Release Note for Vigor2927 Series

Firmware Version:	4.4.3.1
Release Type:	Normal - Upgrade recommended when convenient
Applied Models:	Vigor2927, Vigor2927ac, Vigor2927Vac, Vigor2927L, Vigor2927Lac, Vigor2927ax, Vigor2927F

Vigor2927 series is a broadband router which integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth. The state-of-art routing feature, VPN security, and Dual-WAN provide integrated benefits for professional users and small offices.

New Features

- None.

Improvement

- Corrected: An issue with the firmware upgrade via VigorACS.
- Corrected: An issue with the system reboot while connecting to Google Cloud VPN.

Known Issue

- A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading.

Note

- IPsec HMAC (MD5) is no longer supported.

Release Note for Vigor2927 Series

Firmware Version:	4.4.3
Release Type:	Normal - Upgrade recommended when convenient
Applied Models:	Vigor2927, Vigor2927ac, Vigor2927Vac, Vigor2927L, Vigor2927Lac, Vigor2927ax, Vigor2927F

Vigor2927 series is a broadband router which integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth. The state-of-art routing feature, VPN security, and Dual-WAN provide integrated benefits for professional users and small offices.

New Features

- Support new WCF suppliers.
- Support a new feature Wireguard VPN.
- Support HTTP compression to reduce the TR-069 payload size.
- Support to authenticate user access to CPE from specified external Radius server.

Improvement

- Improved: Improve the web GUI security.
- Improved: Support more SMS commands.
- Improved: Support more LTE SNMP OiDs.
- Improved: Improve Bind IP to MAC security.
- Improved: Improve Auto APN for Gamma SIM.
- Improved: Improve SIM1/SIM2 failover mechanism.
- Improved: Support system statistics on the login page.
- Improved: Support writable/read-only notes for TR-069 parameters.
- Improved: Add a new option to enable/disable the individual SIM slot.
- Improved: Changing the Management/SNMP settings can be valid after without rebooting the device.
- Corrected: Issues with DNS PTR records.
- Corrected: An issue with the DHCP relay not working.
- Corrected: An issue with the router rebooting after WAN IPv6 renew.
- Corrected: An issue that the Bridge VLAN over mesh network did not work.
- Corrected: An issue with empty .json response for CPE when using VigorACS API.
- Corrected: An issue with the firmware was damaged when upgrading from VigorACS.
- Corrected: An issue with gaps appeared on the graphs displayed on the VigorACS page.
- Corrected: An issue with failure to enable/disable the wireless bands via the WPS button.

- Corrected: An issue that strange data used information shown on the WUI when using SIM budget.
- Corrected: An issue that the router rebooted after saving L2TP with IPsec (LAN to LAN) VPN profile.
- Corrected: Issues related to authentication on External Hotspot Server and the External RADIUS Server.
- Corrected: An issue that the Let's Encrypt certificate could not be renewed automatically but manually.
- Corrected: An issue with the key data loss for OpenVPN client config file when exported from VigorACS.
- Corrected: An issue that OpenVPN to Pfsense connected but could not get the push route from the server.
- Corrected: An issue with an error message of HTTP Content Error appeared while trying to import ovpn file.
- Corrected: An issue that the router rebooted when IKEv2 re-dialed and the local ID was set to 32 characters.
- Corrected: An issue with staying in the Firmware Damage state after uploading the wrong firmware (file size was 0).
- Corrected: An issue that VPN 2FA Windows was not popped-up when a SmartVPN client dialed with IKEv2 EAP and the router's LAN IP used not the 1st setting.

Known Issue

- A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading.

Note

- IPsec HMAC (MD5) is no longer supported.

RD NO: 112_09_18