NO:AP1101-2 V.1

Release Note for Vigor2962

Firmware Version:	4.4.5
Release Type:	Important – Review release notes and upgrade if the changes affect your system stability, performance, or security
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

- Support for DrayOS5 APs.
- Support for XMPP.
- Support for VRRP.
- Support for EasyVPN.
- Support for VPN with Port Knocking.

Improvement

Reboot

- Corrected: An issue that system rebooted due to the Web GUI and TR-069 configuration.
- Corrected: An issue with system rebooting during the backup job performed by VigorACS.
- Corrected: An issue that the router stopped responding and then crashed every 5 or more days.
- Corrected: An issue that system rebooted when there was a third VPN (IKEv2 EAP) connection.
- Corrected: An issue that CPE stayed in boot loop after firmware upgrade if the system parameter 15 was enabled.
- Corrected: An issue where the system rebooted after upgrading, which was related to SMS/SSL VPN functionality.
- Corrected: An issue that the system rebooted when a password containing "%" character was entered in External Devices.
- Corrected: A reboot issue that occurred when both WCF and DNS Filters were enabled during periods of unstable Internet connectivity.

VPN

- Improved: Modify the VPN 2FA Email content.
- Improved: Rename "EasyVPN/SSL" with "EasyVPN / SSL VPN".

- Corrected: An issue with failure to pass all traffic (0.0.0.0/0) through VPN.
- Corrected: An issue where DPDK Anti_DoS affected OpenVPN performance.
- Corrected: An issue with routing problem occurred in an MPLS via a VPN connection.
- Corrected: An issue with failure to restore the VPN backup file from Vigor2927 to Vigor3912.
- Corrected: An issue with EasyVPN connection/HTTPS server responding when accessed by a domain name.
- Corrected: An issue that VPN tunnels dropped and did not re-establish because the VPN info was not released properly.
- Corrected: An issue that VPN LAN to LAN with Translate Local Network "Translate Specific IP" always used x.x.x.0 for Local Network.
- Corrected: An issue with failure to establish a VPN connection if the VPN server used UBDDNS and the DNS server responded with TTL=0.

Security / TOTP / Port Knocking

- Improved: Enhance security by removing weak ciphers from the SSH server.
- Improved: Add an option to require both Access List and Port Knocking for router access.
- Corrected: An issue with Firewall filter by MAC Address failed to work.
- Corrected: An issue with failure to add IP to block list in the DoS Flood table.
- Corrected: An issue that the IP of a more remote subnet could scan the service port which was disabled.
- Corrected: An issue that LAN Access Control with IP Object Range Type could not block VPN from accessing the router's Management interface.
- Corrected: An issue that the firewall rule blocked all WAN traffic to the router, however after 5 minutes, the logs indicated that the traffic was still passing through.

Others

- Improved: Refine DPDK SP flush.
- Improved: Display the Link Aggregation in the Dashboard.
- Improved: Add a quick link to the BFP Block IP List on the dashboard.
- Improved: Support to display the detailed information for Port Statistics.
- Improved: Add new service providers, "SerwerSMS.pl" and "www.voipvioce.it(IT)".
- Improved: An error message /warning message in Syslog when SMS quota reaches 0.
- Corrected: An issue with cached DNS for TR-069.
- Corrected: An issue with missing the Chinese interface.
- Corrected: An issue that RADIUS Request Interval did not work.
- Corrected: An issue with failure to update DrayDDNS (behind NAT).
- Corrected: An issue with failure to update dyn.com after changing IP on WAN PPPoE.
- Corrected: An issue with failure to send SMS using MessageBird or customer's settings.
- Corrected: An issue with configuration of the authentication method for local administrator users.
- Corrected: An issue that APP Enforcement Profile did not block SnapChat and WhatsApp.
- Corrected: An issue with WANx-first behavior for DrayDDNS service when Internet IP was used.
- Corrected: An issue with the TR-069 CPE notification, as it did not provide the WAN IP address.
- Corrected: An issue with the route policy specific gateway did not work on new connections.
- Corrected: An issue which CPE did not send Periodic Inform when the ACS kept

requesting Connection Request.

- Corrected: An issue that TR-069 URL could not be removed when deleting the CPE with the option "Clear TR-069 URL" enabled on the ACS.
- Corrected: An issue with SMS failure through SMS Gateway using recipient number format with "+" sign and Custom SMS Service Object.
- Corrected: An issue which Virtual WAN could not establish PPPoE when both physical WAN and virtual WAN used the same VLAN tag or were untagged.

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.

RD NO: 114_07_03