NO:AP1101-2 V.1

Release Note for Vigor3910 Series

Firmware Version:	4.4.3.7
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

VPN

- Corrected: An issue with errors caused by packet fragmentation over the VPN.
- Corrected: An issue with the failure to enter a 2FA code for VPN Host to LAN when "Management from LAN" was not allowed.

Security / TOTP / Port Knocking

- Improved: To comply with NIS2 security requirements, the firmware now applies the following defaults - Telnet is disabled, FTP is disabled, and Enforce HTTPS Access is enabled. If Telnet/ FTP access on LAN1 is unavailable after the upgrade, users are advised to verify the settings under System Maintenance >> LAN Access Control.

Reboot

- Corrected: An issue with the system reboot by replacing risky PPPoE pointers and function with local copies to prevent pointer-related crashes.
- Corrected: An issue with the router reboot when handling multiple fragmented packets over WireGuard VPN.
- Corrected: An issue with the router reboot occurred while saving the Syslog to the USB disk.
- Corrected: An issue with the router reboot occurred when TR069 queried BFP-related parameters.

Web UI / GUI / Interface / Text

- Improved: Disabled WANs will not be shown in the Diagnostics>>Traffic/Resource Graph.

- Improved: The option to change the TTL value for all WANs using PPPoE mode is disabled by default.
- Corrected: An issue with missing the "Hostname Object/Group" option in the IP Filter Rule.
- Corrected: An issue with wrong display of the IPv6 address of WAN3 in the WebUI started with "WAN3".
- Corrected: An issue with failure to click any quick-access links on the dashboard for macOS/iOS Safari users.
- Corrected: An issue with lack of information about the latest stable firmware in System Maintenance>>Firmware Upgrade.
- Corrected: An issue with failure to correctly show details in Applications>>Smart Action due to a single quote in the Routing>>Load-Balance/Route Policy page.

Others

- Corrected: An issue with failure to failover from Multi-WAN Policy Route rules.
- Corrected: An issue that the user management data quota did not work properly.

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.

RD NO: 114_11_17