NO:AP1101-2 V.1

Release Note for Vigor2962

Firmware Version:	4.4.5.3
Release Type:	Regular – Upgrade recommended when convenient, as it includes general improvements and optimizations
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 Reboot

- Corrected: Issues with the router reboot caused by saving Syslog to a USB disk and other unexpected reasons.

VPN

- Corrected: An issue with failure to establish the Teleworker VPN IPsec IKEv2 PSK connection from iOS.
- Corrected: An issue that the VPN WireGuard 2FA pop-up did not show when the firewall rules containing URL Filter/DNS Filter were active.

Security

- Corrected: An issue with failed to clear ICMP sessions after the session timeout.
- Corrected: An issue with failed to select keyword object with the type of domain name for the firewall.

Web UI

- Corrected: An issue with failed to display correct WAN Interface status in Application>>Dynamic DNS.
- Corrected: An issue with failed to display correct DNS filter profile setting page in CSM>>DNS Filter Profile.
- Corrected: An issue that the EasyVPN message incorrectly required the password field when disabled.
- Corrected: An issue with failed to display the correct Src IP in Firewall>>Filter Setup>>Edit Filter Set if using an IP object as the Source IP.
- Corrected: An issue which the function of "This file is encrypted with password" failed to work in System Maintenance>>Configuration Backup.

Others

- Improved: Increase the UDP session timeout from 30 seconds to 180 seconds.
- Improved: Enhance the NAT performance when the admin user logs out of the WebUI.
- Corrected: An issue that the routed subnet stopped working.
- Corrected: An issue with incorrect LAN interface assignment for BGP-learned routes.
- Corrected: An issue which the DDNS(dyn.com) never updated during the WAN backup failover.
- Corrected: An issue with failed to delete any firmware config in System Maintenance>>Configuration Export.
- Corrected: An issue with which the bandwidth limit did not activate after being configured in the Hotspot Web Portal>>Quota Management.

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: 115_04_13