NO:AP1101-2 V.1

# Release Note for Vigor2962

| | |
|---|---|
| Firmware Version: | 4.4.6.3 |
| Release Type: | Critical – Upgrade immediately to address urgent security issues or major system risks |
| 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

**Reboot / Crash / Freeze / High CPU**

- Corrected: An issue in which the router would reboot when an IKEv2 VPN negotiation was split into fragments.
- Corrected: An issue where the router rebooted every 1–1.5 hours, potentially due to a memory leak in the network driver.
- Corrected: An issue where the router crashed after a WireGuard key renewal.
- Corrected: An issue where the router became unresponsive when a LAN host was flooded with traffic from the internet.
- Corrected: An issue where the router rebooted due to the TR-069 connection to the management server.
- Corrected: An issue where the router rebooted due to IGMP logging.

- Corrected: An issue where the router rebooted when HTTPS traffic to MyVigor was blocked upstream.
- Corrected: An issue where the router continuously rebooted due to DDNS.
- Corrected: An issue where the router crashed after L2TP VPN activity.
- Corrected: An issue where the router rebooted under heavy 802.1X (RADIUS) login traffic.
- Corrected: An issue where the router crashed when BitTorrent filtering was applied in a firewall rule.
- Corrected: An issue where the router crashed when applying a wireless profile from Central AP Management.
- Corrected: An issue where the router crashed after repeated wireless mesh resets.
- Corrected: An issue where the router rebooted when importing a configuration file.
- Corrected: An issue where a faulty SFP module kept the port-status service busy on the router.

**VPN & Security**

- Corrected: An issue where only four WireGuard LAN-to-LAN tunnels could be configured.
- Corrected: An issue where an IPsec VPN connection from a routed LAN stopped working after a few minutes.
- Corrected: An issue causing packet loss and latency on the LAN-to-LAN VPN.
- Corrected: An issue causing IKEv2 EAP VPN connections to fail when using the built-in client on Android 16.
- Corrected: An issue where packets were not NATed on L2TP/IPsec dial-out connections.
- Corrected: An issue causing an incorrect AES-GCM encryption setting in the VPN data path.
- Improved: The VPN Connection Status page shows the IPsec type and DH group.
- Improved: Enhanced access control for pages that can be reached before login.
- Corrected: An issue affecting security in SSH, the login page, EasyVPN OTP mail, and Hotspot.
- Corrected: An issue causing a buffer overflow in NAT > Open Ports.
- Corrected: An issue related to the OpenSSL "HollowByte" denial-of-service flaw
- Corrected: An issue affecting the security of user online-status notifications.

**Web UI**

- Corrected: An issue where the firmware update reminder incorrectly blocked other Internet HTTP traffic.
- Improved: Increased the maximum PPPoE username length from 24 to 40 characters.
- Improved: A long admin password is now accepted for Telnet login, in addition to the Web UI.
- Corrected: An issue occurred where switching from LAN DNS to DNS Forward did not clear the IP addresses or DNS cache.
- Improved: The same DHCPv6 option can now be added on different LANs.
- Corrected: An issue occurred where Port Knocking did not display a warning when the first knock port was already in use.
- Corrected: An issue occurred where the configuration backup was truncated, and the corrupted file could not be reported.
- Corrected: An issue occurred where SNMPv3 remained effective even after it was disabled.
- Corrected: An issue occurred where enabling or disabling the SNMP agent caused the WAN connection to go down.
- Corrected: An issue occurred where the Data Flow Monitor failed to display the DHCP host name.
- Corrected: An issue occurred where the WAN name was displayed repeatedly on the IPv6 line in System Status.
- Corrected: An issue that the IPv6 uptime wrapping onto a second line on the Dashboard.
- Corrected: An issue with the Central Management >> Switch pages, including missing ports on a 54-port switch.

**Others**

- Corrected: An issue with User-Based authentication where the time-tracking pop-up reappeared

and user accounts were able to log in.

- Improved: Let's Encrypt certificates will be renewed automatically.
- Corrected: An issue where firmware uploads through the Web UI failed part way through.
- Corrected: An issue where the CPE could not connect to MyVigor after the service was migrated to Cloudflare.
- Corrected: An issue where NAT loopback did not work when the Route Policy used a WAN alias IP.
- Corrected: An issue where Smart Action's scheduled reboot did not run every time.
- Corrected: An issue where an unresolved hostname object flooded DNS queries and the log.
- Corrected: An issue where traffic from accelerated L2TP tunnels after the first tunnel was not displayed in the Web UI.
- Improved: Supported the DrayOS CLI option to the Console Menu.
- Improved: Added the “port sniff” telnet command.
- Improved: Hardened alert-message handling.
- Improved: Added logs for LAN packets dropped by the virtual network card for diagnosis.
- Corrected: An issue where wrong port speed and stale port status displayed on the Dashboard.

# 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.

RD NO: 115_09_22