Release Note for Vigor2962

Firmware Version:	4.3.2
Release Type:	Normal
Applied Models:	Vigor2962, Vigor2962P

Vigor2962, a security VPN router, supports multi-WAN interface with a speed up to 2.5GbE. The Ethernet interfaces are adjustable as LAN or WAN ports. It is suitable for general users, small companies, or small business firms.

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 multilingual login page.
- Support Wired 802.1x for LAN.
- Support LAG Aggregation (LAG Setup).
- Support 2 FA authentication for VPN connection.
- Support Application >> Smart Action for executing certain actions at a certain time.

Improvement

- Improved: Improve the WireGuard VPN feature.
  - stability
  - support "bind to WAN"
- Improved: The APPE module gets upgraded from 15.25 to 15.27.
  - Add the APPE, Statistic, and Route Policy functions related to Yahoo!
  - Add Zalo to the APP Enforcement.
- Improved: Increase the length of characters for username and password fields in Mail Service Object from 32 to 128.
- Improved: Extend the validity of certificate generated by router for OpenVPN server/client from 1 year to 10 years.
- Improved: Increase the length of characters for CN/E-mail fields in VPN and Remote Access >> IPsec Peer Identity from 32 to 64.
- Corrected: An issue of incomplete DrayDDNS logs.
- Corrected: An issue with the LAN DNS malfunction.
- Corrected: An issue where CPU usage was high and also VPN ping was high.
- Corrected: An issue where a non-POE v2962 indicated that itself was a PoE model.
- Corrected: An issue with the malfunction for DHCP relay with tagged VLAN.

- Corrected: An issue with the SSL VPN stability (some NULL pointer problems).
- Corrected: An issue of buffer leakage when SSL VPN dial-out failed in linking state.
- Corrected: An issue with the "Ping to Keep Alive" malfunction in IPsec NAT mode.
- Corrected: Issues where several WUI did not show correctly after upgrading to 4.3.1.1.
- Corrected: An issue of router reboot after configuring "Load Balance Policy" for VPN Trunk.
- Corrected: An issue where SSL VPN stopped responding and router hung after some days.
- Corrected: An issue where an untagged PC got an IP from a network that had a VLAN tag.
- Corrected: An issue with the system rebooting continuously when WAN/LAN IPv6 was enabled.
- Corrected: An issue was that VoIP RTP was sent with an incorrect VLAN tag due to route policy force routing mode.
- Corrected: An issue in which SNMPv3 agent was unable to get data successfully when privacy algorithm was AES.
- Corrected: An issue with some of the WANs in "WAN>> Multi-VLAN" was unable to establish the PPPoE connections.
- Corrected: An issue where H2L clients could not access LAN after changing VPN protocols between PPTP and SSL.
- Corrected: An issue with intermittent packet loss when routing through load balance policy using IP alias on a HA setup.
- Corrected: Unresponsive WUI issues for "System Maintenance >> Max Connection", "VPN >> Wireguard" , "DDNS" and so on.

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