NO:AP1101-2 V.1

# Release Note for Vigor2962

| | |
|---|---|
| Firmware Version: | 4.4.5.1 |
| Release Type: | Critical – Upgrade immediately to address urgent security issues or major system risks |
| 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.
- Before upgrading to 4.4.3, please upgrade to 4.3.2.7 or after to avoid configuration compatibility first.

## New Features

- None.

## Improvement

- Improved: Improve WebGUI security

**Reboot**

- Corrected: An issue with experienced high memory usage for Max Connection number of 150K.
- Corrected: Issues with unexpected router reboots related to IPv6 WAN2 port link down/up, and DPDK Anti-Dos support.

**VPN**

- Improved: Send the next DPD request once again before the router announces the DPD timeout of the VPN connection.
- Improved: Add a note under “VPN and Remote Access>>>PPP General Setup” to explain that Vigor only offers LAN1 IP to OpenVPN clients with AD/LDAP authentication.
- Corrected: An issue with DNS forwarding failed to work over VPN.
- Corrected: An issue that Vigor CPE (e.g., Vigor2925) could not connect to Vigor 3910 via SSL VPN.
- Corrected: An issue with a potential error in "L2TP VPN" where the interface was too large to be stored in an unsigned character.
- Corrected: Issues about typos in the word "XAauth" in "VPN and Remote Access >> PPP General Setup", and the word "Prase error" in Syslog.

**Security / TOTP / Port Knocking**

- Improved: Allow the Port Redirection/Open Ports/Firewall via Source IP using Domain Name.
- Improved: Improve Internet access stability with enhanced DPDK Anti-DoS mechanisms, including: bypassing ICMP packets, automatically adding DNS server IPs to the whitelist, and supporting the whitelists configured on the Firewall DDoS Setup page.
- Corrected: An issue that App Enforcement did not block QUIC because of outdated signatures.
- Corrected: An issue that the BFP view list in the Dashboard showed a blocked IP count, but the BFP table appeared empty.

**Others**

- Improved: Decrypt the QUIC initial packets successfully.
- Improved: Add TR-069 support for VRRP, support for multiple IPv4 VRRP groups.
- Improved: Update the "Firmware Download Link" in the "System Maintenance >> Firmware Upgrade" page.
- Corrected: An issue that wrong IP was displayed in ACS >>Network tree >>Device status.
- Corrected: An issue that the displayed VRRP role status of Master and Backup was incorrect.
- Corrected: An issue which XML with NAT port redirection and Open port configuration did not work until reapplied from the router UI.
- Corrected: An issue with incorrect GeoIP Country Classification.
- Improved: Updated wording from "Applications >> High Availability" to "Applications >> High Availability / VRRP".
- Improved: Update wording from “EasyVPN /SSL Setup" to "EasyVPN / SSL VPN Setup" in VPN and Remote Access.
- Improved: Add the ability to specify IP Alias in Ping Detection (WAN>>Internet Access>>WAN Connection Detection).
- Corrected: An issue with wrong value for DH Group 1 (in “VPN and Remote Access>>LAN to LAN”).
- Corrected: An issue with low Rx throughput while Tx was fine.
- Corrected: An issue that the Disable Ping from the Internet stopped working.
- Corrected: An issue that Ping packets were dropped for unknown reasons.
- Corrected: An issue where NAT loopback/openport did not work for IP Alias WAN and TCP.
- Corrected: An issue that REP Conflict WARN: a=0 p=6 t=2 / showed info about Pseudo Port conflict caused by "srv nat pseudoctl function 4".
- Corrected: An issue with failure to dial VPN via EasyVPN if ACL configured in System Maintenance>>Management.
- Corrected: An issue that TR-069 did not work properly when STUN server was configured with an IP address.
- Corrected: An issue with Netflow interface index for SNMP.
- Corrected: An issue with an error encountered in the Firewall with User-Based.
- Corrected: An issue with failure to block the Alpemix remote control application.

- Corrected: An issue with a DHCPv6 buffer leakage.
- Corrected: An issue while viewing the dashboard, the router was busy due to a high number of BFP entries.
- Corrected: An issue that Vigor router's APM did not support AP1062C.

# Known Issue

- This version (4.4.3.2) introduces support for admin password hashing. If the router is upgraded to this version and later downgraded to a previous firmware version, the admin password will reset to its default value. It will be necessary to log in using the default password and reconfigure it. Other settings will remain unaffected.
- TR-069 parameters for Application >> Smart Action is not completed.
- 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 then the latest version).
- 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.
- Inter-LAN routing setting exported/backed up from firmware 4.3.2 release might be incorrect, please check inter-LAN routing settings.