

Release Note for Vigor2767 Series

Firmware Version:	5.4.4.1
Release Type:	Critical – Upgrade immediately to address urgent security issues or major system risks
Applied Models:	Vigor2767, Vigor2767ax, Vigor2767ax-4G

Vigor2767 Series is a Dual-WAN DSL and Ethernet VPN security router available in wired and Wi-Fi 6 (IEEE 802.11ax) models. It delivers load balancing, automatic failover, secure VPN connectivity, and integrated cybersecurity for reliable, high-speed business networking.

New Features

- Support Threat Protection – Sentry, our new license-based cybersecurity solution.
- Support Route-based VPN with manual remote-network routing without requiring 0.0.0.0/0 in the Routing Table.
- Hardened the TR-069 configuration path by writing the ACS server URL and credentials directly to the configuration file, eliminating a command-injection risk in the web management backend.
- Support NAT Port Forwarding on ports reserved by the router's own services, with conflict notification and forwarding priority options.
- Add the exec sysuptime and exec wanstatus CLI commands, so system uptime and WAN status can be queried over SSH / Telnet.

Improvement

- Improved: Update SQLCipher to 4.17.0 (CVE-2026-11822 / CVE-2026-11824).
- Corrected: The kernel SCTP ASCONF DEL-IP vulnerability "SCTPhantom" (CVE-2026-64564).
- Improved: Updated third-party packages based on CVE information identified during SBOM review, including curl/libcurl, ppp, miniupnpd, libarchive, libxml2, libexpat, jq, and libcap.
- Improved: WAN profile application and WAN AutoHunt retries now reload only the affected interface, preventing other WAN connections from being dropped.
- Corrected: An issue where the SIM slot activity LED stopped illuminating after a firmware upgrade.
- Corrected: An issue in a multi-WAN setup where reply packets from a secondary WAN (including LTE / Cellular) were sent out of the wrong interface, causing ping and remote management to that WAN's IP address to fail.
- Corrected: An issue where LAN clients could not reach a DNS server behind an LAN-to-LAN VPN tunnel without DNS Forwarding, along with a related full-tunnel reconnect loop.
- Corrected: An issue which caused the Physical Interface page to fail to display or save after the router was reset to factory defaults with certain country codes (e.g. Germany).
- Corrected: An issue preventing hosts in an IP Routed Subnet from reaching the gateway and the Internet.

- Corrected: An issue which caused WAN-related log messages to appear only under "Notification" and not in the Log Center log list.
- Corrected: An issue preventing the router from resolving domain names when the LAN IP and Teleworker VPN IP assignment were in different subnets.
- Corrected: An issue causing DHCP Relay over WAN to silently fail after a LAN or WAN interface was reset because the relay daemon did not rebind to the new interface.
- Corrected: An issue which caused a managed node's mDNS name to be overwritten during Virtual Controller configuration sync, resulting in duplicate mDNS names on the network.
- Corrected: An issue which caused the TR-069 ACS username and password to reject or incorrectly store special characters such as ", , , & , ` , and \$.

Known Issue

- None.

File and Modem Code

- "Vigor2767_v5.4.4.1.zip" provides modem code 5.16.19.0.

Note

- Please ensure that you use the ".rst" firmware file when recovering the router. Note that uploading the ".rst" file will reset the router to factory default settings. For certain models, a separate ".rst" (reset) firmware file may not be provided. If the ".rst" version is not available, please manually rename the file extension of the ".all" or ".sfw" firmware file to ".rst" to create an equivalent RST firmware file.

Example:

Rename Vigorxxxx_1.2.3.4.sfw → Vigorxxxx_1.2.3.4.rst

Please ensure you back up your configuration before applying a ".rst" firmware, as all settings will be erased during the process.