Release Note for Vigor3910 Series

Firmware Version:	4.4.3.5
Release Type:	Important – Review release notes and upgrade if the changes affect your system stability, performance, or security
Applied Models:	Vigor3910

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 4.4.3.2, please upgrade to 4.3.2.7 or after to avoid configuration compatibility first.

New Features

- None.

Improvement

- Corrected: An issue with a router reboot due to the Web GUI.
- Corrected: An issue with manual time zone configuration for Athens.
- Corrected: An issue with missing Chinese interface after firmware update.
- Corrected: An issue with missing tab formatting in some CLI help menu items.
- Corrected: An issue where an IP could not be added to the DoS Flood block list.
- Corrected: Unexpected reboots caused by Slab Panic / SOCK_DYNA_BUF errors.
- Corrected: An issue where a single quote in the IP Group name broke the QoS page.
- Corrected: An issue where "Unknown WAN" was displayed in the VigorACS server.
- Corrected: A compatibility issue between the SMS Service Object and BulkSMS.com.
- Corrected: An issue where the Vigor3912 Web UI was not reachable via virtual WAN IP.
- Corrected: A reboot issue when both WCF and DNS Filters were enabled during unstable Internet connections.
- Corrected: An issue where the router became non-responsive every few days due to the anti-DoS queue being full.
- Corrected: An issue with Virtual WAN PPPoE dial-up failure when a VLAN tag overlapped with physical WAN.
- Corrected: An issue where the Remote Dial-In VPN backup configuration could not be restored from Vigor2927 to Vigor3912.
- Corrected: A router reboot issue after Web login using 2FA due to broken 2FA configuration in the previous firmware. It is necessary to regenerate the 2FA settings after

upgrading to the new firmware.

- Corrected: An issue with random firmware upgrade failures occurred via VigorACS when an "Always On" OpenVPN tunnel existed.
- Corrected: An issue where the Web UI crashed when the IP Group name under Object Setting >> IP Group contained a comma.
- Corrected: An issue where LAN Access with IP Object - Range Type could not block VPN from accessing the router's management interface.
- Improved: Automatically deleted the "cpu_busy.tar" file during debug log generation if it was over one month old, to speed up log downloads.
- Corrected: An issue where the router no longer attempted to establish a VPN connection if the DNS server responded to the VPN Server's domain name with TTL=0.

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 factory defaulted if firmware upgrading is performed from v3.9.7 to v4.3.1 or above.
- 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.
- At present, DrayOS5 AP is not supported by Vigor3910.

Note

- After upgrading to 4.4.3, the Max NAT connection will decrease from 1000K to 500K due to memory limitation.