NO:AP1101-2 V.1

Release Note for Vigor2962

Firmware Version:	4.4.5.2
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

- None.

Improvement

System Stability

- Corrected: An issue with an system reboot occurred related to IPv6.
- Corrected: An issue with an intermittent ping responses occurred from WAN.
- Corrected: An issue with the system reboot due to malformed QUIC packets.
- Corrected: An issue with the system reboot occurred during configuration export.
- Corrected: An issue with the system reboot occurred while saving the Syslog to the USB disk.
- Corrected: An issue that the system reboot was caused by overflow during object restoration.
- Corrected: An issue with the system reboot when handling multiple fragmented packets over WireGuard VPN.
- Corrected: An issue with the system reboot by replacing risky PPPoE pointers and function with local copies to prevent pointer-related crashes.

VPN

- Improved: Support routes control (more remote subnets) for EasyVPN.
- Improved: Improve the Teleworker VPN (IKEv2 EAP) flow when wrong username/password is provided.
- Corrected: An issue with errors caused by packet fragmentation over the VPN.
- Corrected: An issue that the VPN status became abnormal when the RADIUS username contained quotes.
- Corrected: An issue that the traffic to the destination domain “sicoob.com.br” was not forwarded

to the VPN tunnel via the route policy.

- Corrected: An issue with failure to access the web user interface from WAN when VPN LAN to LAN remote network was set as 0.0.0.0/0 and the option “Change Default Route” was enabled.

Applications

- Improved: Add the Router MAC info to the Syslog.
- Improved: Add the legends corresponding to show-chart interval in the Diagnostics graphs.
- Improved: Allow selecting IP Group for LAN Access Setup in System Maintenance>>Management.
- Improved: Add an option of "VPN on Slave" under Applications>> High Availability /VRRP for HA failover.
- Improved: The SDWAN data can be subdivided into different types in Monitoring>>Data Usage (SD-WAN).
- Corrected: An issue that false mail alerts occurred after upgrading.
- Corrected: An issue that IP Object (Range Address) failed for WAN Access List.
- Corrected: An issue that the Safari users could not click dashboard quick-access links.
- Corrected: An issue that the “Hostname Object/Group” option was missing in IP Filter Rule.
- Corrected: An issue that “Change TTL value” option for PPPoE WANs was disabled by default.
- Corrected: An issue that settings could not be saved in System Maintenance>>Management.
- Corrected: An issue with failure to display the Smart Action page when load-balance comment contained a single quote.

Others

- Improved: Enhance the stability of High Availability.
- Improved: Add a Note and a Factory-Default option in NAT>>Sessions.
- Improved: Improve overall usage by adjusting the memory allocation.
- Improved: Support the string objects for the Telegram action type in Applications>>Smart Action.
- Improved: Improve a web security issue on the login page by removing the env-eval (environment evaluation) option.
- Corrected: An issue that VRRP worked unstably.
- Corrected: An issue with wrong display of country-code for High Availability.
- Corrected: An issue that Failover from Multi-WAN policy route rule failed to work.
- Corrected: An issue that the policy route to wildcard domains did not function correctly.
- Corrected: An issue with wrong display of the IPv6 address of WAN3 in the WebUI started with "WAN3".
- Corrected: An issue that the DHCP Relay forwarded Discover packets to only one DHCP server on LAN 10.
- Corrected: An issue that the WAN-bandwidth aggregation failed when Fast NAT/Routing was enabled.
- Corrected: An issue that the data quota function failed to work (configured in User Management>>User Profile).
- Corrected: An issue that IPsec Peer Identity did not save the content after a space in VPN and Remote Access>>IPsec Peer Identity.
- Corrected: An issue that the BFP list on the Dashboard showed a blocked IP count while the table in Firewall>>Defense Setup was empty.
- Corrected: An issue with lack of information about the latest stable firmware in System Maintenance>>Firmware Upgrade.

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.

Note

- 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.

RD NO: 114_12_04