NO:AP1101-2 V.1

# Release Note for Vigor2927 Series

| | |
|---|---|
| Firmware Version: | 4.4.0 |
| Release Type: | Normal |
| Applied Models: | Vigor2927, Vigor2927ac, Vigor2927Vac, Vigor2927L, Vigor2927Lac, Vigor2927ax |

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

- Use DNS Pool as a new DNS cache.
- Support Link Aggregation for LAN port.
- Support to block DoH/DoT with DNS Filter.
- Adopt new Certificates Management architecture.
- Support Exception List for Hardware Acceleration.
- Support inbound design for hardware QoS (GRX550).
- Support exporting Netflow (IPFIX) to external collector.
- Support Multi-WAN and Load Balance used on Route Policy.
- Support to restrict/drop unwanted traffic to WAN interface (Firewall local filter).
- Support SNMP WAN and LAN port uptime - ifLastChange (Physical port link up/down detection).
- Support bandwidth limit for applications on Bandwidth Management >> Bandwidth Limit>>APP.
- Support hotspot web portal with asynchronous mode (for not reducing NAT performance).
- Support Webhook (on System Maintenance) for sending periodic keepalive/heartbeat to monitoring Server.
- Support a new encryption mechanism for license obtaining, network connecting, and registering to the MyVigor server.

## Improvement

- Improved: Add a new country code, Tunisia.
- Improved: Support hostname in the remote management access list.
- Improved: Pre-define default settings for TR-069 for certain country (0x04).
- Improved: All service options are grey and ticked when Brute Force Protection is disabled

by default.

- Improved: Function priority and default value change for DoS & Bandwidth Limit and HW NAT.
- Improved: Add notes of the local certificate and trusted CA certificate related to firmware downgrading.
- Corrected: Improve Web GUI Security.
- Corrected: Improved the OpenSSL security (CVE-2022-0778).
- Corrected: An issue of router reboot related to Web Portal.
- Corrected: An issue of Wireless clients cannot reconnect to 2.4 and 5GHz.
- Corrected: An issue of Conditional DNS Forwarding function not working.
- Corrected: An issue of default route deleted wrongly after disabling a LAN static route.
- Corrected: An issue of router reboot related to WiFi connection and SK buffer increasing.
- Corrected: An issue related to WAN2 duplex when connecting to a Switch with physical link 100M.
- Corrected: An issue of accessing clients through IPsec VPN when enabling the function of 'translate local network'.
- Corrected: An issue of Port Redirection failure when enabled Hardware Acceleration for NAT and 802.1Q priority for LAN.
- Corrected: An issue of URL Filter failed to block some HTTPS sites (including SNI) when the TCP port number was reused.

# 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.
- Enable Data Flow Monitor will cause Hardware Acceleration to stop working after the firmware upgrade. Please review the DataFlow Monitor setting when meeting a performance drop issue.

# Note

- None.