Release Note for Vigor3910 Series

Firmware Version:	4.4.3.4
Release Type:	Regular – Upgrade recommended when convenient, as it includes general improvements and optimizations
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

- Improved: Replace the wording "null" with "empty."
- Improved: Support to use the protocol of TCP for Port Knocking.
- Improved: Refine the update method for User Management's data quota.
- Improved: Add the BFP Status (located under Security) on the Dashboard.
- Improved: Hide the CSM profiles that are not enabled on the Main Filter page.
- Improved: Change the text "Product Registration" to "Registration & Services".
- Improved: Add "sms.mitake.com.tw" and "SerwerSMS.pl" as SMS Service Providers.
- Improved: Add TR-069 parameters for Applications >> RADIUS/TACACS+ >> Certificate.
- Improved: Add a note to explain the 'None' item for Protocol on the NAT >> Port Knocking page.
- Improved: Remove "Malloc OSPF config fail" error log when OSPF is enabled but no profiles are configured.
- Improved: Display the Router Policy Name (comment) in the dropdown menus instead of displaying the "Index number."
- Improved: Add a prompt to re-enter the verification code when changing other settings on the NAT>>Port Knocking page.
- Improved: Increase the username length in User Management (and USB >> User Management) to 32 characters from the current limit of 11 characters.
- Improved: Enhance the DPDK Anti-DoS mechanism to reduce high CPU usage caused by UDP broadcast/multicast floods and resolve a router crash issue.
- Corrected: An issue with the STUN server.
- Corrected: An issue with a buffer leakage with SSL VPN.

- Corrected: An issue with router rebooted after login with 2-FA enabled.
- Corrected: An issue with failure to pass all traffic (0.0.0.0/0) through VPN.
- Corrected: An issue with the information displayed for IGMP Status incorrectly.
- Corrected: An issue that WAN IP object/group wasn't listed in firewall source IP.
- Corrected: An issue with High CPU usage due to UDP broadcast/multicast flood.
- Corrected: An issue with failure to establish the IPsec X.509 H2L VPN connection.
- Corrected: An issue with failure to send SMS using MessageBird or custom settings.
- Corrected: An issue that the RADIUS Request Interval was not functioning properly.
- Corrected: An issue that HA Hot-Standby Config Sync was not functioning correctly.
- Corrected: An issue with WANx prioritization for DrayDDNS when using Internet IP.
- Corrected: An issue with the log for updating an external device turned into garbled text.
- Corrected: An issue where the Syslog client failed to work when using the WAN Alias IP.
- Corrected: An issue with DoS attack causing the high CPU usage and freezing the router.
- Corrected: An issue with failure to create a Let's Encrypt certificate with a No-IP domain name.
- Corrected: An issue that Vigor router rebooted when establishing the 3rd IKEv2 EAP VPN connection.
- Corrected: An issue where the online status displayed as "Fiber" even when the Ethernet connection was selected.
- Corrected: An issue with failure to display the correct icon for VigorAP918R, VigorAP805 and VigorAP962C via APM.
- Corrected: An issue with firewall block (with the direction of WAN->Localhost) rule started passing traffic after 5 minutes.
- Corrected: An issue that router reboot occurred when logging into Router Web with TOTP after downgrading from 4.4.3.2 to 4.4.3.1.
- Corrected: An issue that WAN RX Packet Count occasionally displayed negative values when using the CLI command "show state".
- Corrected: An issue that the Gateway setting appeared if WAN/LAN was selected for the Failover to option on Routing>>Route Policy.
- Corrected: Issues with the router that caused it to reboot, primarily related to dray_dpdk, QEMU and configuration backup job via VigorACS server.
- Corrected: An issue that the Internal Syslog Server continued to receive Syslog from the WAN, even after the NAT Open Port rule has been disabled.
- Corrected: An issue with IKEv2 VPN disconnecting when a Peer Domain Name was specified and receiving DNS server responses with a TTL of 0.
- Corrected: An issue when using the packet capture function on the web interface, P1 was incorrectly set enabled even after stopping the packet capture function.

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.

Note

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