & socket leakage in OpenVPN.
- Corrected: An issue with low IPv6 NAT throughput for subnets other than LAN1.
- Corrected: An issue where WAN (static IP) reconnects often in HA hot standby mode.
- Corrected: An issue where the router reboots when APM sent the profile to AP frequently.
- Corrected: An issue with a DHCP WAN frequent disconnection with a specific ISP, Thüringer Netkom.
- Corrected: An issue with sending authentication code via SMS with 2FA for VPN not working.
- Corrected: An issue with missing WAN IP Alias interface selection in Service Status Setup page.
- Corrected: An issue with failure to dial-up NordVPN cloud server via OpenVPN LAN-to-LAN.
- Corrected: An issue with the HotSpot Web Portal profiles' settings were gone after the router rebooted.
- Corrected: An issue of NAT loopback traffic was blocked wrongly when Firewall Default Rule was set to Block.
- Corrected: An issue of Vigor Router's local service was blocked wrongly when Firewall Default Rule was set to Block.
- Corrected: An issue with the USB thermometer(TEMPer1F_V3.4) was not detected correctly when the router rebooted.

- Corrected: An issue with Let's Encrypt - Certificate Auto Renew failure (certificate domain did not match router domain).
- Corrected: An issue with failure to accessing Vigor router via HTTP/HTTPS from LAN and WAN due to buffer & socket leakage.

Known Issue

- The web portal may cause the router to be too busy to respond quickly.
- The encryption method for OpenVPN will be returned to the factory default settings if upgrading the firmware version from V3.9.7.x to V4.3.1.
- To prevent potential errors when upgrading firmware, it is recommended to upgrade firmware sequentially one version at a time. (e.g., if the current firmware is 3.9.1, upgrade to 3.9.2 then 3.9.7.2, and last 4.3.2).
- When the firmware is downgrading via “System Maintenance > Firmware Upgrade”, one might have a chance to experience a config compatibility error, which causes the config of a certain function to return to the default setting. To avoid this error, “System Maintenance >> Configuration Export >> Restore Firmware with config” is the preferred way for firmware “downgrading”. We suggest backup the config file before upgrading any firmware as well.