

Release Note for Vigor2962

Firmware Version:	4.4.6.2
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

- Add Cloudflare as a Dynamic DNS service provider.
- Add a firmware update reminder in System Maintenance and Dashboard.
- Add an enable/disable switch for the administrator block page in CSM >> DNS Filter. The switch is disabled by default to reduce CPU utilization.

Improvement

Reboot / Crash / Freeze / High CPU

- Corrected: An issue where recursive decapsulation of WireGuard packets caused a crash.
- Corrected: An uninitialized-pointer issue in TR-069 that could cause the router to reboot repeatedly.
- Corrected: An issue where a malformed response from a customized DDNS server caused the router to reboot.
- Corrected: An issue where accessing TR-069 CLI parameters before interface initialization caused

read failures or a reboot.

VPN & Security

- Improved: Upgraded the Suricata engine on Vigor3912S to address CVE vulnerabilities.
- Improved: Extended the validity of self-signed OpenVPN server and client certificates to 10 years.
- Corrected: A pre-authentication CGI security issue.
- Corrected: An issue where a firmware upgrade or configuration import changed a VPN LAN to-LAN profile from IKEv1 to IKEv2.
- Corrected: An issue where WireGuard LAN-to-LAN connections were unstable and peer endpoint information was not displayed.
- Corrected: An issue where MyVigor Force Sync and Activate encountered authorization errors after pre-authentication CGI hardening.

Web UI

- Improved: Moved the Port Knocking Status Table to the Diagnostics menu for easier access.
- Corrected: A display issue on Linux Application >> Basic Settings.
- Corrected: An issue where no warning was displayed when an existing username was reused in a Remote Dial-in User profile.

Others

- Corrected: An issue where Strict Bind in Bind IP to MAC required a router reboot before taking effect.
- Corrected: An SNMP response error (Response PDU Too Big / PDU is empty) caused by an incorrect counter length.
- Corrected: An issue where firmware upgrades failed due to insufficient memory, and firmware upgrade errors were not handled properly.

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.