

Release Note for Vigor2962

Firmware Version:	4.4.6.1
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 firmware version 4.4.6.1, please first upgrade to version 4.3.2.7, 4.4.3.2, or later to ensure configuration compatibility. If the currently running firmware version is 3.9.x, you must first upgrade to version 3.9.7.2.
- Since 4.4.3.2 firmware version there is support for admin password hashing, please note that if you upgrade to this version and later downgrade to a previous version, the admin password will reset to the default, and you will need to reconfigure it. Other settings will not be affected.
- 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.
- It is always recommended to take a configuration backup before performing the firmware upgrade.

New Features

- None.

Improvement

- Improved: Improve the VPN security.
- Corrected: An issue with WUI pre-authentication errors.

VPN

- Improved: Enhance the L2TP and L2TP over IPsec performance.
- Improved: Enhance the protection for abnormal L2TP packet parsing.
- Corrected: An issue with the abnormal OpenVPN TCP performance.
- Corrected: An issue where the default VPN Dial-out Server Type for VPN LAN-to-LAN was IPsec IKEv2 instead of PPTP.

Reboot / Crash / Freeze / High CPU

- Corrected: An issue where the router rebooted under high load due to a missing source port in the connection tracking hash.

Web UI

- Improved: Improve the Firmware Version Before and After display in VigorACS Maintenance >> Firmware Upgrade >> View Log.
- Corrected: An issue where the IP Object page broke after changing a range address to a subnet address.

Others

- Improved: Refactor the Virtio-Net driver to improve throughput and VM slow-path network performance.
- Corrected: An issue where the router ignored the Primary DNS server.
- Corrected: An issue where the ping packets with TTL lower than 30 were intermittently dropped.
- Corrected: An issue with failure to display 6 GHz information for AP1070C in Central Management >> AP >> Status.
- Corrected: An issue with failure to obtain the correct time in System Maintenance >> Time and Date >> Browser Time.
- Corrected: An issue where the router was unable to obtain an OAuth2 token with Microsoft 365, while Google worked correctly.
- Corrected: An issue where failure to display the Stable and Mainline firmware correctly in System Maintenance >> Firmware Upgrade.
- Corrected: An issue where NetFlow settings were not applied correctly on Vigor3912S, even though VigorConnect sent the NetFlow profile configuration successfully.

Known Issue

- The web portal may cause the router to be too busy to respond quickly.

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.